Guide de planification de l'architecture de VMware View

View 4.0.1
View Manager 4.0.1
View Composer 2.0.0

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

FR-000241-02

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

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 VMware View à grande échelle.

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.

1 Présentation de VMware View

VMware View permet aux services informatiques d'exécuter des postes de travail virtuels dans le datacenter et de 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

Le protocole PC-over-IP de VMware View 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 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

Le provisionnement de postes de travail pour les utilisateurs finaux est un processus rapide. Plutôt que d'installer des applications une par une sur le PC physique de chaque utilisateur, l'utilisateur final se connecte 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 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 :

- Impression depuis un poste de travail virtuel sur n'importe quelle imprimante locale ou en réseau définie sur le périphérique 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 provisionner 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 :

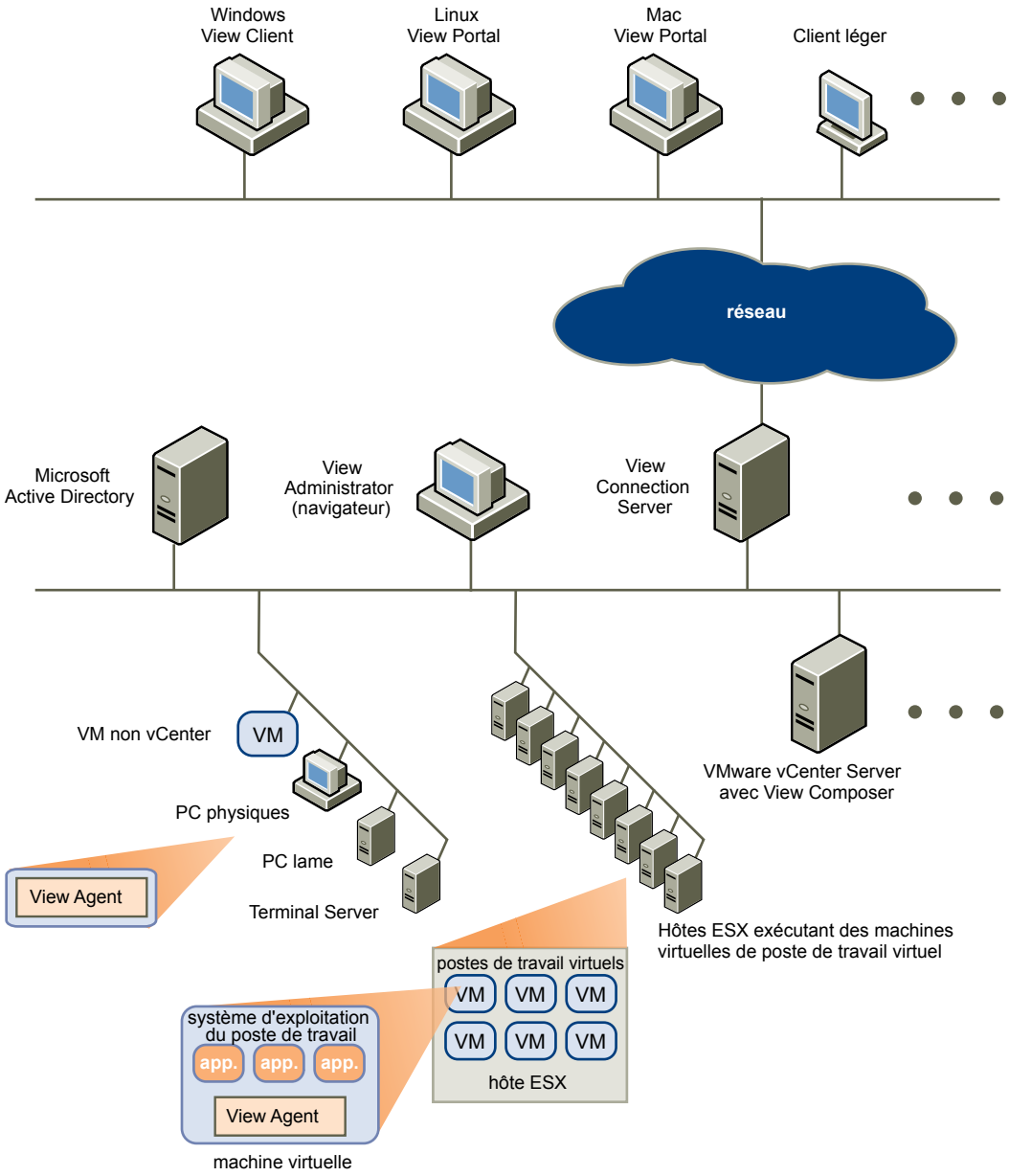
- Intégration à VMware vSphere pour atteindre des densités rentables, des hauts niveaux de disponibilité et un contrôle avancé de l'allocation des ressources pour vos postes de travail virtuels.
- Configuration de View Connection Server pour des connexions de broker entre les utilisateurs finaux et les 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 démarrent View Client ou utilisent View Portal 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 1-1 montre la relation entre les composants principaux d'un déploiement VMware View.

