Guide de planification de l'architecture de VMware View

View 4.5
View Manager 4.5
View Composer 2.5

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-000350-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

À propos de ce manuel

Le *Guide de planification de l'architecture de VMware View* présente VMware View™. Il décrit ses principales fonctions et options de déploiement et présente la façon dont les composants VMware View sont généralement configurés dans un environnement de production.

Ce guide répond aux questions suivantes :

- VMware View résout-il les problèmes pour lesquels vous avez besoin d'une solution ?
- Serait-il possible et rentable de mettre en place une solution VMware View dans votre entreprise ?

Pour vous aider à protéger votre installation VMware View, le guide comporte également une description des fonctions de sécurité.

Public cible

Ces informations sont conçues pour les décideurs, les architectes, les administrateurs informatiques et aux autres personnes qui veulent se familiariser avec les composants et les fonctions de VMware View. Avec ces informations, les architectes et les planificateurs peuvent déterminer si VMware View répond aux exigences de leur entreprise pour fournir de façon efficace et sûre des postes de travail et des applications Windows à leurs utilisateurs. L'exemple d'architecture aide les planificateurs à comprendre les exigences matérielles et à quantifier les efforts nécessaires pour un déploiement de VMware View à grande échelle.

Glossaire de VMware Technical Publications

VMware® Technical Publications fournit un glossaire de termes que vous pouvez ne pas connaître. Pour voir les définitions des termes dans la documentation technique de VMware, rendez-vous sur le site http://www.vmware.com/fr/support/pubs.

Commentaires sur les documents

VMware prend en considérations vos suggestions pour améliorer sa documentation. Si vous avez des commentaires, envoyez-les à docfeedback@vmware.com.

Ressources de support technique et de formation

Les ressources de support technique suivantes sont à votre disposition. Pour accéder à la version actuelle de ce guide et à d'autres guides, allez sur http://www.vmware.com/fr/support/pubs.

Support en ligne et téléphonique

Pour utiliser le support en ligne afin de soumettre des demandes de support technique, consulter les informations relatives à votre produit et à votre contrat et inscrire vos produits, allez sur http://www.vmware.com/fr/support.

Les clients ayant souscrit des contrats de support appropriés peuvent utiliser le support téléphonique pour obtenir une réponse rapide à leurs problèmes prioritaires. Allez sur http://www.vmware.com/fr/support/phone_support.html.

Offres de support

Pour en savoir plus sur la façon dont les offres de support VMware peuvent satisfaire les besoins de votre entreprise, allez sur http://www.vmware.com/fr/support/services.

VMware Professional Services

Les cours VMware Education Services proposent des laboratoires d'essai pratique, des études de cas et des matériaux approfondis conçus pour être utilisés comme outils de référence sur le lieu de travail. Les cours sont disponibles sur le site, dans la classe et en ligne et en direct. Pour les programmes pilotes sur site et les meilleures pratiques d'implémentation, VMware Consulting Services proposent des offres destinées à vous aider à évaluer, planifier, élaborer et gérer votre environnement virtuel. Pour accéder aux informations relatives aux formations, aux programmes de certification et aux services de consulting, allez sur http://www.vmware.com/fr/services.

Présentation de VMware View 1

Avec VMware View, les services informatiques peuvent exécuter des postes de travail virtuels dans le datacenter et fournir des postes de travail aux employés sous forme de service géré. Les utilisateurs bénéficient d'un environnement familier et personnalisé auquel ils peuvent accéder sur un grand nombre de périphériques depuis l'entreprise ou leur domicile. Les administrateurs bénéficient d'un contrôle, d'une efficacité et d'une sécurité centralisés en ayant les données de poste de travail dans le datacenter.

Ce chapitre aborde les rubriques suivantes :

Avantages à utiliser VMware View

Lorsque vous gérez des postes de travail d'entreprise avec VMware View, les avantages sont, entre autres, une fiabilité, une sécurité, une indépendance matérielle et une commodité améliorées.

Fiabilité et sécurité

Les postes de travail virtuels peuvent être centralisés en intégrant des ressources de stockage et de réseau avec VMware vSphere et un serveur de virtualisation. Placer des systèmes d'exploitation de poste de travail et des applications sur un serveur dans le datacenter fournit les avantages suivants :

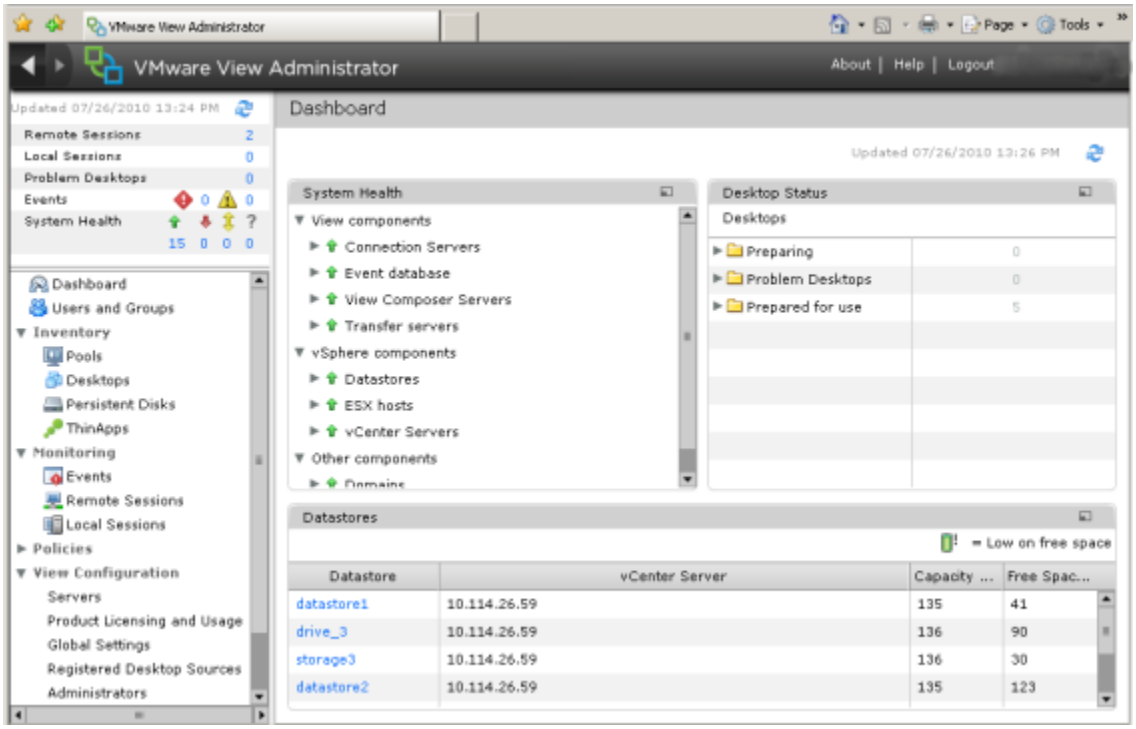
- L'accès aux données peut être limité facilement. La copie de données sensibles sur l'ordinateur personnel d'un employé peut être évitée.
- Des sauvegardes de données peuvent être programmées sans se soucier de l'heure à laquelle les systèmes des utilisateurs peuvent être éteints.
- Les postes de travail virtuels hébergés dans un datacenter rencontrent peu ou pas de temps d'arrêt. Les machines virtuelles peuvent résider sur des clusters à haute disponibilité de serveurs VMware.

Les postes de travail virtuels peuvent également se connecter à des systèmes physiques principaux et des serveurs Windows Terminal Services.

Commodité

La console de gestion unifiée est créée pour l'évolutivité sur Adobe Flex, pour que même les déploiements de View les plus importants puissent être gérés efficacement à partir d'une seule interface View Manager. Des assistants et des tableaux de bord améliorent le workflow et facilitent la descente dans la hiérarchie pour afficher des détails ou pour modifier des paramètres. Figure 1-1 montre un exemple de l'interface utilisateur basée sur un navigateur pour View Administrator.

Figure 1-1. Console administrative de View Manager montrant la vue du tableau de bord



Une autre fonction qui améliore la commodité est le protocole d'affichage à distance PCoIP de VMware. Le protocole d'affichage à distance PCoIP (PC-over-IP) délivre une expérience utilisateur équivalente à l'expérience actuelle d'utilisation d'un ordinateur physique :

- Sur les réseaux LAN, l'affichage est plus rapide et plus lisse que les affichages distants traditionnels.
- Sur les réseaux WAN, le protocole d'affichage peut compenser une augmentation de la latence ou une réduction de la bande passante, et garantir ainsi que les utilisateurs finaux peuvent rester productifs quelles que soient les conditions du réseau.

Gérabilité

L'approvisionnement de postes de travail pour les utilisateurs finaux est un processus rapide. Il n'est pas nécessaire d'installer des applications une par une sur le PC physique de chaque utilisateur final. Les utilisateurs finaux se connectent à un poste de travail virtuel contenant toutes les applications. Les utilisateurs finaux peuvent accéder au même poste de travail virtuel sur plusieurs périphériques à différents emplacements.

Utiliser VMware vSphere pour héberger des postes de travail virtuels fournit les avantages suivants :

- Les tâches administratives et de gestion sont réduites. Les administrateurs peuvent corriger et mettre à niveau des applications et des systèmes d'exploitation sans toucher à l'ordinateur physique d'un utilisateur.
- La gestion du stockage est simplifiée. Grâce à VMware vSphere, vous pouvez virtualiser des volumes et des systèmes de fichiers pour ne pas avoir à gérer des périphériques de stockage séparés.

Indépendance matérielle

Les machines virtuelles sont indépendantes du matériel. Comme un poste de travail View s'exécute sur un serveur dans le datacenter et qu'il n'est accessible que depuis un périphérique client, un poste de travail View peut utiliser des systèmes d'exploitation qui peuvent ne pas être compatibles avec le matériel du périphérique client.

Par exemple, même si Windows Vista peut s'exécuter sur des PC sur lesquels Vista est activé, vous pouvez installer Windows Vista sur une machine virtuelle et utiliser cette machine virtuelle sur un PC sur lequel Vista n'est pas activé. Les postes de travail virtuels s'exécutent sur des PC, des Mac, des clients légers et des PC requalifiés comme clients légers.

Fonctions de VMware View

Les fonctions incluses dans VMware View comprennent la convivialité, la sécurité, le contrôle centralisé et l'évolutivité.

Les fonctions suivantes fournissent une expérience commune pour l'utilisateur final :

- Impression depuis un poste de travail virtuel sur n'importe quelle imprimante locale ou en réseau définie sur le périphérique client, ou utilisation de la fonction d'impression basée sur l'emplacement pour mapper vers des imprimantes qui sont physiquement proches du système client. La fonction d'impression virtuelle résout les problèmes de compatibilité et vous n'avez pas à installer de pilotes d'imprimante supplémentaires sur une machine virtuelle.
- Utilisation de plusieurs écrans. Avec la prise en charge de plusieurs écrans de PCoIP, vous pouvez régler la résolution et la rotation d'affichage séparément pour chaque écran.
- Accès à des périphériques USB et autres connectés au périphérique local qui affiche votre poste de travail virtuel.

VMware View offre les fonctions de sécurité suivantes (parmi d'autres) :

- Utilisation de l'authentification à deux facteurs RSA SecurID ou de cartes à puce pour ouvrir une session.
- Utilisation du tunneling SSL pour garantir que toutes les connexions sont complètement cryptées.
- Utilisation de VMware High Availability pour héberger des postes de travail et pour assurer un basculement automatique.

Les fonctions suivantes fournissent une administration et une gestion centralisées :

- Utilisation de Microsoft Active Directory pour gérer l'accès à des postes de travail virtuels et pour gérer des règles.
- Utilisation de la console administrative Web pour gérer des postes de travail virtuels depuis n'importe quel emplacement.
- Utilisation d'un modèle, ou d'une image maître, pour créer et approvisionner rapidement des pools de postes de travail.
- Envoi de mises à jour et de correctifs à des postes de travail virtuels sans affecter les paramètres, les données ou les préférences utilisateur.

Les fonctions d'évolutivité dépendent de la plate-forme de virtualisation VMware pour gérer à la fois des postes de travail et des serveurs :

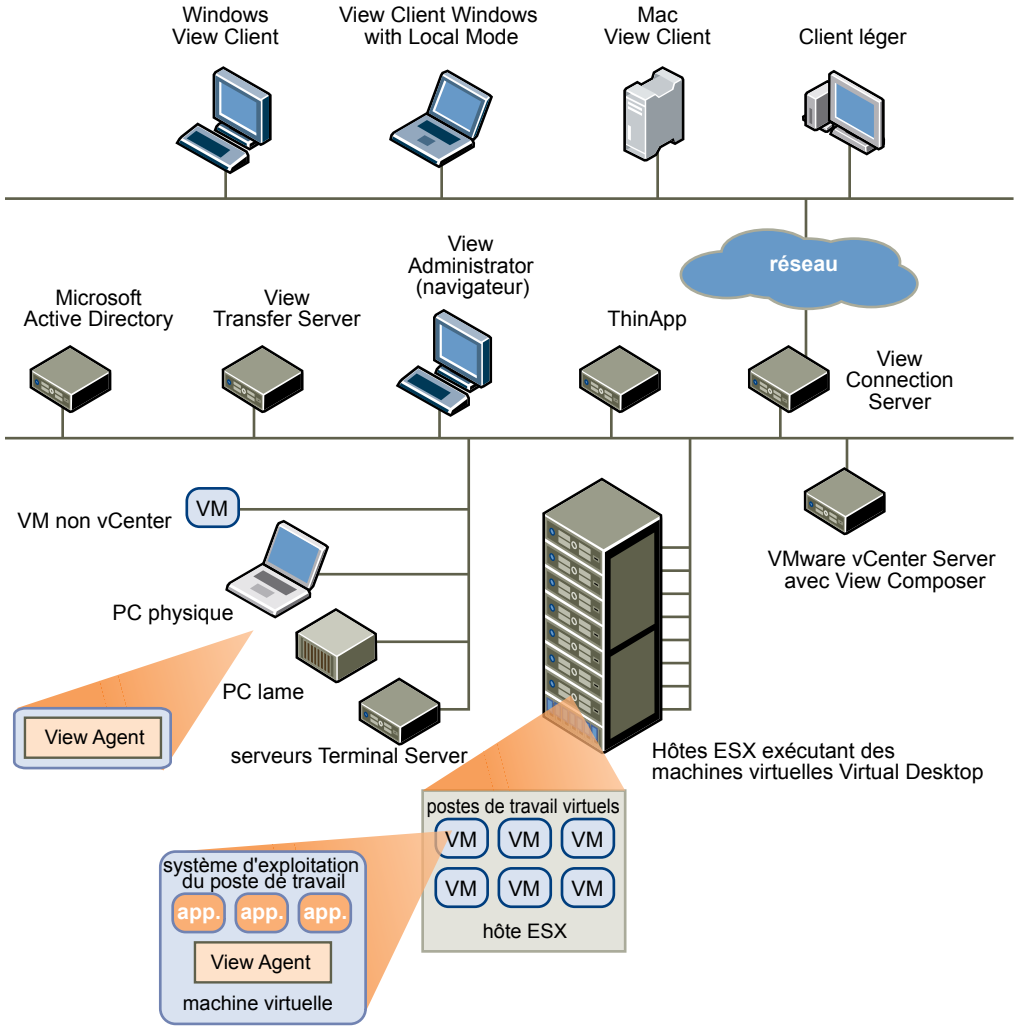
- Intégration à VMware vSphere pour atteindre des densités rentables, des hauts niveaux de disponibilité et un contrôle avancé de l'allocation des ressources pour vos postes de travail virtuels.
- Configuration de View Connection Server pour des connexions de broker entre les utilisateurs finaux et les postes de travail virtuels qu'ils sont autorisés à accéder.
- Utilisation de View Composer pour créer rapidement des images de poste de travail qui partagent des disques virtuels avec une image maître. L'utilisation de clones liés de cette façon conserve l'espace disque et simplifie la gestion des correctifs et des mises à jour du système d'exploitation.

Comment les composants VMware View fonctionnent ensemble

Les utilisateurs finaux démarrent View Client pour ouvrir une session sur View Connection Server. Ce serveur, qui s'intègre à Windows Active Directory, permet d'accéder à un poste de travail virtuel hébergé sur un serveur VMware ESX, un PC lame ou physique ou un serveur Windows Terminal Services.

La Figure 1-2 montre la relation entre les composants principaux d'un déploiement de VMware View.

Figure 1-2. Exemple de haut niveau d'un environnement VMware View



Périphériques clients

L'avantage principal d'utiliser VMware View est que les postes de travail suivent l'utilisateur final quel que soit le périphérique ou l'emplacement. Les utilisateurs peuvent accéder à leur poste de travail virtuel personnalisé depuis un ordinateur portable de l'entreprise, depuis leur ordinateur personnel, depuis un périphérique de client léger ou depuis un Mac.

Sur des ordinateurs portables et des PC Mac et Windows, les utilisateurs finaux ouvrent View Client pour afficher leur poste de travail View. Les périphériques de client léger utilisent le logiciel View Thin Client et peuvent être configurés pour que la seule application pouvant être lancée par les utilisateurs directement sur le périphérique soit View Thin Client. Requalifier un PC hérité en poste de travail de client léger peut allonger la durée de vie du matériel de trois à cinq ans. Par exemple, en utilisant VMware View sur un poste de travail léger, vous pouvez utiliser un système d'exploitation plus récent, comme Windows Vista, sur un matériel de poste de travail antérieur.

View Connection Server

Ce service logiciel agit comme un broker pour les connexions client. View Connection Server authentifie les utilisateurs via Windows Active Directory et dirige la demande vers la machine virtuelle appropriée, le PC physique ou lame, ou le serveur Windows Terminal Services.

View Connection Server fournit les fonctions de gestion suivantes :

- l'authentification d'utilisateurs ;
- l'autorisation d'utilisateurs sur des postes de travail et des pools spécifiques ;
- l'attribution d'applications fournies avec VMware ThinApp à des postes de travail et des pools spécifiques ;
- la gestion des sessions de postes de travail locales et distantes ;
- l'établissement de connexions sécurisées entre utilisateurs et postes de travail ;
- l'activation de l'authentification unique ;
- la définition et l'application de règles.

Dans le pare-feu de l'entreprise, vous installez et configurez un groupe de deux instances de View Connection Server ou plus. Leurs données de configuration sont stockées dans un répertoire LDAP incorporé et sont répliquées sur les membres du groupe.

À l'extérieur du pare-feu de l'entreprise, dans la DMZ, vous pouvez installer et configurer View Connection Server en tant que serveur de sécurité. Des serveurs de sécurité dans la DMZ communiquent avec des serveurs View Connection Server dans le pare-feu de l'entreprise. Des serveurs de sécurité offrent un sous-ensemble de fonctionnalités et ne doivent pas nécessairement se trouver dans un domaine Active Directory.

Vous installez View Connection Server dans un serveur Windows Server 2003 ou 2008, de préférence sur une machine virtuelle VMware.

View Client

Le logiciel client pour accéder aux postes de travail View s'exécute sur un PC Windows ou Mac en tant qu'application Windows native ou sur un client léger si vous possédez View Client pour Linux.

Après avoir ouvert une session, les utilisateurs choisissent parmi une liste de postes de travail virtuels qu'ils sont autorisés à utiliser. L'autorisation peut requérir des informations d'identification Active Directory, un UPN, un code PIN de carte à puce ou un jeton RSA SecurID.

Un administrateur peut configurer View Client pour autoriser les utilisateurs finaux à sélectionner un protocole d'affichage. Les protocoles incluent PCoIP, Microsoft RDP et HP RGS pour des postes de travail View qui sont hébergés sur des PC HP lame. La vitesse et la qualité d'affichage de PCoIP sont équivalentes à celle d'un PC physique.

View Client with Local Mode (connu précédemment sous le nom Offline Desktop) est une version de View Client qui a été étendue pour permettre aux utilisateurs finaux de télécharger des machines virtuelles et de les utiliser sur les systèmes locaux qu'ils aient une connexion réseau ou non.

Les fonctions diffèrent en fonction du View Client que vous utilisez. Ce guide décrit principalement View Client pour Windows et View Client pour Mac. Les types de client suivants ne sont pas décrits en détail dans ce guide :

- View Client pour Linux, disponible uniquement via des partenaires référencés.
- Divers clients tiers, disponibles uniquement via des partenaires référencés.
- View Open Client, qui prend en charge le programme de certification des partenaires VMware. View Open Client n'est pas un client officiel de View et il n'est pas pris en charge comme tel.

View Portal

Sur un PC ou un ordinateur portable Windows , les utilisateurs finaux peuvent ouvrir un navigateur Web et utiliser View Portal pour télécharger, installer, mettre à jour et démarrer View Client pour Windows . Comme avec View 4.5, View Portal installe la version complète de View Client pour Windows, avec ou sans Local Mode.