Figure 1-1. 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 quel que soit le périphérique ou l'emplacement. Les utilisateurs peuvent accéder à leur poste de travail 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 Windows, les utilisateurs finaux ouvrent View Client pour afficher leur poste de travail View. Sur un ordinateur Mac ou Linux, les utilisateurs finaux ouvrent un navigateur Web et utilisent View Portal pour afficher leur poste de travail View. Les périphériques Windows peuvent également utiliser View Portal, mais certaines fonctionnalités ne sont pas prises en charge.

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 ;
- la gestion des sessions de postes de travail ;
- l'établissement de connexions sécurisées entre utilisateurs et postes de travail ;
- l'activation de l'ouverture de session 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 , 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 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 Blade. Le protocole d'affichage PCoIP est désormais disponible avec VMware View 4. La vitesse et la qualité d'affichage de PCoIP sont équivalentes à celle d'un PC physique.

View Client with Offline Desktop est une version de View Client étendue pour prendre en charge la fonction expérimentale Offline Desktop. Cette dernière permet aux utilisateurs finaux de télécharger des machines virtuelles et de les utiliser sur leurs systèmes locaux.

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

- View Portal pour Linux (expérimental) et View Portal pour Mac OS X (expérimental).
- 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 ordinateur Mac, Windows ou Linux, les utilisateurs peuvent ouvrir un navigateur Web et utiliser View Portal pour afficher leur poste de travail View. Cette version Web de View Client installe tous les logiciels View nécessaires sur un périphérique client, mais certaines extensions, telles que celles pour connecter des périphériques USB, peuvent ne pas être installées.

Pour utiliser View Portal, les utilisateurs finaux ouvrent un navigateur Firefox, Internet Explorer ou Safari et saisissent l'URL d'une instance de View Connection Server. View Portal demande aux utilisateurs l'autorisation d'installer les composants View Client requis. Sur les clients Linux, View Portal requiert que `rdesktop` affiche des postes de travail virtuels, et sous Mac OS/X, View Portal requiert que Microsoft Remote Desktop Connection Client pour Mac affiche des postes de travail virtuels.

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 poste 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'ouverture de session 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.

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, le provisionnement 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 , de préférence sur une machine virtuelle VMware.

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. Toutefois, avant de décider quelles fonctions à 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 pour déterminer les systèmes d'exploitation client prenant en charge la fonction.