Pour utiliser View Portal, les utilisateurs finaux ouvrent un navigateur Internet Explorer et saisissent l'URL d'une instance de View Connection Server. View Portal fournit un lien pour télécharger le programme d'installation de la version complète de View Client pour Windows.

View Agent

Vous installez le service View Agent sur l'ensemble des machines virtuelles, des systèmes physiques et des serveurs Terminal Service que vous utilisez comme sources pour les postes de travail View. Cet agent communique avec View Client pour fournir des fonctions comme le contrôle des connexions, l'impression virtuelle et l'accès à des périphériques USB connectés en local.

Si la source de postes de travail est une machine virtuelle, vous devez d'abord installer le service View Agent sur cette machine virtuelle et utiliser la machine virtuelle comme un modèle ou un parent de clones liés. Lorsque vous créez un pool depuis cette machine virtuelle, l'agent est automatiquement installé sur chaque poste de travail virtuel.

Vous pouvez installer l'agent avec une option pour l'authentification unique. Avec cette option, les utilisateurs sont invités à ouvrir une session uniquement lorsqu'ils se connectent à View Connection Server et ne sont pas invités une deuxième fois à se connecter à un poste de travail virtuel.

View Administrator

Cette application Web permet aux administrateurs de configurer View Connection Server, de déployer et de gérer des postes de travail View, de contrôler l'authentification utilisateur et de résoudre des problèmes d'utilisateur.

Lorsque vous installez une instance de View Connection Server, l'application View Administrator est également installée. Cette application permet aux administrateurs de gérer des instances de View Connection Server depuis n'importe quel endroit sans avoir à installer d'application sur leur ordinateur local.

View Composer

Vous installez ce service logiciel sur une instance de vCenter Server qui gère des machines virtuelles. View Composer peut alors créer un pool de clones liés à partir d'une machine virtuelle parente spécifiée. Cette stratégie réduit les coûts de stockage de 90 % au 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 car il partage une image de base avec le parent.

Comme les pools de postes de travail de clone lié partagent une image de base, vous pouvez rapidement déployer des mises à jour et des correctifs en ne mettant à jour que la machine virtuelle parente. Les paramètres, les données et les applications des utilisateurs finaux ne sont pas affectés. Comme avec View 4.5, vous pouvez également utiliser la technologie de clone lié pour des postes de travail View que vous téléchargez et empruntez afin de les utiliser sur des systèmes locaux.

vCenter Server

Ce service agit comme administrateur central des serveurs VMware ESX qui sont connectés sur un réseau. vCenter Server, connu précédemment sous le nom VMware VirtualCenter, fournit le point central pour la configuration, l'approvisionnement et la gestion de machines virtuelles dans le datacenter.

En plus de l'utilisation de ces machines virtuelles comme sources de pools de postes de travail View, vous pouvez utiliser des machines virtuelles pour héberger des composants du serveur de VMware View, y compris des instances de Connection Server, des serveurs Active Directory et des instances de vCenter Server.

Vous pouvez installer View Composer sur le même serveur que vCenter Server pour créer des pools de postes de travail de clone lié. vCenter Server gère ensuite l'attribution des machines virtuelles aux serveurs physiques et au stockage et gère l'attribution de CPU et de ressources de mémoire aux machines virtuelles.

Vous installez vCenter Server dans un serveur Windows Server 2003 ou 2008, de préférence sur une machine virtuelle VMware.

View Transfer Server

Ce logiciel gère et rationalise des transferts de données entre le datacenter et des postes de travail View qui sont empruntés afin d'être utilisés sur des systèmes locaux d'utilisateurs finaux. View Transfer Server est requis pour prendre en charge des postes de travail qui exécutent View Client with Local Mode (connu précédemment sous le nom Offline Desktop).

Plusieurs opérations utilisent View Transfer Server pour envoyer des données entre le poste de travail View dans vCenter Server et le poste de travail local correspondant sur le système client.

- Lorsqu'un utilisateur restitue ou emprunte un poste de travail, View Manager autorise et gère l'opération. View Transfer Server transfère les fichiers entre le datacenter et le poste de travail local.
- View Transfer Server synchronise des postes de travail locaux avec les postes de travail correspondants dans le datacenter en répliquant les modifications générées par l'utilisateur dans le datacenter.

  Les réplications se produisent à des intervalles que vous spécifiez dans des règles de mode local. Vous pouvez également initier des réplications dans View Administrator. Vous pouvez définir une règle qui permet aux utilisateurs d'initier des réplications à partir de leurs postes de travail locaux.
- View Transfer Server maintient les postes de travail locaux à jour en distribuant des données système communes à partir du datacenter vers les clients locaux. View Transfer Server télécharge des images de base de View Composer à partir du référentiel d'images vers des postes de travail locaux.
- Si un ordinateur local est corrompu ou perdu, View Transfer Server peut approvisionner le poste de travail local et restaurer les données utilisateur en téléchargeant les données et l'image système sur le poste de travail local.

Intégration et personnalisation de VMware View

Pour améliorer l'efficacité de VMware View dans votre entreprise, vous pouvez utiliser plusieurs interfaces pour intégrer VMware View avec des applications externes ou pour créer des scripts d'administration que vous pouvez exécuter depuis la ligne de commande ou en mode lot.

Intégration de View avec un logiciel de Business Intelligence

Vous pouvez configurer VMware View pour enregistrer des événements dans une base de données Microsoft SQL Server ou Oracle.

- Des actions d'utilisateur final telles que l'ouverture de session et le lancement d'une session de poste de travail.
- Des actions d'administrateur telles que l'ajout d'autorisations et la création de pools de postes de travail.
- Des alertes qui rapportent des échecs et des erreurs du système.
- Un échantillonnage statistique tel que l'enregistrement du nombre maximum d'utilisateurs sur une période de 24 heures.

Vous pouvez utiliser des moteurs de reporting de Business Intelligence tels que Crystal Reports, IBM Cognos, MicroStrategy 9 et Oracle Enterprise Performance Management System pour accéder à la base de données des événements et l'analyser.

Pour plus d'informations, consultez le *Guide d'intégration de VMware View*.

Utilisation de View PowerCLI pour créer des scripts d'administration

Windows PowerShell est un environnement de ligne de commande et de script conçu pour Microsoft Windows. PowerShell utilise le modèle d'objet .NET et fournit aux administrateurs des fonctions de gestion et d'automatisation. Comme avec tout autre environnement de console, vous utilisez PowerShell en exécutant des commandes, qui sont appelées cmdlets dans PowerShell.

View PowerCLI fournit une interface PowerShell facile à utiliser dans VMware View. Vous pouvez utiliser les cmdlets de View PowerCLI pour effectuer diverses tâches d'administration sur des composants View.

- Créez et mettez à jour des pools de postes de travail.
- Ajoutez des ressources de datacenter à une machine virtuelle complète ou un pool de clone lié.
- Effectuez des opérations de rééquilibrage, d'actualisation ou de recomposition sur des postes de travail de clone lié.
- Échantillonnez l'utilisation de postes de travail ou de pools de postes de travail spécifiques dans le temps.
- Interrogez la base de données des événements.
- Interrogez l'état des services View.

Vous pouvez utiliser les cmdlets avec les cmdlets de vSphere PowerCLI, ce qui fournit une interface administrative au produit VMware vSphere.

Pour plus d'informations, consultez le *Guide d'intégration de VMware View*.

Modification des données de configuration LDAP dans View

Lorsque vous utilisez View Administrator pour modifier la configuration de VMware View, les données LDAP appropriées dans le référentiel sont mises à jour. VMware View stocke ses informations de configuration dans un référentiel compatible avec LDAP. Par exemple, si vous ajoutez un pool de postes de travail, VMware View stocke des informations sur les utilisateurs, les groupes d'utilisateurs et les autorisations dans LDAP.

Vous pouvez utiliser des outils de commande VMware et Microsoft pour exporter et importer des données de configuration LDAP dans des fichiers LDIF (LDAP Data Interchange Format) depuis et vers VMware View. Ces commandes sont destinées aux administrateurs avancés qui souhaitent utiliser des scripts pour mettre à jour des données de configuration sans utiliser View Administrator ou View PowerCLI.

Vous pouvez utiliser des fichiers LDIF pour effectuer plusieurs tâches.

- Transférer des données de configuration entre des instances de View Connection Server.
- Définir un nombre important d'objets View, tels que des pools de postes de travail, et ajouter ces objets à vos instances de View Connection Server sans utiliser View Administrator ou View PowerCLI.
- Sauvegarder votre configuration View pour que vous puissiez restaurer l'état d'une instance de View Connection Server.

Pour plus d'informations, consultez le *Guide d'intégration de VMware View*.

Utilisation de SCOM pour surveiller des composants View

Vous pouvez utiliser Microsoft SCOM (System Center Operations Manager) pour surveiller l'état et les performances de composants VMware View, y compris des instances de View Connection Server et des serveurs de sécurité et des services View exécutés sur ces hôtes.

Pour plus d'informations, consultez le *Guide d'intégration de VMware View*.

Utilisation de la commande vdmadmin pour administrer View

Vous pouvez utiliser l'interface de ligne de commande `vdmadmin` pour effectuer plusieurs tâches d'administration sur une instance de View Connection Server. Vous pouvez utiliser `vdmadmin` pour effectuer des tâches d'administration qui ne sont pas possibles depuis l'interface utilisateur de View Administrator ou qui doivent être exécutées automatiquement depuis des scripts.

Pour plus d'informations, consultez le *Guide de l'administrateur de VMware View*.

Planification d'une expérience d'utilisateur riche

2

VMware View fournit l'environnement de poste de travail familier et personnalisé que tous les utilisateurs finaux attendent. Les utilisateurs finaux peuvent accéder à des périphériques USB et autres connectés à leur ordinateur local, envoyer des documents à une imprimante pouvant être détectée par leur ordinateur local, s'authentifier avec des cartes à puce et utiliser plusieurs écrans.

VMware View inclut plusieurs fonctions que vous pouvez vouloir rendre disponibles à vos utilisateurs finaux. Avant de décider quelles fonctions utiliser, vous devez comprendre les limites et les restrictions de chaque fonction.

Ce chapitre aborde les rubriques suivantes :

Matrice de prise en charge des fonctions

La plupart des fonctions, telles que l'accès à des périphériques USB locaux, l'impression virtuelle, la redirection multimédia Wyse (MMR) et les protocoles d'affichage PCoIP et Microsoft RDP, sont prises en charge sur la plupart des systèmes d'exploitation client.

Lorsque vous décidez du protocole d'affichage et des fonctions à rendre disponibles pour les utilisateurs, utilisez le Tableau 2-1 et le Tableau 2-2 pour déterminer les systèmes d'exploitation client prenant en charge la fonction.

Tableau 2-1. Fonctions prises en charge sur des clients Windows

Fonction	Windows XP Home/Pro SP3, 32 bits	Windows Vista SP1, SP2, 32 bits	Windows 7, 32 bits et 64 bits
Accès USB	X	X	X
Protocole d'affichage RDP	X	X	X
Protocole d'affichage PCoIP	X	X	X

Tableau 2-1. Fonctions prises en charge sur des clients Windows (suite)

Fonction	Windows XP Home/Pro SP3, 32 bits	Windows Vista SP1, SP2, 32 bits	Windows 7, 32 bits et 64 bits
Protocole d'affichage HP RGS	X	X	
Wyse MMR	X	X	
Impression virtuelle	X	X	X
Cartes à puce	X	X	X
RSA SecurID	X	X	X
Authentification unique	X	X	X
Plusieurs écrans	X	X	X
Mode local	X	X	X

Les éditions de Windows Vista incluent Windows Vista Home, Enterprise, Ultimate et Business. Les éditions de Windows 7 incluent Home, Professional, Enterprise et Ultimate.

Tableau 2-2. Fonctions prises en charge sur des clients Mac

Fonction	Mac OS X (10.5,6)	Mac OS X (10.6)
Accès USB		
Protocole d'affichage RDP	X	X
Protocole d'affichage PCoIP		
Protocole d'affichage HP RGS		
Wyse MMR		
Impression virtuelle		
Cartes à puce		
RSA SecurID	X	X
Authentification unique	X	X
Plusieurs écrans		
Mode local		

De plus, plusieurs partenaires de VMware offrent des périphériques de client léger pour les déploiements de VMware View. Les fonctions disponibles pour chaque périphérique de client léger sont déterminées par le fournisseur, le modèle et la configuration qu'une entreprise choisit d'utiliser. Pour plus d'informations sur les fournisseurs et les modèles de périphériques de client léger, consultez le guide *Thin Client Compatibility Guide*, disponible sur le site Web de VMware.

Choisir un protocole d'affichage

Un protocole d'affichage fournit aux utilisateurs une interface graphique sur un poste de travail View qui réside dans le datacenter. Vous pouvez utiliser Microsoft RDP (Remote Desktop Protocol), HP RGS pour machines physiques HP ou PCoIP (PC-over-IP).

Vous pouvez définir des règles pour contrôler quel protocole est utilisé ou pour laisser les utilisateurs finaux choisir le protocole lorsqu'ils ouvrent une session sur un poste de travail.

Remarque Lorsque vous empruntez un poste de travail pour l'utiliser sur un système client local, les protocoles d'affichage à distance RDP ou PCoIP ne sont pas utilisés.

VMware View avec PCoIP

PCoIP est un nouveau protocole d'affichage à distance haute performance fourni par VMware. Ce protocole est disponible pour les postes de travail View qui proviennent de machines virtuelles, de clients Teradici et de machines physiques qui ont des cartes hôte compatibles avec Teradici.

PCoIP peut compenser une augmentation de la latence ou une réduction de la bande passante, et garantir ainsi que les utilisateurs finaux peuvent rester productifs quelles que soient les conditions du réseau. PCoIP est optimisé pour la livraison d'images, de contenu audio et vidéo pour une large gamme d'utilisateurs sur le réseau LAN ou WAN. PCoIP fournit les fonctions suivantes :

- Vous pouvez utiliser jusqu'à 4 écrans et régler la résolution de chaque écran séparément (résolution maximale de 2 560 x 1 600 par écran).
- Vous pouvez copier et coller du texte entre le système local et le poste de travail View, mais vous ne pouvez pas copier et coller des objets système, tels que des dossiers et des fichiers, entre les systèmes.
- Vous pouvez configurer la quantité de bande passante utilisée par le contenu Adobe Flash pour améliorer la qualité globale des recherches Web et rendre d'autres applications plus réactives.
- PCoIP prend en charge les couleurs 32 bits.
- PCoIP prend en charge le cryptage 128 bits.
- PCoIP prend en charge le cryptage AES (Advanced Encryption Standard) qui est activé par défaut.
- Vous pouvez utiliser ce protocole avec le réseau privé virtuel de votre entreprise.

Les exigences matérielles du client sont les suivantes :

- vitesse de processeur d'au moins 800 MHz
- processeur x86 avec extensions SSE2

Les clients View qui utilisent PCoIP peuvent se connecter à des serveurs de sécurité View, mais les sessions PCoIP avec le poste de travail virtuel ignorent le serveur de sécurité. PCoIP utilise le protocole UDP (User Datagram Protocol) pour la diffusion audio et vidéo. Les serveurs de sécurité ne prennent en charge que TCP.

Microsoft RDP

Remote Desktop Protocol est le même protocole que de nombreuses personnes utilisent déjà pour accéder à leur ordinateur professionnel depuis leur ordinateur à domicile. RDP permet d'accéder à toutes les applications, fichiers et ressources réseau sur un ordinateur distant.

Microsoft RDP fournit les fonctions suivantes :

- Vous pouvez utiliser plusieurs écrans en mode étendu.
- Vous pouvez copier et coller du texte entre le système local et le poste de travail View, mais vous ne pouvez pas copier et coller des objets système, tels que des dossiers et des fichiers, entre les systèmes.
- Vous pouvez configurer la quantité de bande passante utilisée par le contenu Adobe Flash pour améliorer la qualité globale des recherches Web et rendre d'autres applications plus réactives.
- RDP prend en charge les couleurs 32 bits.
- RDP prend en charge le cryptage 128 bits.
- Vous pouvez utiliser ce protocole pour sécuriser des connexions cryptées à un serveur de sécurité View dans la zone DMZ de l'entreprise.

Protocole HP RGS

RGS est un protocole d'affichage de HP qui permet aux utilisateurs d'accéder au poste de travail d'un ordinateur physique distant sur un réseau standard.

Vous pouvez utiliser HP RGS comme protocole d'affichage pour une connexion sur des PC HP lame, des stations de travail HP et HP lame. Les connexions à des machines virtuelles qui s'exécutent sur des serveurs VMware ESX ne sont pas prises en charge.

HP RGS fournit les fonctions suivantes :

- Vous pouvez utiliser plusieurs écrans en mode étendu.
- Vous pouvez configurer la quantité de bande passante utilisée par le contenu Adobe Flash pour améliorer la qualité globale des recherches Web et rendre d'autres applications plus réactives.

VMware ne groupe et n'autorise pas HP RGS avec VMware View. Contactez HP pour autoriser une copie de HP RGS version 5.2.5 à utiliser avec VMware View. Pour plus d'informations sur l'installation et la configuration des composants HP RGS, consultez la documentation HP RGS disponible à l'adresse http://www.hp.com.

Utilisation d'un poste de travail View sans connexion réseau

Avec View Client with Local Mode, les utilisateurs peuvent emprunter et télécharger un poste de travail View sur un système local tel qu'un ordinateur portable. Les administrateurs peuvent gérer ces postes de travail View locaux en définissant des règles pour la fréquence des sauvegardes et des contacts avec le serveur, pour l'accès à des périphériques USB et pour l'autorisation de restitution des postes de travail.

Pour les employés dans des bureaux distants, les applications peuvent s'exécuter plus rapidement sur un poste de travail View local que sur un poste de travail distant. De même, les utilisateurs peuvent utiliser la version locale du poste de travail avec ou sans connexion réseau.

Si une connexion réseau est présente sur le système client, le poste de travail emprunté continue de communiquer avec View Connection Server afin de fournir des mises à jour de règles et d'assurer que les critères d'authentification mise en cache en local sont actuels. Par défaut, le contact est tenté toutes les 5 minutes.

View Client with Local Mode est la fonction entièrement prise en charge qui, dans les versions précédentes, était une fonction expérimentale appelée View Client avec Offline Desktop.

Les postes de travail View en mode local se comportent de la même façon que les postes de travail distants équivalents qui peuvent déjà bénéficier de ressources locales. La latence est éliminée et les performances sont améliorées. Les utilisateurs peuvent se déconnecter de leur poste de travail View local puis de nouveau ouvrir une session sans se connecter au serveur View Connection Server. Une fois l'accès au réseau restauré, ou lorsque l'utilisateur est prêt, la machine virtuelle empruntée peut être sauvegardée, restaurée ou restituée.

Utilisation de ressources locales

Une fois emprunté, un poste de travail local peut bénéficier des capacités de mémoire et de CPU du système local. Par exemple, la mémoire disponible au-delà de ce qui est requis pour les systèmes d'exploitation hôte et client est généralement divisée entre l'hôte et le poste de travail View local, quels que soient les paramètres de mémoire spécifiés pour la machine virtuelle dans vCenter Server. De la même façon, le poste de travail View local peut automatiquement utiliser jusqu'à deux CPU disponibles sur le système local, et vous pouvez configurer le poste de travail local pour utiliser jusqu'à quatre CPU.

	Bien qu'un poste de travail local puisse bénéficier de ressources locales, un poste de travail View Windows 7 ou Windows Vista créé sur un hôte ESX 3.5 ne peut pas produire d'effets 3D et Windows Aero. Cette limite s'applique même lorsque le poste de travail est emprunté pour une utilisation locale sur un hôte Windows 7 ou Windows Vista. Les effets Windows Aero et 3D ne sont disponibles que si le poste de travail View est créé à l'aide de vSphere 4.x.
Conservation de ressources de datacenter en demandant le mode local	Vous pouvez réduire les coûts de datacenter associés à la bande passante, à la mémoire et aux ressources de CPU en demandant que des postes de travail View soient téléchargés et utilisés uniquement en mode local. Cette stratégie est parfois appelée programme BRYO (bring-your-own-PC, apporter votre propre PC) pour les employés et les prestataires.
Emprunts	Lorsque le poste de travail View est emprunté, la version vCenter Server du poste de travail est verrouillée pour qu'aucun autre utilisateur ne puisse y accéder. Lorsqu'un poste de travail View est verrouillé, les opérations de vCenter Server sont désactivées, y compris les opérations telles que la mise sous tension du poste de travail en ligne, la prise de snapshots et la modification des paramètres de la machine virtuelle. Toutefois, les administrateurs de View peuvent toujours surveiller la session locale et accéder à la version vCenter Server pour supprimer l'accès ou restaurer le poste de travail.
Sauvegardes	Lors des sauvegardes, le poste de travail View dans vCenter Server est mis à jour avec toutes les nouvelles données et configurations, mais le poste de travail local reste emprunté sur le système local et le verrou reste défini dans vCenter Server.
Restaurations	Lors des restaurations, le poste de travail View local est ignoré et le verrou est retiré dans vCenter Server. Les futures connexions client sont dirigées vers le poste de travail View dans vCenter Server jusqu'à ce que le poste de travail soit emprunté de nouveau.
Restitutions	Lors de la restitution d'un poste de travail View, le poste de travail local est téléchargé dans vCenter Server et le verrou est retiré. Les futures connexions client sont dirigées vers le poste de travail View dans vCenter Server jusqu'à ce que le poste de travail soit emprunté de nouveau.

Les données sur chaque système local sont cryptées avec AES. Le cryptage 128 bits est appliqué par défaut, mais vous pouvez configurer un cryptage 256 bits. Le poste de travail a une durée de vie contrôlée par une règle. Si le client perd le contact avec View Connection Server, la durée maximale sans contact avec le serveur est la période au cours de laquelle l'utilisateur peut continuer à utiliser le poste de travail avant que son accès soit refusé. De même, si l'accès de l'utilisateur est supprimé, le système client devient inaccessible lorsque le cache expire ou que le client détecte cette modification via View Connection Server.

View Client with Local Mode a les limites et restrictions suivantes :

- Vous devez disposer d'une licence View incluant le composant Local Mode.
- Les utilisateurs finaux ne peuvent pas accéder à leur poste de travail local au cours de restaurations et de restitutions.
- Cette fonction n'est disponible que pour les machines virtuelles gérées par vCenter Server.
- L'affection de packages d'application créés avec VMware ThinApp n'est pas prise en charge sur les postes de travail locaux.

- Pour des raisons de sécurité, vous ne pouvez pas accéder au CD-ROM hôte à partir du poste de travail View,
- ni copier et coller du texte ou des objets système tels que des fichiers et des dossiers entre le système local et le poste de travail View.

Accéder à des périphériques USB connectés à un ordinateur local

Les administrateurs peuvent configurer l'utilisation des périphériques USB, tels que des clés USB, des périphériques VoIP (voice-over-IP) et des imprimantes, à partir d'un poste de travail View. Cette fonction est appelée redirection USB.

Lorsque vous utilisez cette fonction, la plupart des périphériques USB fixés au système client local deviennent disponibles à partir d'un menu dans View Client. Vous utilisez le menu pour connecter et déconnecter les périphériques.

Les périphériques USB qui n'apparaissent pas dans le menu, mais qui sont disponibles dans un poste de travail View, comportent des lecteurs de carte à puce et des périphériques d'interface utilisateur tels que des claviers et des dispositifs de pointage. Le poste de travail View et l'ordinateur local utilisent ces périphériques en même temps.

Cette fonction a les limites suivantes :

- Lorsque vous accédez à un périphérique USB depuis un menu de View Client et que vous utilisez le périphérique sur un poste de travail View, vous ne pouvez pas accéder au périphérique sur l'ordinateur local.
- La redirection USB n'est pas prise en charge pour les systèmes Windows 2000 ou pour les postes de travail View provenant de serveurs Microsoft Terminal Server.

Impression à partir d'un poste de travail View

La fonction d'impression virtuelle permet aux utilisateurs finaux d'utiliser des imprimantes locales ou en réseau à partir d'un poste de travail View sans avoir à installer de pilotes d'imprimante supplémentaires sur le poste de travail View. Pour chaque imprimante disponible via cette fonction, vous pouvez définir des préférences pour la compression des données, la qualité d'impression, l'impression recto verso, la couleur, etc.

Une fois une imprimante ajoutée sur l'ordinateur local, View ajoute cette imprimante à la liste d'imprimantes disponibles sur le poste de travail View. Aucune configuration supplémentaire n'est requise. Les utilisateurs qui ont des privilèges d'administrateur peuvent installer des pilotes d'imprimante sur le poste de travail View sans créer de conflit avec le composant d'impression virtuelle.

Pour envoyer des travaux d'impression à une imprimante USB, vous pouvez utiliser la fonction de redirection USB ou la fonction d'impression virtuelle.

De plus, les fonctions d'impression basée sur l'emplacement depuis View 4.5 permettent aux services informatiques de mapper des postes de travail View vers une imprimante qui est 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.

Diffusion multimédia sur un poste de travail View

Wyse MMR (redirection multimédia) permet la lecture haute fidélité lorsque des fichiers multimédia sont diffusés sur un poste de travail View.

La fonction MMR prend en charge les formats de fichier média que le système client prend en charge, car des décodeurs locaux doivent exister sur le client. Les formats fichiers incluent MPEG2, WMV, AVI, WAV, etc.

Cette fonction a les limites suivantes :

- Pour une meilleure qualité, utilisez Windows Media Player 10 ou supérieur et installez-le sur l'ordinateur local, ou un périphérique d'accès client, et sur le poste de travail View.
- Le port Wyse MMR, 9427 par défaut, doit être ajouté en tant qu'exception de pare-feu sur le poste de travail View.
- MMR n'est pas pris en charge sur les clients ou postes de travail virtuels Windows 7.

  Bien que MMR ne soit pas pris en charge sur les postes de travail virtuels Windows 7, si le poste de travail Windows 7 a 1 Go de RAM et 2 CPU virtuelles, vous pouvez utiliser PCoIP pour lire des vidéos aux formats 480 p et 720 p à des résolutions natives. Pour 1 080 p, vous devrez peut-être réduire la taille de la fenêtre et ne pas utiliser le mode plein écran.

Utiliser l'authentification unique pour ouvrir une session sur un poste de travail View

La fonction d'authentification unique (SSO) vous permet de configurer View Manager pour que les utilisateurs finaux soient invités à n'ouvrir une session qu'une seule fois.

Si vous n'utilisez pas la fonction d'authentification unique, les utilisateurs finaux doivent ouvrir une session deux fois. Ils sont d'abord invités à ouvrir une session sur View Connection Server puis de nouveau sur leur poste de travail View. Si des cartes à puce sont également utilisées, les utilisateurs finaux doivent ouvrir une session trois fois car le lecteur de carte à puce leur demande leur code PIN.

SSO est implémenté comme composant facultatif que vous pouvez sélectionner quand vous installez View Agent sur une source de poste de travail. Cette fonction comporte la bibliothèque de liens dynamiques GINA (Graphical Identification and Authentication) pour Windows XP et une bibliothèque de liens dynamiques fournisseur d'informations d'identification pour Windows Vista.

Utilisation de plusieurs écrans avec un poste de travail View

Quel que soit le protocole d'affichage, vous pouvez utiliser plusieurs écrans avec un poste de travail View.

Si vous utilisez le protocole d'affichage VMware PCoIP, vous pouvez régler la résolution et la rotation d'affichage séparément pour chaque écran. PCoIP permet d'utiliser une session à plusieurs écrans plutôt qu'une session en mode étendu.

Une session à distance en mode étendu est en fait une session à un seul écran. Les écrans doivent avoir la même taille et la même résolution, et la disposition de l'écran doit rentrer dans un cadre englobant. Si vous agrandissez la fenêtre d'une application, elle s'étend sur tous les écrans.

Dans une session à plusieurs écrans, les écrans peuvent avoir des résolutions et des tailles différentes, et un écran peut être pivoté. Si vous agrandissez la fenêtre d'une application, elle s'étend au format plein écran uniquement sur l'écran qui la contient.

Cette fonction a les limites suivantes :

- Le nombre maximum d'écrans pouvant être utilisés pour afficher un poste de travail View est de 10 si vous utilisez le protocole d'affichage RDP et de 4 si vous utilisez PCoIP.
- Si vous utilisez le protocole d'affichage Microsoft RDP, Microsoft Remote Desktop Connection (RDC) 6.0 ou supérieur doit être installé sur le poste de travail View.
- Si vous utilisez un poste de travail View en mode local, aucun protocole d'affichage à distance n'est utilisé. Vous pouvez utiliser plusieurs écrans en mode étendu.

Gestion de pools de postes de travail depuis un emplacement central 3

Vous pouvez créer des pools qui comprennent un ou des centaines de postes de travail virtuels. Comme source de postes de travail, vous pouvez utiliser des machines virtuelles, des machines physiques et des serveurs Windows Terminal Services. Créez une machine virtuelle comme image de base et VMware View peut générer un pool de postes de travail virtuels depuis cette image. Vous pouvez facilement installer ou diffuser des applications sur des pools avec VMware ThinApp.

Ce chapitre aborde les rubriques suivantes :

Avantages des pools de postes de travail

VMware 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 virtuels à partir de l'une des sources suivantes :

- Un système physique comme un PC de poste de travail physique ou un serveur Windows Terminal Services
- Une machine virtuelle hébergée sur un serveur ESX et gérée par vCenter Server
- Une machine virtuelle qui s'exécute sur VMware Server ou une autre plate-forme de virtualisation 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. Définir ces paramètres assure que vous possédez toujours assez de postes de travail View disponibles pour une utilisation immédiate mais pas trop pour ne pas abuser des ressources disponibles.

Utiliser des pools pour gérer des postes de travail vous permet d'appliquer des paramètres ou de déployer des applications sur tous les postes de travail virtuels 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 View et si vous autorisez les utilisateurs finaux à remplacer les valeurs par défaut.
- Configurez la qualité d'affichage et la limitation de la bande passante des animations Adobe Flash.

- 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.
- Si vous utilisez vSphere 4.1, 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.
- Spécifiez si le poste de travail View peut ou doit être téléchargé et exécuté sur un système client local.

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

Pools d'affectation dédiée

Un poste de travail View particulier est attribué à chaque utilisateur. Les utilisateurs reviennent au même poste de travail virtuel 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 virtuel 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 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 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.

Réduction et gestion des exigences de stockage

L'utilisation de postes de travail virtuels gérés par vCenter Server fournit toutes les exigences de stockage qui n'étaient auparavant disponibles que pour les serveurs virtualisés. L'utilisation de View Composer accroît les économies de stockage car tous les postes de travail dans un pool partagent un disque virtuel avec une image de base.

- Gestion du stockage avec vSphere page 26

  VMware 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.
- Réduction des exigences de stockage avec View Composer page 27

  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 %.

Gestion du stockage avec vSphere

VMware 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 VMware vSphere pour satisfaire différents besoins de stockage de datacenter. 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.

Avec View 4.5 et vSphere 4.1, vous pouvez désormais utiliser les fonctions suivantes :

- L'approvisionnement fin de vStorage, 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 le serveur ESX pour les fichiers d'échange de la machine virtuelle dans le système d'exploitation client

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 512 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.

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 fonction de rééquilibrage pour déplacer le réplica et les clones liés d'un LUN à un autre.

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.

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. Lorsque la machine virtuelle est désactivée, View Manager supprime le disque supprimable. 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.

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.

Pour plus d'informations, consultez le guide de meilleures pratiques intitulé *Storage Considerations for VMware View*.

Approvisionnement d'application

Avec VMware View, vous avez plusieurs options concernant l'approvisionnement d'application : Vous pouvez utiliser des techniques d'approvisionnement d'application traditionnelles, distribuer des packages d'applications créés avec VMware ThinApp ou déployer des applications dans le cadre d'une image de base de View Composer.

- Déploiement d'applications et de mises à jour système avec View Composer page 28

  Comme les pools de postes de travail de clone lié partagent une image de base, vous pouvez déployer des mises à jour et des correctifs rapidement en mettant à jour la machine virtuelle parente.

- Gestion d'applications VMware ThinApp dans View Administrator page 29

  VMware ThinApp™ vous permet de placer une application dans un seul fichier qui s'exécute dans un sandbox d'application virtualisée. Cette stratégie se traduit par un approvisionnement d'application flexible et sans conflit.

- Utilisation de processus existants pour l'approvisionnement d'application page 29

  Avec VMware View, vous pouvez toujours utiliser les techniques d'approvisionnement d'application que votre entreprise utilise actuellement. Deux considérations supplémentaires incluent la gestion de l'utilisation de CPU du serveur et de l'E/S de stockage et si les utilisateurs sont autorisés à installer des applications.

Déploiement d'applications et de mises à jour système avec View Composer

Comme les pools de postes de travail de clone lié partagent une image de base, vous pouvez déployer des mises à jour et des correctifs rapidement en mettant à jour la machine virtuelle parente.

La fonction de recomposition vous permet de faire des modifications à la machine virtuelle parente, de prendre un snapshot du nouvel état et de faire passer la nouvelle version de l'image à tous les (ou à un sous-ensemble de) utilisateurs et postes de travail. Vous pouvez utiliser cette fonction pour les tâches suivantes :

- L'application de correctifs et de mises à niveau du système d'exploitation et du logiciel
- L'application de Service Packs
- L'ajout d'applications
- L'ajout de périphériques virtuels
- La modification d'autres paramètres de machine virtuelle, comme la mémoire disponible

Vous pouvez créer un disque persistant View Composer qui contient des paramètres d'utilisateur et d'autres données générées par l'utilisateur. Ce disque persistant n'est pas affecté par une opération de recomposition. Lorsqu'un clone lié est supprimé, vous pouvez conserver les données utilisateur. Lorsqu'un employé quitte l'entreprise, un autre employé peut accéder aux données utilisateur de l'employé sur le départ. Un utilisateur avec plusieurs postes de travail peut consolider les données utilisateur sur un seul poste de travail.

Si vous voulez supprimer l'autorisation d'ajouter ou de supprimer un logiciel ou de modifier des paramètres aux utilisateurs, vous pouvez utiliser la fonction d'actualisation pour remettre le poste de travail à ses valeurs par défaut. Cette fonction réduit également la taille des clones liés, qui ont tendance à croître avec le temps.

Gestion d'applications VMware ThinApp dans View Administrator

VMware ThinApp™ vous permet de placer une application dans un seul fichier qui s'exécute dans un sandbox d'application virtualisée. Cette stratégie se traduit par un approvisionnement d'application flexible et sans conflit.

ThinApp fournit la virtualisation d'application en découplant une application du système d'exploitation sous-jacent et de ses bibliothèques et cadre et en groupant l'application dans un fichier exécutable appelé package d'application. Comme avec View 4.5, vous pouvez utiliser View Administrator pour distribuer des applications ThinApp à des postes de travail et des pools.

Après avoir créé une application virtualisée avec ThinApp, vous pouvez choisir de diffuser l'application à partir d'un serveur de fichiers partagés ou d'installer l'application sur les postes de travail virtuels. Si vous configurez l'application virtualisée pour la diffusion, vous devez remplir les considérations architecturales suivantes :

- Accès aux référentiels d'applications spécifiques (dans lesquels le package d'application est stocké) par des groupes d'utilisateurs spécifiques
- Configuration de stockage pour le référentiel d'application
- Trafic réseau généré par la diffusion, qui dépend largement du type d'application

Pour les applications diffusées, les utilisateurs lancent les applications en utilisant un raccourci du bureau.

Si vous affectez un package ThinApp pour qu'il soit installé sur un poste de travail virtuel, les considérations architecturales sont semblables à celles que vous remplissez lorsque vous utilisez l'approvisionnement logiciel MSI traditionnel. La configuration de stockage pour le référentiel d'applications est une considération à la fois pour les applications diffusées et pour les packages ThinApp installés dans des postes de travail virtuels.

Remarque L'affectation de packages d'application créés avec VMware ThinApp n'est pas prise en charge pour les postes de travail View téléchargés et utilisés en mode local.

Utilisation de processus existants pour l'approvisionnement d'application

Avec VMware View, vous pouvez toujours utiliser les techniques d'approvisionnement d'application que votre entreprise utilise actuellement. Deux considérations supplémentaires incluent la gestion de l'utilisation de CPU du serveur et de l'E/S de stockage et si les utilisateurs sont autorisés à installer des applications.

Si vous placez des applications sur un grand nombre de postes de travail virtuels au même moment, vous pouvez voir des pointes dans l'utilisation de CPU et l'E/S de stockage. Ces pics de charges de travail peuvent avoir des effets visibles sur les performances des postes de travail. Il est recommandé de planifier les mises à jour d'application au cours des heures creuses et d'échelonner les mises à jour sur les postes de travail si cela est possible. Vous devez également vérifier que votre solution de stockage est conçue pour prendre en charge de telles charges de travail.

Si votre entreprise autorise les utilisateurs à installer des applications, vous pouvez toujours utiliser vos stratégies actuelles, mais vous ne pouvez pas bénéficier des fonctions de View Composer, telles que l'actualisation et la recomposition du poste de travail. Avec View Composer, si une application n'est pas virtualisée ou incluse dans le profil ou les paramètres de données de l'utilisateur, cette application est ignorée lorsqu'une opération d'actualisation, de recomposition ou de rééquilibrage de View Composer se produit. Dans de nombreux cas, cette possibilité de contrôler quelles applications sont installées est un avantage. Les postes de travail View Composer sont facilement pris en charge car ils sont conservés avec une configuration connue.

Si des utilisateurs doivent absolument installer leurs propres applications et les faire durer sur la durée de vie du poste de travail virtuel, au lieu d'utiliser View Composer pour l'approvisionnement d'application, vous pouvez créer des postes de travail persistants et autoriser les utilisateurs à installer des applications.

Utilisation de GPO Active Directory pour gérer des utilisateurs et des postes de travail

VMware View comporte de nombreux modèles d'administration de stratégie de groupe pour centraliser la gestion et la configuration de composants et de postes de travail View.

Après l'importation de ces modèles dans Active Directory, vous pouvez les utiliser pour définir des stratégies qui s'appliquent aux groupes et composants suivants :

- Tous les systèmes quels que soient les utilisateurs ouvrant une session
- Tous les utilisateurs quel que soit le système sur lequel ils ouvrent une session
- La configuration de View Connection Server
- La configuration de View Client
- La configuration de View Agent

Une fois le GPO appliqué, les propriétés sont stockées dans le Registre Windows local du composant spécifié.

Vous pouvez utiliser des GPO pour définir toutes les stratégies disponibles à partir de l'interface utilisateur de View Administrator. Vous pouvez également utiliser des GPO pour définir des stratégies non disponibles depuis l'interface utilisateur. Pour obtenir une liste complète des paramètres disponibles dans les modèles d'administration, consultez le *Guide de l'administrateur de VMware View*.

Recommandations sur la planification et les éléments de conception d'architecture

4

Une conception classique d'architecture de VMware View utilise une stratégie de bloc constitutif pour atteindre l'évolutivité. La définition de chaque bloc constitutif peut varier en fonction de la configuration matérielle, des versions logicielles de View et de vSphere utilisées et d'autres facteurs de conception spécifique de l'environnement.

Ce chapitre décrit un exemple validé de bloc constitutif composé de composants prenant en charge jusqu'à 2 000 postes de travail virtuels à l'aide de vSphere 4.1. Le déploiement global intègre 5 de ces blocs constitutifs pour un total de 10 000 postes de travail virtuels dans ce qu'on appelle un « groupe ».

Cette architecture fournit une conception évolutive standard que vous pouvez adapter à l'environnement de votre entreprise et à des exigences spéciales. Ce chapitre inclut des détails clés sur les exigences concernant la mémoire, la CPU, la capacité de stockage, les composants réseau et le matériel pour permettre aux architectes et aux planificateurs informatiques de comprendre les éléments impliqués dans le déploiement d'une solution VMware View.

Ce chapitre aborde les rubriques suivantes :

Exigences de machine virtuelle

Lorsque vous programmez les spécifications de postes de travail View, les choix que vous faites concernant la RAM, la CPU et l'espace disque ont un effet significatif sur vos choix concernant le matériel serveur et de stockage et les dépenses.

- Planification en fonction des types de travailleurs page 32

  Pour de nombreux éléments de configuration, y compris la RAM, la CPU et le dimensionnement du stockage, les exigences dépendent en grande partie du type de travailleur qui utilise le poste de travail virtuel et des applications qui doivent être installées.

- Estimation des exigences de mémoire pour les postes de travail virtuels page 33

  La RAM a un coût plus élevé pour les serveurs que pour les ordinateurs. Comme le coût de RAM représente un pourcentage important du coût total du matériel de serveur et de la capacité totale de stockage nécessaire, il est essentiel de déterminer la bonne allocation de mémoire pour planifier le déploiement de poste de travail.

- Estimation des exigences de CPU pour les postes de travail virtuels page 35

  Lorsque vous estimez la CPU, vous devez rassembler des informations sur l'utilisation de la CPU moyenne pour divers types de travailleurs dans votre entreprise. De plus, calculez que 10 à 25 % de la puissance de traitement sont nécessaires pour la charge de virtualisation et les périodes de pic d'utilisation.