Tableau 2-1. Fonctions prises en charge sur des clients Windows 32 bits

Fonction	Win 2000	Win XP Pro	Win XP Home	Vista Bus SP1, SP2	Vista Ult SP1, SP2	Vista Ent SP2
Accès USB		X	X	X	X	X
Protocole d'affichage RDP	X	X	X	X	X	X
Protocole d'affichage PCoIP		X	X	SP2 uniquement	SP2 uniquement	X

Tableau 2-1. Fonctions prises en charge sur des clients Windows 32 bits (suite)

Fonction	Win 2000	Win XP Pro	Win XP Home	Vista Bus SP1, SP2	Vista Ult SP1, SP2	Vista Ent SP2
Protocole d'affichage HP RGS		X		X	SP2 uniquement	X
Wyse MMR		X	X		SP1 uniquement	
Impression virtuelle	X	X	X		SP1 uniquement	
Offline Desktop		X				

Remarque Les protocoles d'affichage HP RGS et PCoIP ne sont pas disponibles si vous utilisez Web Portal au lieu de View Client natif. Pour plus d'informations sur les exigences matérielles du client et sur les exigences du poste de travail View pour PCoIP, reportez-vous à la section « VMware View avec PCoIP », page 17.

Comme le Tableau 2-2 l'indique, les options sont limitées pour les clients Linux et Mac qui sont pris en charge de façon expérimentale par Web Portal.

Tableau 2-2. Fonctions prises en charge par Web Portal pour les clients Mac OS X et Linux 32 bits

Fonction	Red Hat Ent Linux 5.1	SUSE Linux Ent Desktop 10	Ubuntu Linux 8.04	Mac OS X (10,5)	Mac OS X (10.4)
Accès USB					
Protocole d'affichage RDP	X	X	X	X	X
Protocole d'affichage PCoIP					
Protocole d'affichage HP RGS					
Wyse MMR					
Impression virtuelle					
Offline Desktop					

De plus, plusieurs partenaires de VMware offrent des périphériques de client léger pour les déploiements 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.

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 1920 x 1200 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.

PCoIP a les limites suivantes :

- Le système d'exploitation du poste de travail View doit être Windows XP Professional SP 2 ou 3 ou Windows Vista SP 1 ou 2.
- L'utilisation des cartes à puce n'est pas prise en charge si vous utilisez PCoIP.
- Les utilisateurs qui accèdent à leurs postes de travail virtuels avec View Portal ne peuvent pas utiliser PCoIP.

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 Blade, des stations de travail HP et HP Blade. 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.

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 sur les systèmes Windows 2000.
- Si vous utilisez View Portal pour accéder à un poste de travail View, cette fonction n'est disponible que sur les clients Windows puis uniquement si vous installez d'abord View Client sur le système Windows local avec le composant de redirection USB facultatif.
- Pour utiliser une imprimante USB sur un poste de travail View, vous devez installer les pilotes d'imprimante requis sur le poste de travail View.

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'imprimantes 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.

La fonction d'impression virtuelle a les limites suivantes :

- Si vous utilisez View Portal pour accéder à un poste de travail View, cette fonction n'est disponible que sur les clients Windows puis uniquement si vous installez d'abord View Client sur le système Windows local avec le composant de redirection USB facultatif.
- Cette fonction n'est pas disponible pour les imprimantes USB. Pour utiliser une imprimante USB sur un poste de travail View, vous devez installer les pilotes d'imprimante requis sur le poste de travail View.

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 suivants :

- AC3
- MP3
- MPEG-1, MPEG-2, MPEG-4-part2
- WMA
- WMV 7, 8 et 9

Cette fonction a les limites suivantes :

- Pour une meilleure qualité, utilisez le Lecteur Windows Media 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.

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

La fonction d'ouverture de session 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'ouverture de session 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 installer 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 le 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.

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 poste 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.

Ce chapitre aborde les rubriques suivantes :

Avantages des pools de postes de travail

VMware View permet de créer et de provisionner 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 vCenter comme source de poste 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 à tous les postes de travail virtuels dans un pool. Les exemples suivants indiquent des paramètres disponibles :

- Spécifiez le protocole d'affichage 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.

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

Pools persistants 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 non persistants 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 non persistant 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 non persistants 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 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 22

  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 22

  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 provisionnement aux machines virtuelles.

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 sont 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.

Lorsque vous créez des pools de postes de travail persistants, View Composer crée également un disque de données utilisateur séparé pour chaque poste de travail virtuel. Le profil et les données d'application de l'utilisateur final sont enregistrés sur le disque de données utilisateur. VMware vous recommande de conserver les disques de données utilisateur sur un magasin de données séparé. Vous pouvez ensuite sauvegarder l'ensemble de LUN qui conserve les disques de données utilisateur.