- Choisir la taille de disque système appropriée page 36

  Lors de l'allocation d'espace disque, ne fournissez que l'espace suffisant pour le système d'exploitation, les applications et le contenu supplémentaire que les utilisateurs peuvent installer ou générer. Habituellement, cette quantité est inférieure à la taille du disque inclus sur un ordinateur physique.

Planification en fonction des types de travailleurs

Pour de nombreux éléments de configuration, y compris la RAM, la CPU et le dimensionnement du stockage, les exigences dépendent en grande partie du type de travailleur qui utilise le poste de travail virtuel et des applications qui doivent être installées.

Pour la planification de l'architecture, les travailleurs peuvent être classés en plusieurs types.

Travailleurs	Les travailleurs et les travailleurs administratifs effectuent des tâches répétitives dans un petit nombre d'applications, habituellement sur un ordinateur stationnaire. Les applications ne sont généralement pas gourmandes en mémoire et en CPU comme celles utilisées par les travailleurs du savoir. Les travailleurs qui ont des horaires spécifiques peuvent tous ouvrir une session sur leurs postes de travail virtuels en même temps. Les travailleurs comprennent les analystes de centre d'appels, les employés du détail, les employés d'entrepôt, etc.
Travailleurs du savoir	Les tâches quotidiennes des travailleurs du savoir incluent l'accès à Internet, l'utilisation d'e-mails et la création de documents complexes, de présentations et de feuilles de calcul. Les travailleurs du savoir comprennent les comptables, les directeurs commerciaux, les analystes en recherche marketing, etc.
Utilisateurs expérimentés	Les utilisateurs expérimentés comprennent les développeurs d'application et les personnes qui utilisent des applications gourmandes en fonction graphique.

Employés qui utilisent des postes de travail uniquement en mode local	Ces utilisateurs téléchargent et exécutent leurs postes de travail View uniquement sur leurs systèmes locaux, ce qui réduit les coûts de datacenter associés à la bande passante, à la mémoire et aux ressources de CPU. Les réplications programmées assurent la sauvegarde des systèmes et des données. Les administrateurs configurent la fréquence à laquelle les systèmes des utilisateurs finaux doivent contacter View Manager pour éviter d'être verrouillés.
Utilisateurs de kiosque	Ces utilisateurs doivent partager un poste de travail qui est placé dans un lieu public. Parmi les utilisateurs de kiosque, on trouve des étudiants utilisant un ordinateur partagé dans une salle de classe, des infirmières dans un poste de garde et des ordinateurs utilisés pour la recherche d'emploi et le recrutement. Ces postes de travail requièrent une ouverture de session automatique. L'authentification peut être effectuée via certaines applications si nécessaire.

Estimation des exigences de mémoire pour les postes de travail virtuels

La RAM a un coût plus élevé pour les serveurs que pour les ordinateurs. Comme le coût de RAM représente un pourcentage important du coût total du matériel de serveur et de la capacité totale de stockage nécessaire, il est essentiel de déterminer la bonne allocation de mémoire pour planifier le déploiement de poste de travail.

Si l'allocation de RAM est trop faible, l'E/S de stockage peut être affectée négativement car il se produit trop d'échange de mémoire. Si l'allocation de RAM est trop élevée, la capacité de stockage peut être affectée négativement car le fichier de pagination dans le système d'exploitation client et les fichiers d'échange et de suspension de chaque machine virtuelle deviennent trop volumineux.

Remarque Cette rubrique résout des problèmes liés à l'allocation de mémoire pour accéder à distance à des postes de travail View. Si des utilisateurs exécutent des postes de travail View en mode local, sur leurs systèmes client, la quantité de mémoire utilisée représente une partie de la mémoire disponible sur le périphérique client.

Impact du dimensionnement de la RAM sur les performances

Lors de l'allocation de RAM, évitez de choisir un paramètre trop conservateur. Prenez en compte les considérations suivantes :

- Des allocations de RAM insuffisantes peuvent provoquer un échange de client excessif, qui peut générer une E/S causant des dégradations importantes des performances et augmentant la charge d'E/S de stockage.
- VMware ESX prend en charge des algorithmes de gestion de ressource de mémoire sophistiqués comme le partage transparent de mémoire et le gonflage de mémoire, qui peuvent réduire significativement la RAM physique nécessaire pour prendre en charge une allocation de RAM client donnée. Par exemple, même si 2 Go peuvent être alloués à un poste de travail virtuel, seule une fraction de ce nombre est consommée dans la RAM physique.
- Comme les performances des postes de travail virtuels sont sensibles aux temps de réponse, sur le serveur ESX, définissez des valeurs non nulles pour les paramètres de réservation de RAM. Réserver un peu de RAM garantit que les postes de travail en veille mais utilisés ne sont jamais complètement délogés sur le disque. Cela peut également réduire l'espace de stockage consommé par les fichiers d'échange ESX. Cependant, des paramètres de réservation supérieurs affectent votre capacité de surcharger la mémoire sur un serveur ESX et peuvent affecter les opérations de maintenance de VMotion.

Impact du dimensionnement de la RAM sur le stockage

La quantité de RAM que vous allouez à une machine virtuelle est directement liée à la taille de certains fichiers utilisés par la machine virtuelle. Pour accéder aux fichiers de la liste suivante, utilisez le système d'exploitation client Windows pour localiser la page Windows et mettre des fichiers en veille prolongée, et utilisez le système de fichiers du serveur ESX pour localiser les fichiers d'échange et de suspension ESX.

Ficher d'échange de Windows
Par défaut, ce fichier est dimensionné à 150 % de la RAM du client. Situé par défaut dans `C:\pagefile.sys`, ce fichier provoque le stockage approvisionné finement car on y accède souvent. Sur des machines virtuelles de clone lié, le fichier d'échange et les fichiers temporaires peuvent être redirigés vers un disque virtuel séparé qui est supprimé lorsque les machines virtuelles sont désactivées. La redirection du fichier d'échange supprimable économise de l'espace de stockage en ralentissant la croissance des clones liés. Elle peut également améliorer les performances. Bien que vous puissiez ajuster la taille dans Windows, cela peut avoir un effet négatif sur les performances de l'application.

Fichier de mise en veille prolongée de Windows pour ordinateurs portables
Ce fichier peut égaler 100 % de la RAM du client. Vous pouvez supprimer ce fichier en toute sécurité car il n'est pas nécessaire dans les déploiements de View, même si vous utilisez View Client with Local Mode.

Ficher d'échange ESX
Ce fichier, qui comporte l'extension `.vswp`, est créé si vous réservez moins de 100 % de la RAM d'une machine virtuelle. La taille du fichier d'échange est égale à la partie non réservée de la RAM du client. Par exemple, si 50 % de la RAM du client sont réservés et que la RAM du client est de 2 Go, le fichier d'échange ESX est de 1 Go. Ce fichier peut être stocké sur le magasin de données local sur l'hôte ou le cluster ESX.

Fichier de suspension ESX
Ce fichier, qui comporte l'extension `.vmss`, est créé si vous définissez la règle de fermeture de session du pool de postes de travail pour que le poste de travail virtuel soit interrompu quand l'utilisateur ferme sa session. La taille de ce fichier est égale à la taille de la RAM du client.

Dimensionnement de la RAM pour des configurations d'écran spécifiques lors de l'utilisation de PCoIP

Si vous utilisez le protocole d'affichage VMware PCoIP, la quantité de RAM supplémentaire requise par l'hôte ESX dépend en partie du nombre d'écrans configurés pour les utilisateurs finaux et de la résolution de l'écran. Le Tableau 4-1 répertorie la quantité de RAM supplémentaire requise pour diverses configurations. Les quantités de mémoire répertoriées dans les colonnes complètent la quantité de mémoire requise pour d'autres fonctionnalités de PCoIP.

Tableau 4-1. Surcharge d'affichage de client PCoIP

Standard de résolution d'affichage	Largeur, en pixels	Hauteur, en pixels	Surcharge avec 1 écran	Surcharge avec 2 écrans	Surcharge avec 4 écrans
VGA	640	480	2,34 Mo	4, 69 Mo	9,38 Mo
SVGA	800	600	3,66 Mo	7,32 Mo	14,65 Mo
720 p	1 280	720	7,03 Mo	14,65 Mo	28,13 Mo
UXGA	1 600	1 200	14,65 Mo	29,30 Mo	58,59 Mo
1 080 p	1 920	1 080	15,82 Mo	31,64 Mo	63,28 Mo
WUXGA	1 920	1 200	17,58 Mo	35,16 Mo	70,31 Mo

Tableau 4-1. Surcharge d'affichage de client PCoIP (suite)

Standard de résolution d'affichage	Largeur, en pixels	Hauteur, en pixels	Surcharge avec 1 écran	Surcharge avec 2 écrans	Surcharge avec 4 écrans
QXGA	2 048	1 536	24 Mo	48 Mo	96 Mo
WQXGA	2 560	1 600	31,25 Mo	62,50 Mo	125 Mo

Lorsque vous prenez en considération ces exigences, notez que la configuration de machine virtuelle de RAM allouée ne change pas. Cela signifie que vous n'avez pas à allouer 1 Go de RAM pour des applications et 31 Mo pour des écrans 1 080 p double. Au lieu de cela, prenez en considération la RAM supplémentaire lorsque vous calculez la RAM physique totale requise pour chaque serveur ESX. Additionnez la RAM du système d'exploitation client et la RAM supplémentaire et multipliez par le nombre de machines virtuelles.

Dimensionnement de la RAM pour des charges de travail et des systèmes d'exploitation spécifiques

Comme la quantité de RAM requise peut largement varier, en fonction du type de travailleur, beaucoup d'entreprises mènent une phase pilote pour déterminer le bon paramètre pour divers pools de travailleurs dans leur entreprise.

Un bon point de départ est d'allouer 1 Go pour des postes de travail Windows XP et des postes de travail Windows Vista et Windows 7 32 bits et 2 Go pour des postes de travail Windows 7 64 bits. Au cours d'un pilotage, surveillez les performances et l'espace disque utilisé avec divers types de travailleurs et procédez à des réglages jusqu'à ce que vous trouviez le paramètre optimal pour chaque pool de travailleurs.

Estimation des exigences de CPU pour les postes de travail virtuels

Lorsque vous estimez la CPU, vous devez rassembler des informations sur l'utilisation de la CPU moyenne pour divers types de travailleurs dans votre entreprise. De plus, calculez que 10 à 25 % de la puissance de traitement sont nécessaires pour la charge de virtualisation et les périodes de pic d'utilisation.

Remarque Cette rubrique résout des problèmes liés aux exigences de CPU lors de l'accès à distance à des postes de travail View. Si des utilisateurs exécutent un poste de travail View en mode local sur leurs systèmes client, le poste de travail View utilise les CPU disponibles sur le périphérique client, jusqu'à 2 CPU.

Les exigences de CPU varient en fonction du type de travailleur. Au cours de votre phase de pilotage, utilisez un outil de contrôle des performances, comme Perfmon dans la machine virtuelle et ESX Top dans ESX, pour comprendre les niveaux d'utilisation de CPU moyen et maximum pour ces groupes de travailleurs. Utilisez également les recommandations suivantes :

- Les développeurs ou autres utilisations de la puissance avec des besoins en haute performance peuvent avoir des exigences de CPU beaucoup plus élevées que les travailleurs du savoir et les travailleurs. Les CPU virtuelles doubles sont recommandées pour les tâches nécessitant beaucoup de ressources système ou pour les postes de travail Windows 7 qui doivent lire des vidéos 720 p avec le protocole d'affichage PCoIP.
- Les CPU virtuelles simples sont en général recommandées pour d'autres cas.

Comme un grand nombre de machines virtuelles sont exécutées sur un serveur, la CPU peut subir des pics si des agents comme des agents antivirus recherchent tous des mises à jour en même temps. Déterminez les agents, et leur nombre, qui peuvent causer des problèmes de performance et adoptez une stratégie pour résoudre ces problèmes. Par exemple, les stratégies suivantes peuvent être utiles dans votre entreprise :

- Utilisez View Composer pour mettre à jour des images plutôt que de laisser des agents de gestion logicielle télécharger des mises à jour logicielles sur chaque poste de travail virtuel individuel.
- Programmez des mises à jour antivirus et logicielles pour qu'elles s'exécutent à des heures creuses, quand peu d'utilisateurs sont susceptibles d'ouvrir une session.
- Échelonnez ou randomisez les dates des mises à jour.

Comme approche de dimensionnement initial informelle, pour commencer, supposez que chaque machine virtuelle requiert 1/8 à 1/16 d'un cœur de CPU comme puissance de calcul minimale garantie. Prévoyez pour cela un pilotage qui utilise 8 à 16 machines virtuelles par cœur. Par exemple, si vous supposez 16 machines virtuelles par cœur et que vous possédez un serveur ESX quadricœur à 2 sockets, vous pouvez héberger 128 machines virtuelles sur le serveur au cours du pilotage. Contrôlez l'utilisation de CPU totale sur l'hôte au cours de cette période et vérifiez qu'elle dépasse rarement une marge de sécurité telle que 80 % pour laisser assez de hauteur aux pics.

Choisir la taille de disque système appropriée

Lors de l'allocation d'espace disque, ne fournissez que l'espace suffisant pour le système d'exploitation, les applications et le contenu supplémentaire que les utilisateurs peuvent installer ou générer. Habituellement, cette quantité est inférieure à la taille du disque inclus sur un ordinateur physique.

Comme l'espace disque du datacenter a un coût généralement plus élevé par gigaoctet que l'espace disque du poste de travail ou de l'ordinateur portable dans un déploiement de PC traditionnel, optimisez la taille d'image du système d'exploitation. Les suggestions suivantes peuvent aider à optimiser la taille d'image :

- Supprimez les fichiers inutiles. Par exemple, réduisez les quotas sur les fichiers Internet temporaires.
- Choisissez une taille de disque virtuel suffisante pour permettre une croissance future, mais qui n'est pas trop importante.
- Utilisez des partages de fichiers centralisés ou un disque persistant View Composer pour le contenu créé par les utilisateurs et les applications installées par les utilisateurs.

La quantité d'espace de stockage requis doit prendre en compte les fichiers suivants pour chaque poste de travail virtuel :

- Le fichier de suspension ESX équivaut à la quantité de RAM allouée à la machine virtuelle.
- Le fichier d'échange de Windows équivaut à 150 % de RAM.
- Les fichiers journaux utilisent environ 100 Mo pour chaque machine virtuelle.
- Le disque virtuel, ou fichier `.vmdk`, doit contenir le système d'exploitation, les applications, ainsi que les applications et les mises à jour logicielles futures. Le disque virtuel doit également contenir des données utilisateur locales et des applications installées par l'utilisateur si elles sont situées sur le poste de travail virtuel plutôt que sur les partages de fichiers.

  Si vous utilisez View Composer, les fichiers `.vmdk` croissent avec le temps, mais vous pouvez contrôler la croissance en programmant des opérations d'actualisation View Composer, en définissant une règle de surcharge de stockage pour des pools de postes de travail View et en redirigeant des fichiers d'échange et temporaires Windows sur un disque non persistant séparé.

Vous pouvez également ajouter 15 % de cette estimation pour vous assurer que les utilisateurs ont toujours suffisamment d'espace disque.

Nœud de VMware View ESX

Un nœud est un serveur VMware ESX qui héberge des postes de travail de machine virtuelle dans un déploiement de VMware View.

VMware View est plus rentable lorsque vous optimisez le taux de consolidation, qui est le nombre de postes de travail hébergés sur un serveur ESX. Bien que de nombreux facteurs affectent la sélection de serveur, si vous effectuez une optimisation uniquement pour le prix d'acquisition, vous devez d'abord trouver des configurations de serveur qui ont un équilibre approprié de puissance de traitement et de mémoire.

Il n'existe pas d'autres solutions pour mesurer les performances dans des scénarios réels, comme dans un pilotage, pour déterminer un taux de consolidation approprié pour votre environnement et votre configuration matérielle. Les taux de consolidation peuvent varier significativement, en fonction de modes d'utilisation et de facteurs environnementaux. Utilisez les conseils suivants :

- De façon générale, prenez en considération la capacité de calcul en termes de postes de travail virtuels par cœur de CPU. Avec ESX 4.1, vous pouvez avoir entre 8 et 16 postes de travail virtuels par cœur de CPU. Pour plus d'informations sur le calcul des exigences de CPU pour chaque machine virtuelle, reportez-vous à la section « Estimation des exigences de CPU pour les postes de travail virtuels », page 35.
- Pensez à la capacité de mémoire en termes de RAM de poste de travail virtuel, de RAM d'hôte et de taux de surcharge. Bien que vous puissiez avoir entre 8 et 16 postes de travail virtuels par cœur de CPU, si des postes de travail virtuels ont 1 Go ou plus de RAM, vous devez également faire attention aux exigences de RAM physique. Pour plus d'informations sur le calcul de la quantité de RAM requise par machine virtuelle, reportez-vous à la section « Estimation des exigences de mémoire pour les postes de travail virtuels », page 33.

  Notez également que les coûts de RAM physique ne sont pas linéaires et que, dans certaines situations, il peut être rentable d'acheter davantage de serveurs plus petits qui n'utilisent pas de puces DIMM coûteuses. Dans d'autres cas, la densité de rack, la connectivité de stockage, la gérabilité et d'autres considérations font de la réduction du nombre de serveurs dans un déploiement un meilleur choix.
- Enfin, prenez en considération des exigences de cluster et de basculement. Pour plus d'informations, reportez-vous à la section « Déterminer des exigences de haute disponibilité », page 46.

Pour plus d'informations sur les spécifications des hôtes ESX dans vSphere, consultez le document *VMware vSphere Configuration Maximums*.

Pools de postes de travail pour des types de travailleurs spécifiques

VMware View offre de nombreuses fonctions qui vous aident à conserver de l'espace de stockage et à réduire la quantité de puissance de traitement requise pour plusieurs exemples 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 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 ce qui permet de gérer l'image basée sur View Composer et d'avoir des coûts de stockage réduits. 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 requièrent 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 complètes. 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 meilleures 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 page 39

  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.

- Pools pour travailleurs du savoir et utilisateurs expérimentés page 39

  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.

- Pools pour utilisateurs mobiles page 40

  Ces utilisateurs peuvent emprunter un poste de travail View et l'exécuter localement sur leur ordinateur portable ou leur poste de travail sans connexion réseau.

- Pools pour utilisateurs de kiosque page 41

  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 View. Il peut toujours être demandé aux utilisateurs de fournir des informations d'identification d'authentification pour certaines applications.

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 dans 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, 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.

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 une affectation dédiée pour que chaque travailleur du savoir ou utilisateur expérimenté ouvre une session sur le même poste de travail à chaque fois.
- Utilisez l'approvisionnement fin de vStorage pour que chaque poste de travail n'utilise que l'espace de stockage dont le disque a besoin pour son fonctionnement initial.
- 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. Ces images de poste de travail sans état partagent la même image de base et utilisent moins d'espace de stockage que des machines virtuelles complètes.
- Si vous utilisez des postes de travail de clone lié View Composer, vous pouvez implémenter une solution de profil itinérant ou virtuel pour stocker des données utilisateur de façon centralisée ou vous pouvez configurer un disque persistant pour le poste de travail. Toutefois, gardez à l'esprit qu'une fois que vous avez actualisé ou recomposé un poste de travail, les données stockées de façon centralisée et le disque persistant sont conservés, mais le disque qui contient le système d'exploitation et les applications ne l'est pas.
- 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. Ces utilisateurs ont besoin d'images de poste de travail avec état.

Pools pour utilisateurs mobiles

Ces utilisateurs peuvent emprunter un poste de travail View et l'exécuter localement sur leur ordinateur portable ou leur poste de travail sans connexion réseau.

View Client with Local Mode offre des avantages à la fois pour les utilisateurs finaux et les administrateurs informatiques. Pour les administrateurs, le mode local permet d'étendre des règles de sécurité View sur des ordinateurs portables qui n'étaient pas gérés précédemment. Les administrateurs peuvent garder un contrôle strict sur les applications qui s'exécutent sur le poste de travail View. Ils peuvent aussi gérer de façon centralisée le poste de travail comme ils le font pour les postes de travail View à distance. Avec le mode local, tous les avantages de VMware View peuvent également s'étendre à des bureaux à distance ou des succursales qui ont des réseaux lents ou non fiables.

Pour les utilisateurs finaux, les avantages comprennent la flexibilité de continuer à utiliser leurs propres ordinateurs en ligne ou hors ligne. Le poste de travail View est automatiquement crypté et peut facilement être synchronisé avec une image dans le datacenter à des fins de récupération d'urgence.

Recommandations générales

Les utilisateurs du mode local peuvent avoir besoin d'accéder aux applications et données sur leur poste de travail depuis leur ordinateur portable lorsque aucune connexion réseau n'est disponible. De plus, ils peuvent avoir besoin que ces données soient régulièrement et automatiquement sauvegardées dans le datacenter en cas de perte, d'endommagement ou de vol de l'ordinateur portable. Pour fournir ces fonctions, vous pouvez utiliser les paramètres de pool suivants.

- Lors de la création d'une machine virtuelle sur laquelle sera basé le pool, configurez la quantité minimale de RAM et de CPU virtuelle requise par le système d'exploitation client. Les postes de travail qui s'exécutent en mode local ajustent la quantité de mémoire et de puissance de traitement qu'ils utilisent en fonction de la quantité disponible sur l'ordinateur client.
- 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 dédiée car les utilisateurs en mode local doivent ouvrir une session sur le même poste de travail à chaque fois.
- 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.
- Si vous souhaitez que le processus d'approvisionnement génère un ID de sécurité d'ordinateur local unique et un GUID pour chaque clone lié dans le pool, sélectionnez une spécification de personnalisation Sysprep lorsque vous créez le pool. Sysprep crée de nouveaux ID de sécurité et GUID au cours de l'approvisionnement initial et après des opérations de recomposition. Comme nous n'allez probablement pas recomposer des pools en mode local, les ID de sécurité et GUID ne sont pas susceptibles de changer.
- N'incluez dans le pool que les postes de travail prévus pour une utilisation en mode local. Les machines virtuelles en mode local peuvent être placées sur des magasins de données avec des exigences d'IOPS inférieures au stockage prévu pour prendre en charge un nombre important de postes de travail View distants.

Recommandations supplémentaires pour des dépenses minimales en capital

Vous pouvez réduire le nombre de serveurs ESX requis pour votre pool en mode local si vous augmentez le nombre de machines virtuelles par serveur ESX. Un serveur ESX 4.1 peut héberger jusqu'à 500 machines virtuelles si la plupart n'est pas activée simultanément, comme c'est fréquemment le cas pour des pools en mode local.

Utilisez les recommandations suivantes pour réduire la quantité de bande passante et d'opérations d'E/S requise par chaque machine virtuelle, et pour augmenter le nombre de machines virtuelles sur un serveur ESX.

- Définissez une règle de View obligeant les utilisateurs finaux à utiliser leurs postes de travail View en mode local uniquement. Avec ce paramètre, les machines virtuelles du datacenter restent verrouillées et désactivées.
- Définissez des règles de mode local empêchant les utilisateurs finaux d'initier des restaurations de poste de travail, des sauvegardes de données ou des restitutions dans le datacenter.
- Ne planifiez pas de sauvegardes automatiques.
- N'activez pas SSL pour l'approvisionnement ou le téléchargement de postes de travail en mode local.
- Si les performances de View Connection Server sont affectées par le nombre de postes de travail locaux, définissez un intervalle de pulsation inférieur. La pulsation indique à View Connection Server que le poste de travail local a une connexion réseau. L'intervalle par défaut est de cinq minutes.

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 View. Il peut toujours être demandé aux utilisateurs de fournir des informations d'identification d'authentification pour certaines applications.

Les postes de travail View 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 View Connection Server 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 *Guide de l'administrateur de VMware 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.
- 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 une liste complète des paramètres disponibles dans les modèles d'administration de stratégie de groupe, consultez le *Guide de l'administrateur de VMware View*.
- 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.

Configuration de machine virtuelle de poste de travail

Comme la quantité de RAM et de CPU et l'espace disque requis par les postes de travail virtuels dépendent du système d'exploitation client, des exemples de configuration séparée sont fournis pour les postes de travail Windows XP, Windows Vista et Windows 7.

Les exemples de paramètres des machines virtuelles, tels que la mémoire, le nombre de processeurs virtuels et l'espace disque, sont spécifiques de VMware View.

Les recommandations répertoriées dans le Tableau 4-2 s'appliquent aux postes de travail virtuels standard avec Windows XP exécutés en mode distant.

Tableau 4-2. Exemple de machine virtuelle de poste de travail pour Windows XP

Élément	Exemple
Système d'exploitation	Windows XP 32 bits (avec le dernier Service Pack)
RAM	1 Go (valeur basse de 512 Mo, valeur haute de 2 Go)
CPU virtuelle	1
Capacité de disque système	16 Go (valeur basse de 8 Go, valeur haute de 40 Go)
Capacité des données utilisateur (sous forme de disque persistant)	5 Go (point de départ)
Type d'adaptateur SCSI virtuel	LSI Logic (pas par défaut)
Adaptateur de réseau virtuel	Flexible (par défaut)

La quantité d'espace disque système requise dépend du nombre d'applications requises dans l'image de base. VMware a validé une configuration qui comprenait 8 Go d'espace disque. Les applications incluaient Microsoft Word, Excel, PowerPoint, Adobe Reader, Internet Explorer, McAfee Antivirus et PKZIP.

La quantité d'espace disque requise pour les données utilisateur dépend du rôle de l'utilisateur et des règles organisationnelles liées au stockage des données. Si vous utilisez View Composer, ces données sont conservées sur un disque persistant.

Les recommandations répertoriées dans le Tableau 4-3 s'appliquent aux postes de travail virtuels standard avec Windows Vista exécutés en mode distant.

Tableau 4-3. Exemple de machine virtuelle de poste de travail pour Windows Vista

Élément	Exemple
Système d'exploitation	Windows Vista 32 bits (avec le dernier Service Pack)
RAM	1 Go
CPU virtuelle	1
Capacité de disque système	20 Go (standard)
Capacité des données utilisateur (sous forme de disque persistant)	5 Go (point de départ)
Type d'adaptateur SCSI virtuel	LSI Logic (par défaut)
Adaptateur de réseau virtuel	E1000 (par défaut)

Les recommandations répertoriées dans le Tableau 4-4 s'appliquent aux postes de travail virtuels standard avec Windows 7 exécutés en mode distant.

Tableau 4-4. Exemple de machine virtuelle de poste de travail pour Windows 7, hébergé sur un serveur ESX 4.1

Élément	Exemple
Système d'exploitation	Windows 7 32 bits
RAM	1 Go
CPU virtuelle	1
Capacité de disque système	20 Go (un peu moins que la norme)
Capacité des données utilisateur (sous forme de disque persistant)	5 Go (point de départ)
Type d'adaptateur SCSI virtuel	LSI Logic SAS (par défaut)
Adaptateur de réseau virtuel	E1000 (par défaut)

Configuration de machines virtuelles vCenter et View Composer et nombre maximum de pool de postes de travail

Vous installez vCenter Server et View Composer sur la même machine virtuelle. Comme cette machine virtuelle est un serveur, elle requiert beaucoup plus de mémoire et de puissance de traitement qu'une machine virtuelle de poste de travail.

View Composer peut créer et approvisionner jusqu'à 512 postes de travail par pool. View Composer peut également effectuer une opération de recomposition sur un maximum de 512 postes de travail à la fois.

Bien que vous puissiez installer vCenter Server et View Composer sur une machine physique, cet exemple utilise une machine virtuelle avec les spécifications répertoriées dans le Tableau 4-5. Le serveur ESX qui héberge cette machine virtuelle peut faire partie d'un cluster VMware HA pour se protéger contre les échecs du serveur physique.

Cet exemple suppose que vous utilisez VMware View avec vSphere 4.1 et vCenter Server 4.1.

Tableau 4-5. Exemple de machine virtuelle vCenter Server et taille maximale de pool

Élément	Exemple
Système d'exploitation	Windows Server 2008 R2 Enterprise 64 bits
RAM	4 Go
CPU virtuelle	2
Capacité de disque système	40 Go
Type SCSI	LSI SAS Logic (par défaut pour Windows Server 2008)
Adaptateur réseau	E1000 (par défaut)
Taille de pool maximale de View Composer	512 postes de travail

IMPORTANT Placez la base de données à laquelle vCenter et View Composer se connectent sur une machine virtuelle séparée. Pour des conseils sur le dimensionnement de la base de données, consultez le document *vCenter Server 4.x Database Sizing Calculator for Microsoft SQL Server* à l'adresse http://www.vmware.com/support/vsphere4/doc/vsp_4x_db_calculator.xls.

Configuration de machine virtuelle et nombre maximum dans View Connection Server

Lorsque vous installez View Connection Server, l'interface utilisateur de View Administrator est également installée. Ce serveur requiert plus de mémoire et de ressources de traitement qu'une instance de vCenter Server.

Configuration de View Connection Server

Bien que vous puissiez installer View Connection Server sur une machine physique, cet exemple utilise une machine virtuelle avec les spécifications répertoriées dans le Tableau 4-6. Le serveur ESX qui héberge cette machine virtuelle peut faire partie d'un cluster VMware HA pour se protéger contre les échecs du serveur physique.

Tableau 4-6. Exemple de machine virtuelle de Connection Server

Élément	Exemple
Système d'exploitation	Windows Server 2008 R2 64 bits
RAM	10 Go
CPU virtuelle	4
Capacité de disque système	40 Go
Type SCSI	LSI SAS Logic (par défaut pour Windows Server 2008)
Adaptateur réseau	E1000 (par défaut)
1 carte réseau	1 Gigabit

Considérations sur la conception de cluster de View Connection Server

Vous pouvez déployer plusieurs instances de View Connection Server répliquées dans un groupe pour prendre en charge l'équilibrage de charge et la haute disponibilité. Des groupes d'instances répliquées sont conçus pour prendre en charge le clustering dans un environnement de datacenter unique connecté à un réseau LAN. VMware ne recommande pas l'utilisation d'un groupe d'instances de View Connection Server répliquées sur un réseau WAN à cause du trafic de communication nécessaire entre les instances groupées. Dans les cas où un déploiement de View doit étendre des datacenters, créez un déploiement de View séparé pour chaque datacenter.

Nombre de connexions maximum pour View Connection Server

Le Tableau 4-7 fournit des informations sur les limites testées concernant le nombre de connexions simultanées auquel un déploiement de VMware View peut s'adapter.

Cet exemple suppose que vous utilisez VMware View avec vSphere 4.1 et vCenter Server 4.1.

Tableau 4-7. Connexions de postes de travail View

Serveurs Connection Server par déploiement	Type de connexion	Nombre maximum de connexions simultanées
1 serveur Connection Server	Connexion directe, RDP ou PCoIP	2 000
7 serveurs Connection Server (5 + 2 de rechange)	Connexion directe, RDP ou PCoIP	10 000
3 serveurs Connection Server	Connexion par tunnel, RDP	2 000
1 serveur Connection Server	Accès unifié à des PC physiques	100
1 serveur Connection Server	Accès unifié à des serveurs Terminal Server	200

Les connexions par tunnel sont requises si vous utilisez des serveurs de sécurité pour les connexions RDP en dehors du réseau d'entreprise interne.

Configuration et stockage d'une machine virtuelle View Transfer Server

View Transfer Server est requis pour prendre en charge des postes de travail qui exécutent View Client with Local Mode (connu précédemment sous le nom Offline Desktop). Ce serveur requiert moins de mémoire que View Connection Server.

Configuration de View Transfer Server

Vous devez installer View Transfer Server sur une machine virtuelle plutôt que physique et la machine virtuelle doit être gérée par la même instance de vCenter Server que les postes de travail locaux qu'elle gérera. Le Tableau 4-8 répertorie les spécifications de machine virtuelle pour une instance de View Transfer Server.

Tableau 4-8. Exemple de machine virtuelle de View Transfer Server

Élément	Exemple
Système d'exploitation	Windows Server 2008 R2 64 bits
RAM	4 Go
CPU virtuelle	2
Capacité de disque système	20 Go
Type SCSI	LSI Logic (pas par défaut, qui est SAS)
Adaptateur réseau	E1000 (par défaut)
1 carte réseau	1 Gigabit

Exigences de stockage et de bande passante pour View Transfer Server

Plusieurs opérations utilisent View Transfer Server pour envoyer des données entre le poste de travail View dans vCenter Server et le poste de travail local correspondant sur le système client. Lorsqu'un utilisateur restitue ou emprunte un poste de travail, View Transfer Server transfère les fichiers entre le datacenter et le poste de travail local. View Transfer Server synchronise également des postes de travail locaux avec les postes de travail correspondants dans le datacenter en répliquant les modifications générées par l'utilisateur dans le datacenter.

Si vous utilisez des clones liés View Composer pour des postes de travail locaux, le disque dur sur lequel vous configurez le référentiel de Transfer Server doit avoir suffisamment d'espace pour stocker vos fichiers d'image statique. Les fichiers d'image sont des images de base de View Composer. Plus vos disques de stockage réseau sont rapides, meilleures sont les performances. Pour plus d'informations sur la façon de déterminer la taille des fichiers d'image de base, consultez le *Guide de l'administrateur de VMware View*.

Chaque instance de Transfer Server peut gérer 60 opérations de disque simultanées, mais la bande passante réseau sera sûrement saturée avec un nombre inférieur. VMware a testé 20 opérations de disque simultanées, par exemple 20 clients téléchargeant un poste de travail local simultanément, avec une connexion réseau de plus de 1 Go par seconde.

Clusters vSphere

Les déploiements de VMware View peuvent utiliser des clusters VMware HA pour se protéger contre les échecs du serveur physique. À cause des limites de View Composer, le cluster ne doit pas contenir plus de 8 serveurs, ou nœuds.

VMware vSphere et vCenter fournissent un ensemble complet de fonctions pour la gestion des clusters de serveurs qui hébergent des postes de travail View. La configuration de cluster est également importante car chaque pool de postes de travail View doit être associé à un pool de ressources vCenter. Par conséquent, le nombre maximum de postes de travail par pool est lié au nombre de serveurs et de machines virtuelles que vous prévoyez d'exécuter par cluster.

Dans les déploiements de VMware View très importants, les performances et la réactivité de vCenter peuvent être améliorées en ne plaçant qu'un objet de cluster par objet de datacenter, ce qui n'est pas le comportement par défaut. Par défaut, VMware vCenter crée de nouveaux clusters dans le même objet de datacenter.

Déterminer des exigences de haute disponibilité

VMware vSphere, par son efficacité et sa gestion des ressources, vous permet d'atteindre des niveaux exceptionnels de machines virtuelles par serveur. Mais atteindre une haute densité de machines virtuelles par serveur signifie que plus d'utilisateurs sont affectés si un serveur échoue.

Les exigences de haute disponibilité peuvent différer considérablement en fonction de l'objectif du pool de postes de travail. Par exemple, un pool (d'affectation flottante) d'image de poste de travail sans état peut avoir différentes exigences d'objectif de point de récupération (RPO) qu'un pool (d'affectation dédiée) d'image de poste de travail avec état. Pour un pool d'affectation flottante, une solution acceptable peut consister à faire ouvrir une session aux utilisateurs sur un poste de travail différent si le poste de travail qu'ils utilisent devient indisponible.

Dans les cas où les exigences de disponibilité sont élevées, il est impératif de bien configurer VMware HA. Si vous utilisez VMware HA et que vous prévoyez un nombre fixe de postes de travail par serveur, exécutez chaque serveur à une capacité réduite. Si un serveur échoue, la capacité de postes de travail par serveur n'est pas dépassée lorsque les postes de travail sont redémarrés sur un hôte différent.

Par exemple, dans un cluster à 8 hôtes, où chaque hôte est capable d'exécuter 128 postes de travail, et que le but est de tolérer un seul échec de serveur, assurez-vous que 128 * (8 - 1) = 896 postes de travail maximum sont exécutés sur ce cluster. Vous pouvez également utiliser VMware DRS (Distributed Resource Scheduler) pour équilibrer les postes de travail sur les 8 hôtes. Vous pouvez utiliser complètement la capacité de serveur supplémentaire sans laisser des ressources de secours rester inactives. De plus, DRS peut permettre de rééquilibrer le cluster après la restauration d'un serveur échoué.

Vous devez également vous assurer que le stockage est correctement configuré pour supporter la charge d'E/S qui résulte du redémarrage simultané de plusieurs machines virtuelles après l'échec d'un serveur. L'IOPS de stockage a le plus d'effet sur la rapidité de récupération des postes de travail après l'échec d'un serveur.

Exemple : Exemple de configuration de cluster

Les paramètres répertoriés dans le Tableau 4-9 sont spécifiques de VMware View. Pour plus d'informations sur les limites des clusters HA dans vSphere, consultez le document *VMware vSphere Configuration Maximums*.

Tableau 4-9. Exemple de cluster HA

Élément	Exemple
Nœuds (serveurs ESX)	8 (y compris 1 nœud de secours)
Type de cluster	DRS (Distributed Resource Scheduler)/HA
Composant de réseau	Réseau de cluster ESX 4.1 standard
Ports commutés	80

Les exigences de réseau dépendent du type de serveur, du nombre d'adaptateurs réseau et de la façon dont vMotion est configuré.

Blocs constitutifs de VMware View

Un bloc constitutif de 2 000 utilisateurs comprend des serveurs physiques, une infrastructure VMware vSphere, des serveurs VMware View, un stockage partagé et 2 000 postes de travail de machines virtuelles. Vous pouvez inclure jusqu'à cinq blocs constitutifs dans un groupe View.

Tableau 4-10. Exemple de bloc constitutif de View sur le réseau LAN

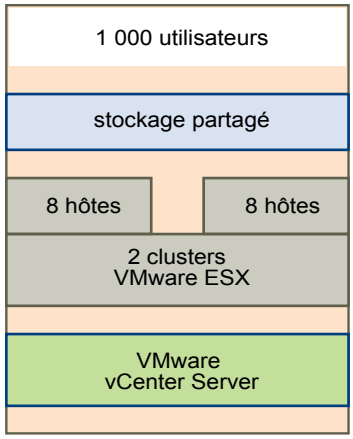
Élément	Exemple
Clusters vSphere	2 ou plus (avec 8 hôtes ESX maximum dans chaque cluster)
Commutateur de réseau à 80 ports	1
Système de stockage partagé	1
vCenter Server avec View Composer	1 (peut être exécuté dans le bloc lui-même)
Base de données	MS SQL Server ou serveur de base de données Oracle (peut être exécuté dans le bloc lui-même)
VLAN	3 (un réseau Ethernet 1 Gbit pour chaque réseau de gestion, réseau de stockage et réseau VMotion)

Avec vCenter 4.1, qui a une limite de 10 000 machines virtuelles par vCenter, vous pouvez utiliser des serveurs vCenter Server qui gèrent des postes de travail virtuels dans plusieurs blocs constitutifs. Lors de la rédaction de ce document, VMware n'avait pas encore validé une telle approche avec VMware View. Le test de vCenter Server 4.1 avec VMware View 4.5 était limité au test de 2 000 postes de travail virtuels avec un serveur vCenter Server.

Si vous ne possédez qu'un bloc constitutif dans un groupe, utilisez deux instances de View Connection Server pour la redondance.

La Figure 4-1 montre les composants d'un bloc constitutif de View.

Figure 4-1. Bloc constitutif de VMware View



Stockage partagé pour des blocs constitutifs de View

Les considérations sur la conception de stockage sont parmi les éléments les plus importants d'une architecture View réussie. La décision qui a le plus d'impact architectural est de choisir d'utiliser des postes de travail View Composer qui utilisent la technologie de clone lié.

Le système de stockage externe utilisé par VMware vSphere peut être un réseau SAN (Storage Area Network) Fibre Channel ou iSCSI, ou un réseau NAS (Network-Attached Storage) NFS (Network File System) ou CIFS (Common Internet File System). Les binaires ESX, les fichiers d'échange de machine virtuelle et les réplicas View Composer de machines virtuelles parentes sont stockés sur ce système.

D'un point de vue architectural, View Composer crée des images de poste de travail qui partagent une image de base pouvant réduire les exigences de stockage de 50 % ou plus. Vous pouvez réduire davantage les exigences de stockage en définissant une règle d'actualisation qui renvoie périodiquement le poste de travail à son état d'origine et libère l'espace utilisé pour suivre les modifications depuis la dernière actualisation.

Vous pouvez également réduire l'espace disque du système d'exploitation en utilisant des disques persistants de View Composer ou un serveur de fichiers partagés comme référentiel principal pour le profil et les documents de l'utilisateur. Comme View Composer vous permet de séparer des données utilisateur du système d'exploitation, vous pouvez voir que seul le disque persistant doit être sauvegardé ou répliqué, ce qui réduit davantage les exigences de stockage. Pour plus d'informations, reportez-vous à la section « Réduction des exigences de stockage avec View Composer », page 27.

Remarque Vous pouvez prendre la décision d'utiliser ou non un composant de stockage dédié séparé pour chaque bloc constitutif au cours d'une phase de pilotage. La considération principale est les E/S par seconde (IOPS). Vous pouvez mettre en place une stratégie de stockage étagé sur plusieurs blocs constitutifs pour optimiser les performances et réduire les coûts.

Pour plus d'informations, consultez le guide de meilleures pratiques intitulé *Storage Considerations for VMware View*.