Provisionnement d'application

Avec VMware View, vous pouvez utiliser des techniques de provisionnement d'application traditionnelles, virtualiser des applications 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 23

  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.

- Virtualisation d'applications avec VMware ThinApp page 24

  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 provisionnement d'application flexible et sans conflit.

- Utilisation de processus existants pour le provisionnement d'application page 24

  Avec VMware View, vous pouvez toujours utiliser les techniques de provisionnement 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 instantané 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

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.

Virtualisation d'applications avec VMware ThinApp

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 provisionnement d'application flexible et sans conflit.

Lorsque vous créez une application virtualisée avec ThinApp, les utilisateurs peuvent diffuser l'application à partir d'un serveur de fichiers partagés ou copier l'application sur leurs postes de travail virtuels. Si vous configurez l'application virtualisée pour la diffusion, vous devez remplir les considérations architecturales suivantes :

- Accès aux applications spécifiques par des groupes d'utilisateurs spécifiques
- Configuration de stockage pour le référentiel partagé
- Trafic réseau généré par la diffusion, qui dépend largement du type d'application

Pour les applications diffusées, les utilisateurs peuvent lancer les applications directement depuis le serveur de fichiers partagés ou indirectement en utilisant un raccourci du bureau.

Si vous configurez un fichier de package ThinApp pour qu'il soit copié sur un poste de travail virtuel et qu'il s'y exécute, les considérations architecturales sont semblables à celles que vous remplissez lorsque vous utilisez le provisionnement logiciel MSI traditionnel.

Utilisation de processus existants pour le provisionnement d'application

Avec VMware View, vous pouvez toujours utiliser les techniques de provisionnement 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. 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 le provisionnement 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 GPO (Objet de stratégie de groupe) pour centraliser la gestion et la configuration de postes de travail View Manager et 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 GPO, consultez le *Guide d'administration de View Manager*.

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. Chaque bloc constitutif comporte des composants qui prennent en charge jusqu'à 1 000 postes de travail virtuels. La conception globale intègre 5 de ces blocs constitutifs.

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 assez de détails 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 :

Configuration de machine virtuelle de poste de travail

Les machines virtuelles utilisées comme postes de travail View pour les utilisateurs ne requièrent pas autant d'espace disque et de ressources de traitement que les machines virtuelles de serveur.

Lorsque vous créez une machine virtuelle qui doit être utilisée comme poste 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 les dépenses.

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 leur poste de travail virtuel 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.

Allocation de mémoire à un système d'exploitation client

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, 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.

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, vous devez définir 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. 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.

ficher d'échange de Windows	Par défaut, ce fichier est dimensionné à 150 % de la RAM du client. Généralement situé dans `C:\pagefile.sys`, ce fichier provoque l'agrandissement des machines virtuelles de clone lié et du stockage provisionné finement car on y accède souvent. Réduire la taille du fichier d'échange réduit souvent la taille des disques virtuels (fichiers `.vmdk`) des clones liés. 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 View, même si vous utilisez View Client with Offline Desktop.
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.
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 mémoire requise 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 mémoire requise pour diverses configurations. Les quantités de mémoire répertoriées dans les colonnes complètent la quantité de mémoire requise pour d'autres fonctionnalités de PCoIP.

Comme vous allouez de la RAM par incréments, le tableau indique l'incrément à utiliser. Par exemple, une configuration à un seul écran qui utilise VGA requiert 37,03 Mo, mais le plus petit incrément de RAM est de 64 Mo.