Considérations de bande passante de stockage

Bien que de nombreux éléments soient importants pour concevoir un système de stockage prenant en charge un environnement VMware View, il est essentiel de prévoir la bonne bande passante de stockage pour la configuration de serveur. Vous devez également prendre en compte les effets du matériel de consolidation de port.

Occasionnellement, les environnements VMware View peuvent rencontrer des charges de tempête d'E/S, au cours desquelles toutes les machines virtuelles entreprennent une activité en même temps. Les tempêtes d'E/S peuvent être déclenchées par des agents client comme un antivirus ou des agents de mise à jour logicielle. Elles peuvent également être déclenchées par un comportement humain, comme lorsque tous les employés ouvrent une session à peu près au même moment le matin.

Vous pouvez réduire ces charges de travail de tempête par des meilleures pratiques opérationnelles, comme en déclenchant des mises à jour sur différentes machines virtuelles. Vous pouvez également tester différentes règles de fermeture de session au cours d'une phase pilote pour déterminer si l'interruption ou la mise hors tension des machines virtuelles lorsque des utilisateurs ferment leur session provoque une tempête d'E/S. En stockant des réplicas View Composer sur des magasins de données haute performance séparés, vous pouvez accélérer les opérations de lecture simultanées intensives pour faire face aux charges de tempête d'E/S.

En plus des meilleures pratiques, VMware vous recommande de fournir une bande passante de 1 Gbit/s pour 100 machines virtuelles, même si la bande passante moyenne doit être 10 fois inférieure à cela. Une telle planification conservatrice garantit une connectivité de stockage suffisante pour les pics de charges.

Considérations de bande passante réseau

Pour le trafic de l'affichage, de nombreux éléments peuvent affecter la bande passante réseau, comme le protocole utilisé, la résolution et la configuration de l'écran et la quantité de contenu multimédia dans la charge. Le lancement simultané d'applications diffusées peut également provoquer des pics d'utilisation.

Comme les effets de ces problèmes peuvent largement varier, beaucoup d'entreprises surveillent la consommation de bande passante dans le cadre d'un projet pilote. Comme point de départ pour un pilote, prévoyez entre 150 et 200 Kbit/s de capacité pour un travailleur du savoir classique.

Avec le protocole d'affichage PCoIP, si vous avez un réseau LAN d'entreprise avec 100 Mbits ou un réseau commuté de 1 Gbit, vos utilisateurs finaux peuvent espérer d'excellentes performances dans les conditions suivantes :

- Deux écrans (1 920 x 1 080)
- Utilisation renforcée d'applications Microsoft Office
- Utilisation renforcée de la navigation Web Flash
- Utilisation fréquente de multimédia avec une utilisation limitée du mode plein écran
- Utilisation fréquente de périphériques USB
- Impression sur le réseau

Ces informations sont extraites du guide d'information intitulé *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide*.

Prise en charge WAN et PCoIP

Pour les réseaux WAN (Wide-Area Network), vous devez prendre en compte les contraintes de bande passante et les problèmes de latence. Le protocole d'affichage PCoIP fourni par VMware s'adapte aux conditions variables de latence et de bande passante.

Si vous utilisez le protocole d'affichage RDP, vous devez avoir un produit d'optimisation WAN pour accélérer des applications pour des utilisateurs dans des succursales ou des petits bureaux. Avec PCoIP, de nombreuses techniques d'optimisation WAN sont créées avec le protocole de base.

- L'optimisation WAN est intéressante pour les protocoles TCP, tels que RDP, car ces protocoles requièrent plusieurs négociations entre client et serveur. La latence de ces négociations peut être assez élevée. L'usurpation des accélérateurs WAN répond aux négociations pour que la latence du réseau soit masquée pour le protocole. Comme PCoIP est basé sur UDP, cette forme d'accélération WAN n'est pas nécessaire.
- Les accélérateurs WAN compriment également le trafic réseau entre client et serveur, mais cette compression est généralement limitée à des taux de compression de 2:1. PCoIP peut fournir des taux de compression allant jusqu'à 100:1 pour les images et le son.

Les exemples suivants montrent comment PCoIP devrait fonctionner dans plusieurs scénarios WAN :

Travail au domicile

Un utilisateur avec une connexion câblée ou DSL dédiée avec un téléchargement de 4 à 8 Mo et moins de 300 ms de latence peut espérer d'excellentes performances dans les conditions suivantes :

- Deux écrans (1 920 x 1 080)
- Applications Microsoft Office
- Utilisation modérée de la navigation Web Flash
- Utilisation périodique de multimédia
- Impression modérée avec une imprimante USB connectée en local

Utilisateur mobile

Un utilisateur avec une connexion 3G dédiée avec un téléchargement de 5 à 500 Kbits et moins de 300 ms de latence peut espérer une bande passante adéquate et une latence tolérable dans les conditions suivantes :

- Un écran
- Applications Microsoft Office
- Utilisation modérée de la navigation Web Flash
- Impression modérée avec une imprimante USB connectée en local

Encouragez les utilisateurs mobiles à utiliser des applications locales pour accéder au contenu multimédia.

Succursale ou bureau à distance

Prévoyez 3 utilisateurs actifs simultanés pour 1 Mbit de bande passante. Les utilisateurs dans un bureau avec un VPN de site à site, basé sur UDP, de 20 Mbits et dédié avec moins de 200 ms de latence peuvent espérer des performances acceptables dans les conditions suivantes :

- Deux écrans (1 920 x 1 080)
- Applications Microsoft Office
- Utilisation modérée de la navigation Web Flash
- Impression modérée avec une imprimante USB connectée en local

Ces informations sont extraites du guide d'information intitulé *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide*.

Pour plus d'informations sur la configuration de VPN pour utiliser PCoIP, consultez les présentations de solutions suivantes, disponibles sur le site Web de VMware :

- *VMware View and Juniper Networks SA Servers SSL VPN Solution*
- *VMware View and F5 BIG-IP SSL VPN Solution*
- *VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution*

Groupe VMware View

Un groupe VMware View comporte cinq blocs constitutifs de 2 000 utilisateurs dans une installation View Manager que vous pouvez gérer comme une entité.

Un groupe est une unité d'organisation déterminée par des limites d'évolutivité de VMware View. Le Tableau 4-11 répertorie les composants d'un groupe View.

Tableau 4-11. Exemple de groupe VMware View

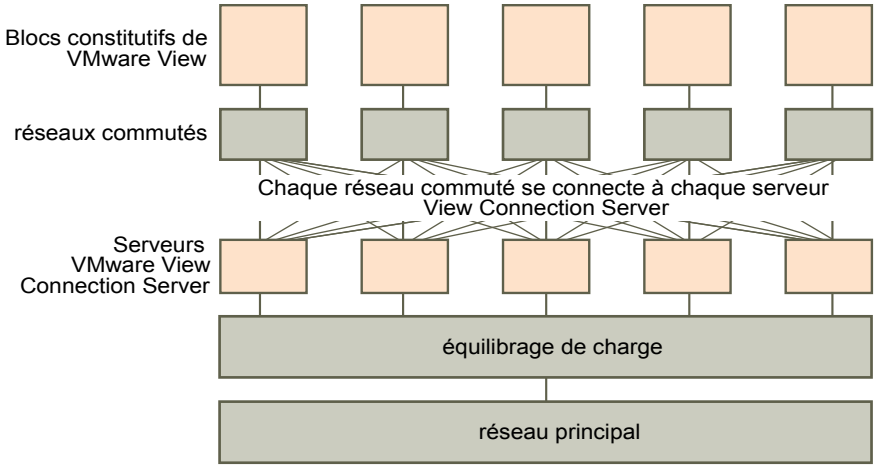
Élément	Nombre
Blocs constitutifs de View	5
View Connection Server	7 (1 pour chaque bloc constitutif et 2 de rechange)
Module Ethernet 10 Gb	1
Commutateur de réseau modulaire	1
Module d'équilibrage de charge	1
VPN pour WAN	1 (facultatif)

La charge de cœur de réseau équilibre des demandes entrantes dans les instances de View Connection Server. La prise en charge d'un mécanisme de redondance et de basculement, habituellement au niveau du réseau, évite que l'équilibreur de charge ne devienne un point de défaillance. Par exemple, le protocole VRRP (Virtual Router Redundancy Protocol) communique avec l'équilibreur de charge pour ajouter des capacités de redondance et de basculement.

Si une instance de View Connection Server échoue ou ne répond pas au cours d'une session active, les utilisateurs ne perdent pas de données. Les états de poste de travail sont préservés dans le poste de travail de machine virtuelle pour que les utilisateurs puissent se connecter à une instance de View Connection Server différente et leur session de poste de travail reprend à l'endroit où elle était lors de l'échec.

La Figure 4-2 indique comment tous les composants peuvent être intégrés dans une entité gérable.

Figure 4-2. Graphique de groupe pour 10 000 postes de travail View



Planification des fonctions de sécurité 5

VMware View offre une sécurité réseau renforcée pour protéger les données d'entreprise sensibles. Pour plus de sécurité, vous pouvez intégrer VMware View avec certaines solutions d'authentification utilisateur tierces, utiliser un serveur de sécurité et mettre en place la fonction d'autorisations limitées.

Ce chapitre aborde les rubriques suivantes :

Comprendre les connexions client

View Client et View Administrator communiquent avec un hôte View Connection Server sur des connexions sécurisées HTTPS.

La connexion View Client initiale, utilisée pour l'authentification utilisateur et la sélection de poste de travail View, est créée lorsqu'un utilisateur fournit une adresse IP à View Client. La connexion View Administrator est créée lorsqu'un administrateur saisit l'URL de View Administrator dans un navigateur Web.

Un certificat SSL de serveur par défaut est généré au cours de l'installation de View Connection Server. Par défaut, les clients sont présentés avec ce certificat lorsqu'ils visitent une page sécurisée telle que View Administrator.

Vous pouvez utiliser le certificat par défaut pour le test, mais il vous est recommandé de le remplacer par votre propre certificat dès que possible. Le certificat par défaut n'est pas signé par une autorité de certification commerciale. L'utilisation de certificats non certifiés peut permettre à des parties non approuvées d'intercepter le trafic en se faisant passer pour votre serveur.

- Connexions client par tunnel avec Microsoft RDP page 54

  Lorsque des utilisateurs se connectent à un poste de travail View avec le protocole d'affichage Microsoft RDP, View Client effectue une deuxième connexion HTTPS avec l'hôte View Connection Server. Cette connexion est appelée connexion par tunnel car elle fournit un tunnel pour le transport des données RDP.

- Connexions client directes avec PCoIP et HP RGS page 54

  Les administrateurs peuvent configurer des paramètres de View Connection Server pour que les sessions de postes de travail View soient établies directement entre le système client et la machine virtuelle de poste de travail View, en outrepassant l'hôte de View Connection Server. Ce type de connexion est appelé connexion client directe.

- Connexions client de View Client with Local Mode page 55

  View Client with Local Mode permet aux utilisateurs mobiles d'emprunter des postes de travail View sur leur ordinateur local.

Connexions client par tunnel avec Microsoft RDP

Lorsque des utilisateurs se connectent à un poste de travail View avec le protocole d'affichage Microsoft RDP, View Client effectue une deuxième connexion HTTPS avec l'hôte View Connection Server. Cette connexion est appelée connexion par tunnel car elle fournit un tunnel pour le transport des données RDP.

La connexion par tunnel offre les avantages suivants :

- Les données RDP sont transportées par tunnel via HTTPS et sont cryptées avec SSL. Ce protocole de sécurité puissant est cohérent avec la sécurité fournie par d'autres sites Web sécurisés, comme celles utilisées pour les banques et les paiements par carte de crédit en ligne.
- Un client peut accéder à plusieurs postes de travail sur une seule connexion HTTPS, ce qui réduit la surcharge totale du protocole.
- Comme VMware View gère la connexion HTTPS, la fiabilité des protocoles sous-jacents est considérablement améliorée. Si un utilisateur perd temporairement une connexion réseau, la connexion HTTP est de nouveau établie après la restauration de la connexion réseau et la connexion RDP reprend automatiquement sans que l'utilisateur n'ait à se reconnecter et à rouvrir une session.

Dans un déploiement standard d'instances de View Connection Server, la connexion sécurisée HTTPS se termine sur View Connection Server. Dans le déploiement d'une zone DMZ, la connexion sécurisée HTTPS se termine sur un serveur de sécurité. Pour plus d'informations sur les déploiements de zone DMZ et les serveurs de sécurité, reportez-vous à la section « Préparation pour l'utilisation d'un serveur de sécurité », page 60.

Les clients qui utilisent les protocoles d'affichage PCoIP ou HP RGS n'utilisent pas la connexion par tunnel.

Connexions client directes avec PCoIP et HP RGS

Les administrateurs peuvent configurer des paramètres de View Connection Server pour que les sessions de postes de travail View soient établies directement entre le système client et la machine virtuelle de poste de travail View, en outrepassant l'hôte de View Connection Server. Ce type de connexion est appelé connexion client directe.

Avec des connexions client directes, une connexion HTTPS est toujours établie entre le client et l'hôte de View Connection Server pour que les utilisateurs authentifient et sélectionnent des postes de travail View, mais la deuxième connexion HTTPS (la connexion tunnel) n'est pas utilisée.

Les clients qui utilisent les protocoles d'affichage PCoIP ou HP RGS utilisent des connexions client directes. Ils ne peuvent pas utiliser la connexion par tunnel.

Les connexions PCoIP comportent les fonctions de sécurité intégrées suivantes :

- PCoIP prend en charge le cryptage AES (Advanced Encryption Standard) qui est activé par défaut.
- L'implémentation matérielle de PCoIP utilise AES et IPsec (IP Security).
- PCoIP fonctionne avec des clients VPN tiers.

Pour les clients qui utilisent le protocole d'affichage Microsoft RDP, les connexions client directes ne sont appropriées que si votre déploiement se trouve sur un réseau d'entreprise. Avec des connexions client directes, le trafic RDP est envoyé non crypté sur la connexion entre le client et la machine virtuelle de poste de travail View.

Connexions client de View Client with Local Mode

View Client with Local Mode permet aux utilisateurs mobiles d'emprunter des postes de travail View sur leur ordinateur local.

View Client with Local Mode prend en charge les communications par tunnel et hors tunnel pour les transferts de données sur réseau LAN. Avec les communications par tunnel, tout le trafic est routé via l'hôte de View Connection Server et vous pouvez spécifier de crypter les communications et les transferts de données. Avec les communications hors tunnel, les données non cryptées sont transférées directement entre le poste de travail local sur le système client et la machine virtuelle de poste de travail View dans vCenter Server.

Les données locales sont toujours cryptées sur l'ordinateur de l'utilisateur, même si vous configurez des communications par tunnel ou hors tunnel.

Choisir une méthode d'authentification utilisateur

VMware View utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs. Pour plus de sécurité, vous pouvez intégrer VMware View avec les solutions d'authentification RSA SecurID et par carte à puce.

- Authentification Active Directory page 55

  Chaque instance de View Connection Server est associée à un domaine Active Directory et les utilisateurs sont authentifiés par Active Directory pour le domaine associé. Les utilisateurs sont également authentifiés par des domaines d'utilisateur supplémentaires avec lesquels un accord d'approbation existe.

- Authentification RSA SecurID page 56

  RSA SecurID fournit une sécurité améliorée avec une authentification à deux facteurs, ce qui requiert de connaître le code PIN et le code de jeton de l'utilisateur. Le code de jeton n'est disponible que sur le jeton SecurID physique.

- Authentification par carte à puce page 56

  Une carte à puce est une petite carte en plastique dans laquelle se trouve une puce d'ordinateur. La plupart des agences gouvernementales et des grandes entreprises utilisent des cartes à puce pour authentifier des utilisateurs qui accèdent à leurs réseaux d'ordinateur. Une carte à puce fait également référence à une CAC (Common Access Card).

- Fonction Se connecter en tant qu'utilisateur actuel page 57

  Lorsque les utilisateurs de View Client cochent la case **[Se connecter en tant qu'utilisateur actuel]** , les informations d'identification qu'ils ont fournies lors de l'ouverture de session sur le système client sont utilisées pour les authentifier sur l'instance de View Connection Server et sur le poste de travail View. Aucune autre authentification utilisateur n'est requise.

Authentification Active Directory

Chaque instance de View Connection Server est associée à un domaine Active Directory et les utilisateurs sont authentifiés par Active Directory pour le domaine associé. Les utilisateurs sont également authentifiés par des domaines d'utilisateur supplémentaires avec lesquels un accord d'approbation existe.

Par exemple, si une instance de View Connection Server est membre du Domaine A et qu'un accord d'approbation existe entre le Domaine A et le Domaine B, les utilisateurs du Domaine A et du Domaine B peuvent se connecter à une instance de View Connection Server avec View Client.

De la même façon, si un accord d'approbation existe entre le Domaine A et un domaine MIT Kerberos dans un environnement de domaine mixte, des utilisateurs du domaine Kerberos peuvent sélectionner le nom du domaine Kerberos lorsqu'ils se connectent à l'instance de View Connection Server avec View Client.

View Connection Server détermine les domaines qui sont accessibles en traversant des relations d'approbation, en commençant par le domaine dans lequel réside l'hôte. Pour un petit ensemble de domaines bien connectés, View Connection Server peut déterminer rapidement une liste complète de domaines, mais le temps que cela prend augmente car le nombre de domaines accroît ou car la connectivité entre les domaines diminuent. La liste peut également inclure des domaines que vous ne souhaitez pas proposer aux utilisateurs lorsqu'ils ouvrent une session sur leurs postes de travail.

Les administrateurs peuvent utiliser l'interface de ligne de commande `vdmadmin` pour configurer le filtrage de domaines, qui limite les domaines qu'une instance de View Connection Server recherche et qu'elle affiche aux utilisateurs Pour plus d'informations, consultez le *Guide de l'administrateur de VMware View*.

Les règles, telles que la restriction des heures autorisées pour ouvrir une session et la définition de la date d'expiration des mots de passe, sont également gérées par des procédures opérationnelles Active Directory existantes.

Authentification RSA SecurID

RSA SecurID fournit une sécurité améliorée avec une authentification à deux facteurs, ce qui requiert de connaître le code PIN et le code de jeton de l'utilisateur. Le code de jeton n'est disponible que sur le jeton SecurID physique.

Les administrateurs peuvent activer des instances de View Connection Server individuelles pour l'authentification RSA SecurID en installant le logiciel RSA SecurID sur l'hôte View Connection Server et en modifiant des paramètres View Connection Server.

Lorsque des utilisateurs ouvrent une session via une instance de View Connection Server qui est activée pour l'authentification RSA SecurID, ils doivent d'abord s'authentifier en fournissant leur nom d'utilisateur et leur code de passe RSA. S'ils ne sont pas authentifiés à ce niveau, l'accès est refusé. S'ils sont bien authentifiés avec RSA SecurID, ils continuent normalement et doivent ensuite saisir leurs informations d'identification Active Directory.

Si vous possédez plusieurs instances de View Connection Server, vous pouvez configurer l'authentification RSA SecurID sur certaines instances et configurer une méthode d'authentification utilisateur différente sur d'autres. Par exemple, vous pouvez configurer l'authentification RSA SecurID uniquement pour les utilisateurs qui accèdent à des postes de travail View à distance sur Internet.

VMware View est certifié par le programme RSA SecurID Ready et prend en charge l'ensemble des fonctionnalités SecurID, y compris New PIN Mode, Next Token Code Mode, RSA Authentication Manager et l'équilibrage de charge.

Authentification par carte à puce

Une carte à puce est une petite carte en plastique dans laquelle se trouve une puce d'ordinateur. La plupart des agences gouvernementales et des grandes entreprises utilisent des cartes à puce pour authentifier des utilisateurs qui accèdent à leurs réseaux d'ordinateur. Une carte à puce fait également référence à une CAC (Common Access Card).

L'authentification par carte à puce n'est prise en charge que par View Client pour Windows et View Client with Local Mode. Elle n'est pas prise en charge par View Administrator.

Les administrateurs peuvent activer des instances de View Connection Server individuelles pour l'authentification par carte à puce. L'activation d'une instance de View Connection Server pour utiliser l'authentification par carte à puce nécessite généralement l'ajout de votre certificat racine à un fichier du magasin d'approbations et la modification de paramètres de View Connection Server.

SSL doit être activé pour les connexions client qui utilisent l'authentification par carte à puce. Les administrateurs peuvent activer SSL pour les connexions client en définissant un paramètre global dans View Administrator.

Pour utiliser des cartes à puce, des machines client doivent comporter un intergiciel de carte à puce et un lecteur de carte à puce. Pour installer des certificats sur des cartes à puce, vous devez configurer un ordinateur afin qu'il agisse comme station d'inscription.

Pour utiliser des cartes à puce avec des postes de travail locaux, vous devez sélectionner une clé de 1 024 bits ou de 2 048 bits au cours de l'inscription de carte à puce. Des certificats avec des clés de 512 bits ne sont pas pris en charge pour les postes de travail locaux. Par défaut, View Connection Server utilise AES-128 pour crypter le fichier de disque virtuel lorsque des utilisateurs restituent et empruntent un poste de travail local. Vous pouvez modifier le cryptage de clé de chiffrement sur AES-192 ou AES-256.

Fonction Se connecter en tant qu'utilisateur actuel

Lorsque les utilisateurs de View Client cochent la case **[Se connecter en tant qu'utilisateur actuel]** , les informations d'identification qu'ils ont fournies lors de l'ouverture de session sur le système client sont utilisées pour les authentifier sur l'instance de View Connection Server et sur le poste de travail View. Aucune autre authentification utilisateur n'est requise.

Pour prendre en charge cette fonction, les informations d'identification d'utilisateur sont stockées sur l'instance de View Connection Server et sur le système client.

- Sur l'instance de View Connection Server, les informations d'identification d'utilisateur sont cryptées et stockées dans la session utilisateur avec le nom d'utilisateur, le domaine et l'UPN facultatif. Les informations d'identification sont ajoutées lors de l'authentification et supprimées lorsque l'objet de session est détruit. L'objet de session est détruit quand l'utilisateur ferme sa session, quand la session expire ou quand l'authentification échoue. L'objet de session réside dans la mémoire volatile et n'est pas stocké dans View LDAP ou dans un fichier de disque.
- Sur le système client, les informations d'identification d'utilisateur sont cryptées et stockées dans un tableau dans Authentication Package, qui est un composant de View Client. Les informations d'identification sont ajoutées au tableau quand l'utilisateur ouvre sa session et sont supprimées du tableau quand l'utilisateur ferme sa session. Le tableau réside dans une mémoire volatile.

Les administrateurs peuvent utiliser des paramètres de stratégie de groupe View Client pour contrôler la disponibilité de la case **[Se connecter en tant qu'utilisateur actuel]** et pour spécifier sa valeur par défaut. Les administrateurs peuvent également utiliser la stratégie de groupe pour spécifier quelles instances de View Connection Server acceptent l'identité et les informations d'identification de l'utilisateur qui sont transmises lorsque les utilisateurs cochent la case **[Se connecter en tant qu'utilisateur actuel]** dans View Client.

La fonction Se connecter en tant qu'utilisateur actuel a les limites et exigences suivantes :

- Si l'authentification par carte à puce est définie sur Requis sur une instance de View Connection Server, les utilisateurs de carte à puce qui cochent la case **[Se connecter en tant qu'utilisateur actuel]** doivent toujours se réauthentifier avec leur carte à puce et leur code PIN lors de l'ouverture de session sur le poste de travail View.
- Les utilisateurs ne peuvent pas emprunter un poste de travail pour une utilisation en mode local s'ils ont coché la case **[Se connecter en tant qu'utilisateur actuel]** lors de l'ouverture de leur session.
- L'heure sur le système sur lequel le client ouvre une session et l'heure sur l'hôte de View Connection Server doivent être synchronisées.
- Si les affectations de droits d'usage **[Accéder à cet ordinateur à partir du réseau]** sont modifiées sur le système client, elles doivent être modifiées comme décrit dans l'article 1025691 de la base de connaissances de VMware.

Restriction de l'accès aux postes de travail View

Vous pouvez utiliser la fonction d'autorisations limitées pour limiter l'accès aux postes de travail View en fonction de l'instance de View Connection Server à laquelle un utilisateur se connecte.

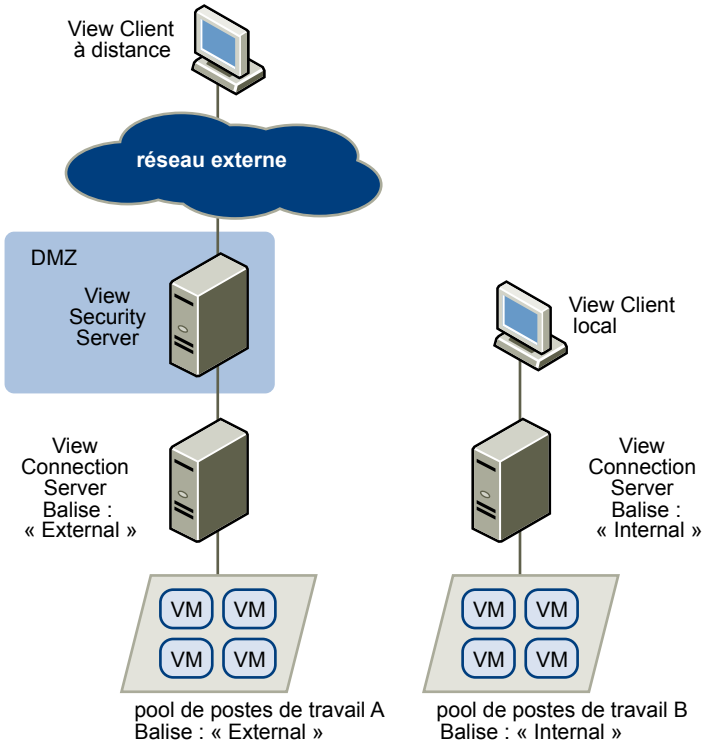
Avec des autorisations limitées, vous affectez une ou plusieurs balises à une instance de View Connection Server. Ensuite, lorsque vous configurez un pool de postes de travail, vous sélectionnez les balises des instances de View Connection Server que vous voulez rendre capables d'accéder au pool de postes de travail. Lorsque les utilisateurs ouvrent une session via une instance marquée de View Connection Server, 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.

Par exemple, votre déploiement de VMware View peut comporter deux instances de View Connection Server. 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 :

- Attribuez la balise « Internal » à l'instance de View Connection Server qui prend en charge les utilisateurs internes.
- Attribuez la balise « External » à l'instance de View Connection Server qui est couplée avec le serveur de sécurité et qui prend en charge les utilisateurs externes.
- Attribuez la balise « Internal » aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs internes.
- Attribuez 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 View Connection Server 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 View Connection Server marqué comme Internal. La Figure 5-1 illustre cette configuration.

Figure 5-1. Exemple d'autorisations limitées



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 de View Connection Server 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.

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 de View Connection Server particulière.

Utilisation de paramètres de stratégie de groupe pour sécuriser des postes de travail View

VMware View comporte des modèles d'administration de stratégie de groupe qui contiennent des paramètres de stratégie de groupe liés à la sécurité que vous pouvez utiliser pour sécuriser vos postes de travail View.

Par exemple, vous pouvez utiliser des paramètres de stratégie de groupe pour exécuter les tâches suivantes.

- Spécifier les instances de View Connection Server qui peuvent accepter l'identité et les informations d'identification d'utilisateur qui sont transmises quand un utilisateur coche la case **[Se connecter en tant qu'utilisateur actuel]** dans View Client.
- Activer l'authentification unique pour l'authentification par carte à puce dans View Client.
- Configurer la vérification de certificat SSL de serveur dans View Client.
- Empêcher les utilisateurs de fournir des informations d'identification avec des options de ligne de commande de View Client.

Pour plus d'informations sur l'utilisation des paramètres de stratégie de groupe de View Client, consultez le *Guide de l'administrateur de VMware View*.

Implémentation de meilleures pratiques pour sécuriser des systèmes client

Il vous est recommandé d'implémenter des meilleures pratiques pour sécuriser des systèmes client.

- Assurez-vous que les systèmes client sont configurés pour passer en veille après une période d'inactivité et que les utilisateurs doivent saisir un mot de passe avant de réveiller l'ordinateur.
- Les utilisateurs doivent saisir un nom d'utilisateur et un mot de passe lors du démarrage des systèmes client. Ne configurez pas les systèmes client pour qu'ils autorisent les ouvertures de session automatiques.
- Pour les systèmes client Mac, pensez à définir différents mots de passe pour la chaîne de clé et le compte d'utilisateur. Lorsque les mots de passe sont différents, les utilisateurs sont invités avant que le système n'entre des mots de passe en leur nom. Pensez également à activer la protection FileVault.
- Les systèmes client en mode local peuvent avoir plus d'accès au réseau lorsqu'ils sont exécutés en mode local que lorsqu'ils sont distants et connectés à l'intranet. Pensez à appliquer des stratégies de sécurité du réseau intranet pour les systèmes client en mode local ou désactivez l'accès au réseau pour les systèmes client en mode local lorsqu'ils sont exécutés en mode local.

Affectation de rôles d'administrateur

Une tâche de gestion clé dans un environnement VMware View consiste à déterminer qui peut utiliser View Administrator et les tâches que ces utilisateurs sont autorisés à effectuer.

L'autorisation d'effectuer des tâches dans View Administrator est déterminée par un système de contrôle d'accès composé de rôles et de privilèges d'administrateur. Un rôle est un ensemble de privilèges. Les privilèges accordent la possibilité d'effectuer des actions spécifiques, comme autoriser un utilisateur sur un pool de postes de travail ou modifier un paramètre de configuration. Les privilèges contrôlent également ce qu'un administrateur peut voir dans View Administrator.

Un administrateur peut créer des dossiers pour subdiviser des pools de postes de travail et déléguer l'administration de pools de postes de travail spécifiques à différents administrateurs dans View Administrator. Un administrateur configure un accès administrateur aux ressources dans un dossier en affectant un rôle à un utilisateur sur ce dossier. Les administrateurs ne peuvent accéder qu'aux ressources qui résident dans des dossiers pour lesquels ils ont affecté des rôles. Le rôle qu'un administrateur a sur un dossier détermine son niveau d'accès sur les ressources contenues dans ce dossier.

View Administrator comporte un ensemble de rôles prédéfinis. Les administrateurs peuvent également créer des rôles personnalisés en combinant des privilèges sélectionnés.

Préparation pour l'utilisation d'un serveur de sécurité

Un serveur de sécurité est une instance spéciale de View Connection Server qui exécute un sous-ensemble de fonctions de View Connection Server. Vous pouvez utiliser un serveur de sécurité pour fournir une couche supplémentaire de sécurité entre Internet et votre réseau interne.

Un serveur de sécurité réside dans une zone DMZ et agit comme un hôte proxy pour les connexions dans votre réseau approuvé. Chaque serveur de sécurité est couplé avec une instance de View Connection Server et transmet tout le trafic à cette instance. Cette conception fournit une couche supplémentaire de sécurité en protégeant l'instance de View Connection Server 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 de View Connection Server sur le réseau interne. Pour plus d'informations sur les ports spécifiques, reportez-vous à la section « Règles de pare-feu pour serveurs de sécurité basés sur une zone DMZ », page 64.

Comme les utilisateurs peuvent se connecter directement à n'importe quelle instance de View Connection Server à partir de leur réseau interne, vous n'avez pas à implémenter de serveur de sécurité dans un déploiement sur réseau LAN.

Remarque Les clients View qui utilisent PCoIP peuvent se connecter à des serveurs de sécurité View, mais les sessions PCoIP avec le poste de travail virtuel ignorent le serveur de sécurité. PCoIP utilise le protocole UDP (User Datagram Protocol) pour la diffusion audio et vidéo. Les serveurs de sécurité ne prennent en charge que TCP.

Pour plus d'informations sur la configuration de VPN pour utiliser PCoIP, consultez les présentations de solutions suivantes, disponibles sur le site Web de VMware :

- *VMware View and Juniper Networks SA Servers SSL VPN Solution*
- *VMware View and F5 BIG-IP SSL VPN Solution*
- *VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution*

Meilleures pratiques pour des déploiements de serveur de sécurité

Il vous est recommandé de suivre des règles de sécurité et des procédures de meilleure pratique lorsque vous utilisez un serveur de sécurité dans une zone DMZ.

Le livre blanc *DMZ Virtualization with VMware Infrastructure* comprend des exemples de meilleures pratiques pour une zone DMZ virtualisée. Plusieurs recommandations de ce livre blanc s'appliquent également à une zone DMZ physique.

Pour limiter la portée des émissions d'image, les instances de View Connection Server couplées avec des serveurs de sécurité doivent être déployées sur un réseau isolé. Cette topologie peut permettre d'empêcher un utilisateur malveillant sur le réseau interne de surveiller les communications entre les serveurs de sécurité et des instances de View Connection Server.

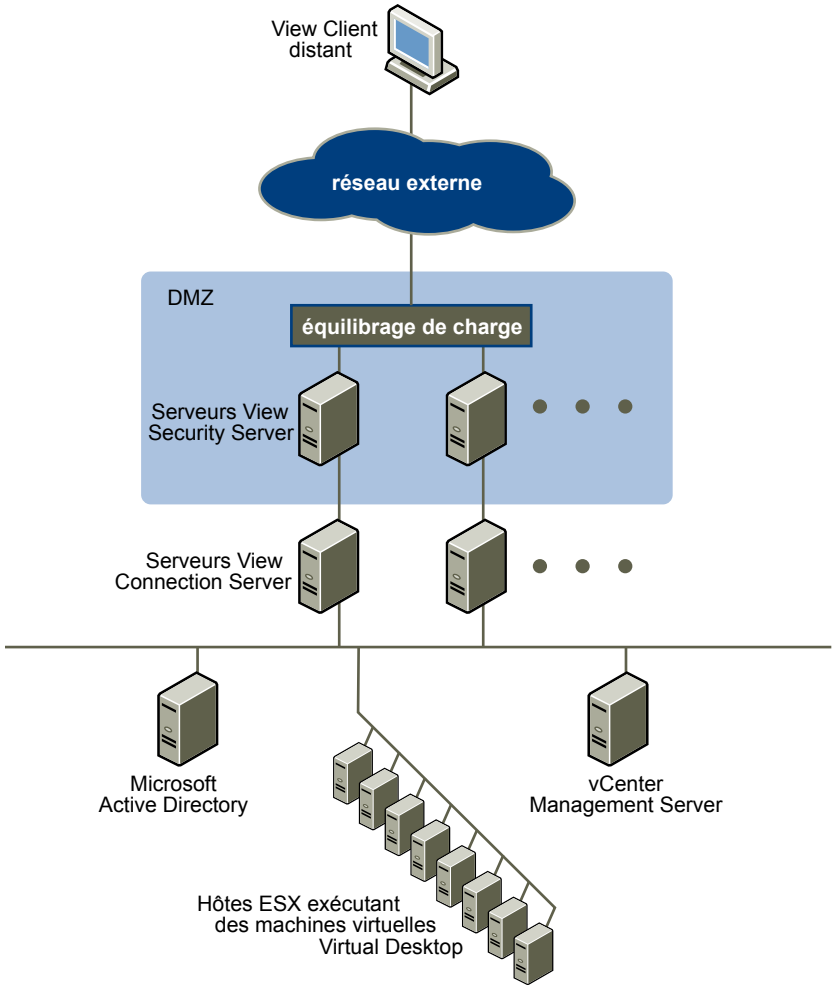
Vous pouvez également utiliser des fonctions de sécurité avancées sur votre commutateur de réseau pour empêcher le contrôle malintentionné de la communication entre un serveur de sécurité et View Connection Server et pour éviter les attaques de contrôle comme le ARP Cache Poisoning. Pour plus d'informations, consultez la documentation d'administration de votre équipement de réseau.

Topologies de serveur de sécurité

Vous pouvez implémenter plusieurs topologies de serveur de sécurité différentes.

La topologie illustrée dans la Figure 5-2 montre un environnement hautement disponible qui comprend deux serveurs de sécurité avec équilibrage de charge dans une zone DMZ. Les serveurs de sécurité communiquent avec deux instances de View Connection Server dans le réseau interne.

Figure 5-2. Serveurs de sécurité avec équilibrage de charge dans une zone DMZ

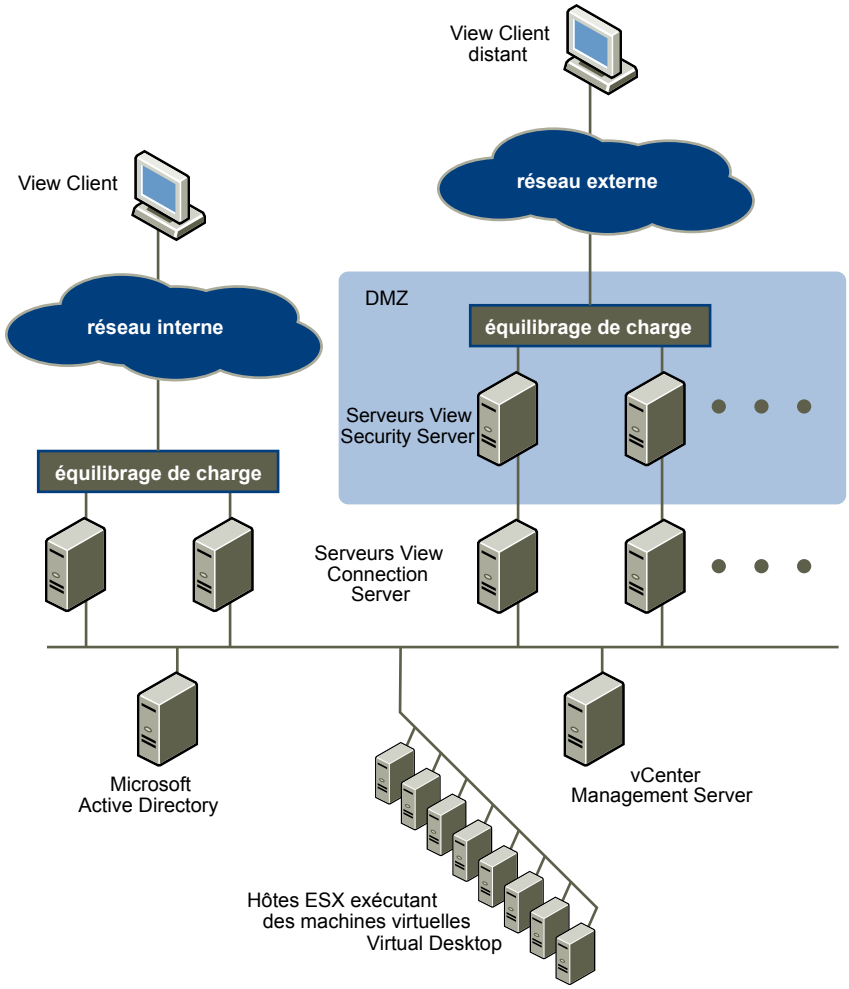


Lorsque des utilisateurs distants se connectent à un serveur de sécurité, ils doivent s'authentifier avant de pouvoir accéder à des postes de travail View. Avec des règles de pare-feu adéquates des deux côtés de la zone DMZ, cette topologie est appropriée pour accéder à des postes de travail View à partir de périphériques client situés sur Internet.

Vous pouvez connecter plusieurs serveurs de sécurité à chaque instance de View Connection Server. Vous pouvez également combiner le déploiement d'une zone DMZ à un déploiement standard pour permettre l'accès aux utilisateurs internes et externes.

La topologie illustrée dans la Figure 5-3 montre un environnement où quatre instances de View Connection Server agissent comme un groupe. Les instances du réseau interne sont dédiées aux utilisateurs du réseau interne et les instances du réseau externe sont dédiées aux utilisateurs du réseau externe. Si les instances de View Connection Server couplées avec les serveurs de sécurité sont activées pour l'authentification RSA SecurID, tous les utilisateurs du réseau externe doivent s'authentifier avec des jetons RSA SecurID.

Figure 5-3. Plusieurs serveurs de sécurité



Vous devez implémenter une solution d'équilibrage de charge matérielle ou logicielle si vous installez plusieurs serveurs de sécurité. View Connection Server ne fournit pas sa propre fonctionnalité d'équilibrage de charge. View Connection Server fonctionne avec des solutions d'équilibrage de charge tierces standard.

Pare-feu pour serveurs de sécurité basés sur une zone DMZ

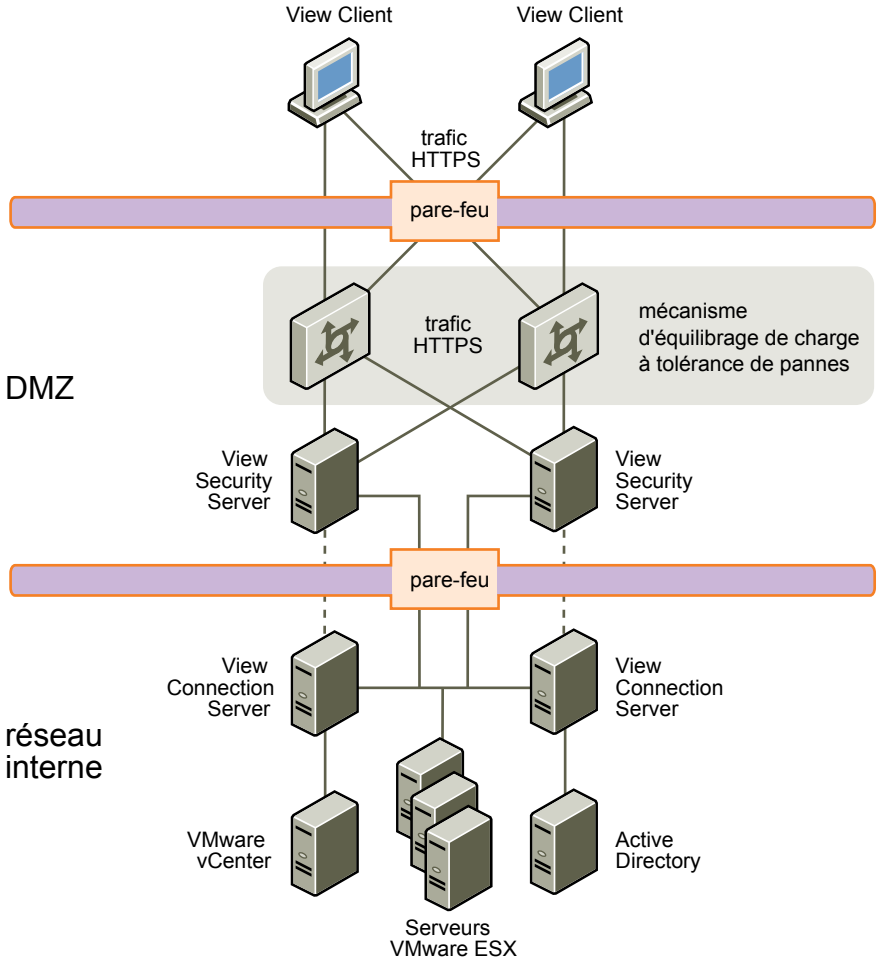
Un déploiement de serveur de sécurité basé sur une zone DMZ doit comporter deux pare-feu.

- Un pare-feu frontal externe en réseau est nécessaire pour protéger la zone DMZ et le réseau interne. Vous configurez ce pare-feu pour permettre au trafic réseau externe d'atteindre la zone DMZ.
- Un pare-feu principal, entre la zone DMZ et le réseau interne, est requis pour fournir un deuxième niveau de sécurité. Vous configurez ce pare-feu pour accepter uniquement le trafic qui provient des services dans la zone DMZ.

La règle de pare-feu contrôle exclusivement les communications entrantes provenant des services de la zone DMZ, ce qui réduit considérablement le risque que le réseau interne soit compromis.

La Figure 5-4 montre un exemple de configuration qui comporte des pare-feu frontal et principal.

Figure 5-4. Topologie de double pare-feu



Règles de pare-feu pour serveurs de sécurité basés sur une zone DMZ

Les serveurs de sécurité basés sur une zone DMZ requièrent certaines règles de pare-feu sur les pare-feu frontaux et principaux.

Règles de pare-feu frontal

Pour autoriser des périphériques client externes à se connecter à un serveur de sécurité dans la zone DMZ, le pare-feu frontal doit autoriser le trafic entrant sur certains ports TCP. Le Tableau 5-1 résume les règles de pare-feu frontal.

Tableau 5-1. Règles de pare-feu frontal

Source	Protocole	Port	Destination	Remarques
Toutes	HTTP	80	Serveur de sécurité	Les périphériques client externes utilisent le port 80 pour se connecter à un serveur de sécurité dans la zone DMZ quand SSL est désactivé.
Toutes	HTTPS	443	Serveur de sécurité	Les périphériques client externes utilisent le port 443 pour se connecter à un serveur de sécurité dans la zone DMZ quand SSL est activé (valeur par défaut).

Règles de pare-feu principal

Pour autoriser un serveur de sécurité à communiquer avec chaque instance de View Connection Server qui réside sur le réseau interne, le pare-feu principal doit autoriser le trafic entrant sur certains ports TCP. Derrière le pare-feu principal, les pare-feu internes doivent être configurés de la même manière pour autoriser les postes de travail View et les instances de View Connection Server à communiquer entre eux. Le Tableau 5-2 résume les règles de pare-feu principal.

Tableau 5-2. Règles de pare-feu principal

Source	Protocole	Port	Destination	Remarques
Serveur de sécurité	AJP13	8009	View Connection Server	Les serveurs de sécurité utilisent le port 8009 pour transmettre le trafic Web AJP13 aux instances de View Connection Server.
Serveur de sécurité	JMS	4001	View Connection Server	Les serveurs de sécurité utilisent le port 4001 pour transmettre le trafic JMS (Java Message Service) aux instances de View Connection Server.
Serveur de sécurité	RDP	3389	Poste de travail View	Les serveurs de sécurité utilisent le port 3389 pour transmettre le trafic RDP aux postes de travail View. **Remarque** Pour la redirection USB, le port TCP 32111 est utilisé avec le RDP. Pour MMR, le port TCP 9427 est utilisé avec le RDP.

Ports TCP pour l'intercommunication de View Connection Server

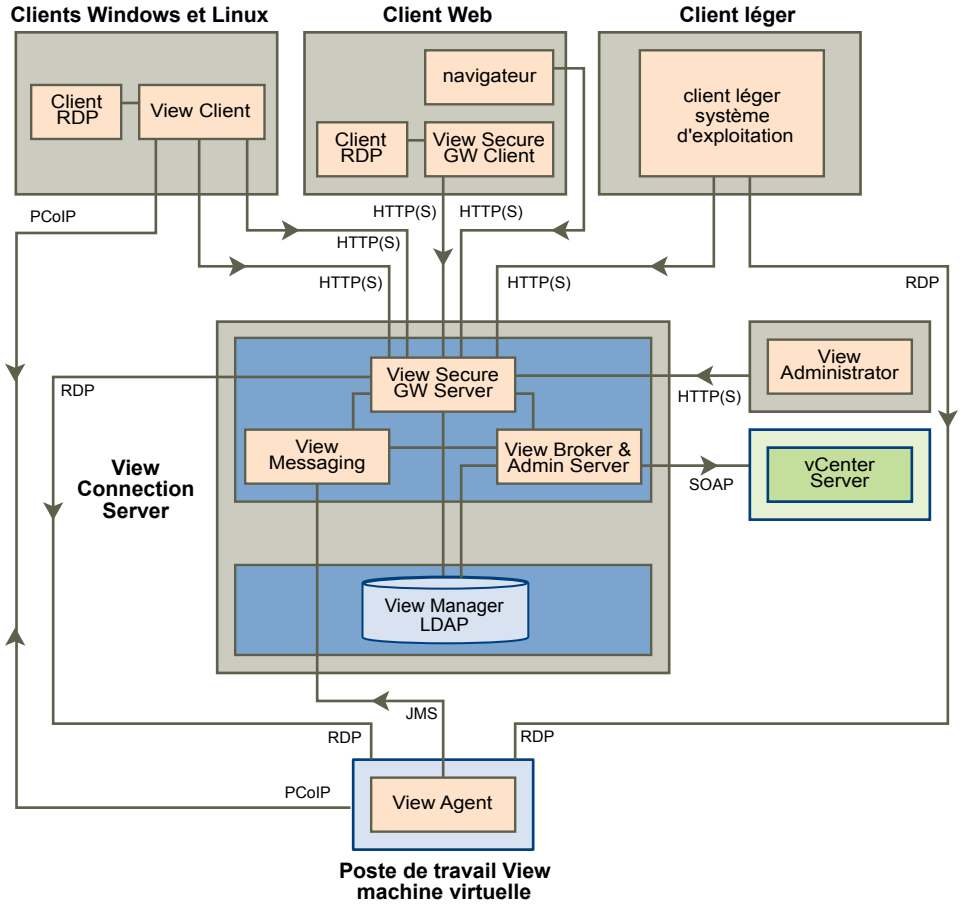
Les groupes d'instances de View Connection Server utilisent des ports TCP supplémentaires pour communiquer entre eux. Par exemple, les instances de View Connection Server utilisent le port 4100 pour se transmettre le trafic interroutage JMS (JMSIR). Les pare-feu ne sont généralement pas utilisés entre les instances de View Connection Server d'un groupe.

Comprendre les protocoles de communication de VMware View

Les composants VMware View échangent des messages en utilisant plusieurs protocoles différents.

La Figure 5-5 illustre les protocoles que chaque composant utilise pour communiquer lorsqu'un serveur de sécurité n'est pas configuré.

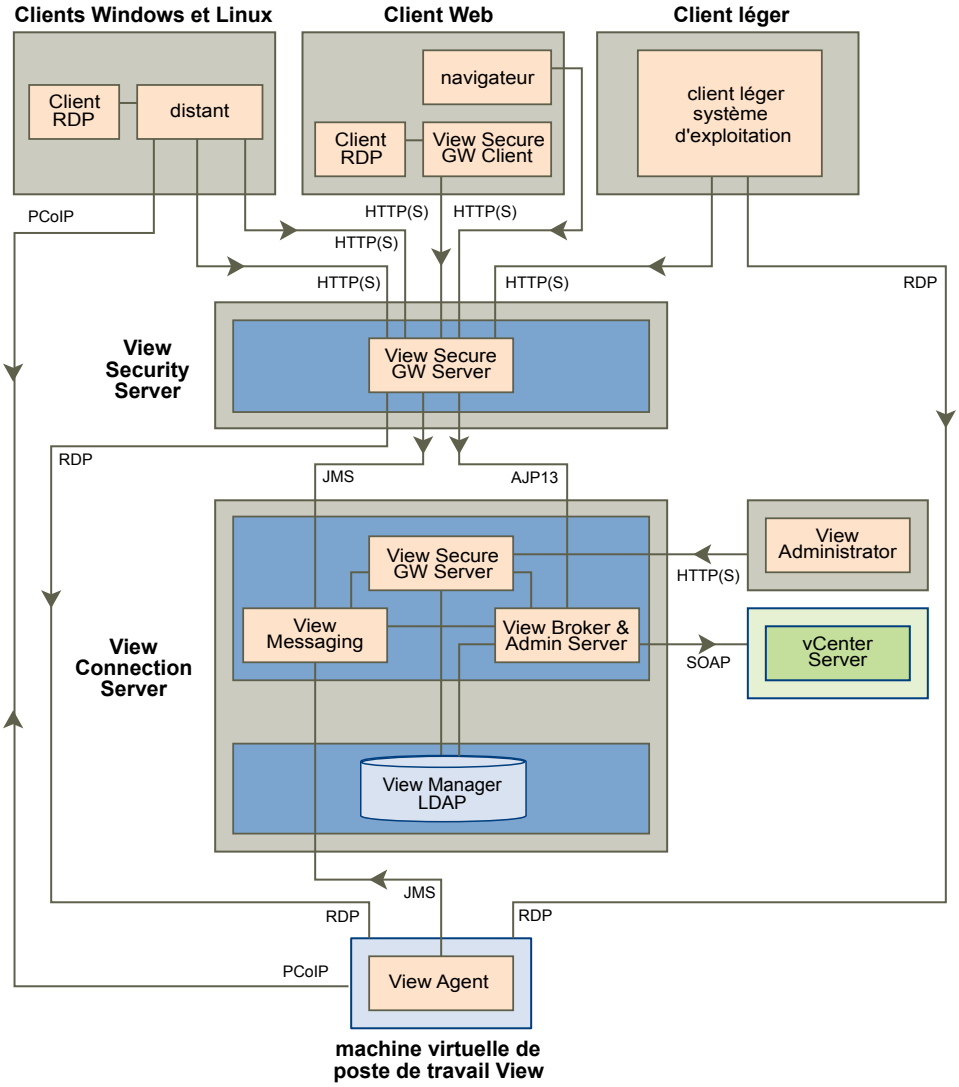
Figure 5-5. Composants VMware View et protocoles sans serveur de sécurité



Pour connaître les ports par défaut utilisés pour chaque protocole, reportez-vous au Tableau 5-3.

La Figure 5-6 illustre les protocoles que chaque composant utilise pour communiquer lorsqu'un serveur de sécurité est configuré.

Figure 5-6. Composants VMware View et protocoles avec un serveur de sécurité



Le Tableau 5-3 répertorie les ports par défaut utilisés par chaque protocole.

Tableau 5-3. Ports par défaut

Protocole	Port
JMS	Port TCP 4001
AJP13	Port TCP 8009 **Remarque** AJP13 n'est utilisé que dans une configuration avec serveur de sécurité.
HTTP	Port TCP 80
HTTPS	Port TCP 443
RDP	Port TCP 3389 Pour la redirection USB, le port TCP 32111 est utilisé avec le RDP. Pour MMR, le port TCP 9427 est utilisé avec le RDP. **Remarque** Si l'instance de View Connection Server est configurée pour des connexions client directes, ces protocoles se connectent directement depuis le client au poste de travail View et ne sont pas transportés via le composant View Secure GW Server.

Tableau 5-3. Ports par défaut (suite)

Protocole	Port
SOAP	Port TCP 80 ou 443
PCoIP	Port TCP 4172 depuis View Client vers le poste de travail View. PCoIP utilise également le port UDP 4172 dans les deux sens. Pour la redirection USB, le port TCP 32111 est utilisé avec PCoIP depuis le client vers le poste de travail View.

View Broker et Administration Server

Le composant View Broker, qui est le centre de View Connection Server, est responsable des interactions d'utilisateurs entre les clients VMware View et View Connection Server. View Broker comprend également le serveur Administration Server utilisé par le client Web de View Administrator.

View Broker fonctionne avec vCenter Server pour fournir une gestion avancée de postes de travail View, y compris les opérations de création et d'alimentation de machines virtuelles.

View Secure Gateway Server

View Secure Gateway Server est le composant côté serveur pour la connexion sécurisée HTTPS entre des clients VMware View et un serveur de sécurité ou une instance de View Connection Server.

Lorsque vous configurez la connexion par tunnel pour View Connection Server, le trafic RDP, USB et MMR (Multimedia Redirection) est transporté via le composant View Secure Gateway. Lorsque vous configurez des connexions client directes, ces protocoles se connectent directement à partir du client au poste de travail View et ne sont pas transportés via le composant View Secure Gateway Server.

Remarque PCoIP et HP RGS n'utilisent pas la connexion par tunnel.

View Secure Gateway Server est également responsable du transfert d'autre trafic Web, y compris l'authentification utilisateur et le trafic de sélection de poste de travail, à partir de clients VMware View vers le composant View Broker. View Secure Gateway Server transmet également le trafic Web du client View Administrator au composant Administration Server.

View LDAP

View LDAP est un répertoire LDAP incorporé dans View Connection Server. Il s'agit également du référentiel de configuration de toutes les données de configuration de VMware View.

View LDAP contient des entrées qui représentent chaque poste de travail View, chaque poste de travail View accessible, plusieurs postes de travail View gérés ensemble et des paramètres de configuration de composant View.

View LDAP comporte également un ensemble de DLL de plug-in de View qui fournissent des services d'automatisation et de notification pour d'autres composants de VMware View.

View Messaging

Le composant View Messaging fournit le routeur de messagerie pour la communication entre les composants View Connection Server et entre View Agent et View Connection Server.

Ce composant prend en charge l'API JMS (Java Message Service) qui est utilisé pour la messagerie dans VMware View.

Par défaut, les clés RSA utilisées pour la validation de message intercomposant sont de 512 bits. Vous pouvez passer la taille de clé RSA à 1 024 bits si vous préférez un chiffrement renforcé.

Si vous souhaitez que toutes les clés soient de 1 024 bits, la taille de clé RSA doit être modifiée immédiatement après l'installation de la première instance de View Connection Server et avant la création de serveurs et de postes de travail supplémentaires. Pour plus d'informations, consultez l'article 1024431 de la base de connaissances de VMware.

Règles de pare-feu pour View Connection Server

Certains ports TCP entrants doivent être ouverts sur le pare-feu pour des instances de View Connection Server et des serveurs de sécurité.

Lorsque vous installez View Connection Server sous Windows Server 2008, le programme d'installation peut configurer facultativement les règles de pare-feu Windows requises. Lorsque vous installez View Connection Server sous Windows Server 2003, vous devez configurer les règles de pare-feu Windows requises manuellement.

Tableau 5-4. Ports TCP ouverts pendant l'installation de View Connection Server

Protocole	Ports	Type d'instance de View Connection Server
JMS	4001	Standard et réplica
JMSIR	4100	Standard et réplica
AJP13	8009	Standard et réplica
HTTP	80	Standard, réplica et serveur de sécurité
HTTPS	443	Standard, réplica et serveur de sécurité

Règles de pare-feu pour View Agent

Le programme d'installation de View Agent ouvre certains ports TCP sur le pare-feu. Les ports sont entrants sauf indication contraire.

Tableau 5-5. Ports TCP ouverts pendant l'installation de View Agent

Protocole	Ports
RDP	3389
Redirection USB	32111
MMR	9427
PCoIP	4172 (TCP et UDP)
HP RGS	42966

Le programme d'installation de View Agent configure la règle de pare-feu locale pour les connexions RDP entrantes pour correspondre au port RDP actuel du système d'exploitation hôte, qui est en général 3389. Si vous modifiez le numéro de port RDP, vous devez modifier les règles de pare-feu associées.

Si vous demandez au programme d'installation de View Agent de ne pas activer la prise en charge du Bureau à distance, il n'ouvre pas les ports 3389 et 32111 et vous devez ouvrir ces ports manuellement.

L'application HP RGS Sender est le composant côté serveur du protocole d'affichage à distance HP RGS. HP RGS Sender utilise le port 42966 par défaut.

Si vous utilisez un modèle de machine virtuelle en tant que source de postes de travail, les exceptions de pare-feu ne continuent sur les postes de travail déployés que si le modèle est membre du domaine de poste de travail. Vous pouvez utiliser les paramètres de stratégie de groupe de Microsoft pour gérer les exceptions de pare-feu locales. Pour plus d'informations, consultez l'article 875357 de la base de connaissances de Microsoft.

Règles de pare-feu pour Active Directory

Si un pare-feu se trouve entre votre environnement VMware View et votre serveur Active Directory, vous devez vous assurer que tous les ports nécessaires sont ouverts.

Par exemple, View Connection Server doit pouvoir accéder aux serveurs Catalogue global Active Directory et LDAP (Lightweight Directory Access Protocol). Si les ports Catalogue global et LDAP sont bloqués par votre pare-feu, les administrateurs auront des problèmes pour configurer les autorisations des utilisateurs.

Consultez la documentation Microsoft pour connaître la version de votre serveur Active Directory et obtenir des informations relatives aux ports qui doivent être ouverts pour qu'Active Directory fonctionne correctement via un pare-feu.

Règles de pare-feu pour View Client with Local Mode

Les données de View Client with Local Mode sont téléchargées via le port 902. Si vous prévoyez d'utiliser la fonction View Client with Local Mode, le port 902 doit être accessible à votre hôte ESX.

Présentation des étapes de configuration d'un environnement VMware View

6

Effectuez ces tâches de haut niveau pour installer VMware View et configurer un déploiement initial.

Tableau 6-1. Liste de vérification Installation et configuration de View

Étape	Tâche
1	Configurez les utilisateurs et les groupes d'administrateurs requis dans Active Directory. Instructions : *Guide d'installation de VMware View* et documentation de vSphere
2	Si vous ne l'avez pas déjà fait, installez et configurez des serveurs VMware ESX et vCenter Server. Instructions : documentation de vSphere
3	Si vous voulez déployer des postes de travail de clone lié, installez View Composer sur le système vCenter Server. Instructions : *Guide d'installation de VMware View*
4	Installez et configurez View Connection Server. Instructions : *Guide d'installation de VMware View*
5	Si vous voulez utiliser des postes de travail en mode local, installez Transfer Server. Instructions : *Guide d'installation de VMware View*
6	Créez une ou plusieurs machines virtuelles pouvant être utilisées comme modèle pour des pools de postes de travail de clone complet ou comme parent pour des pools de postes de travail de clone lié. Instructions : *Guide de l'administrateur de VMware View*
7	Créez un pool de postes de travail. Instructions : *Guide de l'administrateur de VMware View*
8	Contrôlez l'accès des utilisateurs aux postes de travail. Instructions : *Guide de l'administrateur de VMware View*
9	Installez View Client sur des machines d'utilisateurs finaux et demandez aux utilisateurs finaux d'accéder à leurs postes de travail View. Instructions : *Guide d'installation de VMware View*
10	(Facultatif) Créez et configurez des administrateurs supplémentaires pour autoriser différents niveaux d'accès à des objets d'inventaire et des paramètres spécifiques. Instructions : *Guide de l'administrateur de VMware View*
11	(Facultatif) Configurez des règles pour contrôler le comportement de composants View, de pools de postes de travail et d'utilisateurs de poste de travail. Instructions : *Guide de l'administrateur de VMware View*
12	(Facultatif) Pour plus de sécurité, intégrez des solutions d'authentification par carte à puce et RSA SecurID. Instructions : *Guide de l'administrateur de VMware View*

Index