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

Standard de résolution d'affichage	Largeur, en pixels	Hauteur, en pixels	Surcharge avec 1 écrans (Incréments de RAM)	Surcharge avec 2 écrans (Incréments de RAM)	Surcharge avec 4 écrans (Incréments de RAM)
VGA	640	480	37,03 Mo (64 Mo)	44,06 Mo (64 Mo)	58,13 Mo (64 Mo)
SVGA	800	600	40,06 Mo (64 Mo)	51,97 Mo (64 Mo)	73,95 Mo (96 Mo)
720 p	1280	720	51,09 Mo (64 Mo)	72,19 Mo (96 Mo)	114,38 Mo (128 Mo)
UXGA	1600	1200	73,95 Mo (96 Mo)	117,89 Mo (128 Mo)	205,78 Mo (256 Mo)
1080 p	1920	1080	77,46 Mo (96 Mo)	124,92 Mo (128 Mo)	219,84 Mo (256 Mo)
WUXGA	1920	1200	82,73 Mo (96 Mo)	135,47 Mo (196 Mo)	240,94 Mo (256 Mo)
QXGA	2048	1536	102 Mo (128 Mo)	174 Mo (196 Mo)	318 Mo (384 Mo)
WQXGA	2560	1600	123,75 Mo (128 Mo)	217,50 Mo (256 Mo)	405 Mo (512 Mo)

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 1 024 Mo pour des postes de travail Windows XP et 1 536 Mo pour des postes de travail Windows Vista. 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.

Les exigences de CPU varient en fonction du type de travailleur. 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. Les travailleurs du savoir, à leur tour, peuvent avoir des exigences de CPU plus élevées que les travailleurs de saisie de l'information. Au cours de votre phase de pilotage, utilisez un outil de contrôle des performances, comme Perfmon, pour comprendre les niveaux d'utilisation de CPU moyen et maximum pour ces groupes de travailleurs.

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.

Pour définir le dimensionnement, VMware vous recommande de déterminer combien de postes de travail virtuels peuvent être contenus par cœur de CPU. Vous pouvez commencer par piloter 8 machines virtuelles par cœur. Par exemple, si vous surveillez un PC physique avec un processeur 2,2 GHz à cœur unique et que vous trouvez que l'utilisation de CPU moyenne est de 2,79 %, la quantité de CPU est de 130 MHz. Si vous possédez un serveur ESX quadricœur à 2 sockets, vous pouvez héberger 64 machines virtuelles sur le serveur au cours du pilotage. Allouer 130 MHz à chacune des 64 machines virtuelles signifie que la CPU moyenne totale requise est de 8,3 GHz.

En plus de la CPU requise pour le système d'exploitation client et les applications, vous devez également prendre en compte la puissance de traitement supplémentaire requise pour la virtualisation du poste de travail et pour les pics d'utilisation. Cette surcharge prend entre 10 et 25 % de la CPU moyenne. Pour cet exemple, une estimation classique de CPU requise serait de 25 % de 8,3 GHz. Par conséquent, la vitesse de CPU totale du serveur ESX devrait être de 10,38 GHz.

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 de données utilisateur VMware View 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 et en définissant une règle de surcharge de stockage pour des pools de postes de travail View.

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

Exemple de configuration pour un poste de travail de machine virtuelle

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 et Windows Vista.

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 et sont basés sur des informations qui ont été collectées au cours de la validation du guide *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*. Cette architecture utilisait VMware Infrastructure 3.5 pour héberger et gérer des machines virtuelles. Pour plus d'informations sur les limites des machines virtuelles dans vSphere, consultez le document *VMware vSphere Configuration Maximums*.

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

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	1 024 Mo (valeur basse de 512 Mo, valeur haute de 2 048)
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 de données utilisateur ou de profil redirigé)	5 Go (point de départ)
Type d'adaptateur SCSI virtuel	Utilisez LSI Logic, qui n'est pas l'adaptateur par défaut
Adaptateur de réseau virtuel	Utilisez l'adaptateur par défaut, qui est dépendant du système d'exploitation

La quantité d'espace disque système requise dépend du nombre d'applications requises dans l'image de base. L'architecture de référence View 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 de données utilisateur. Si vous utilisez un produit de gestion de profil tiers, ces données peuvent être redirigées dans un profil itinérant Windows vers un système de fichiers CIFS.

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

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	1 536 Mo (standard)
CPU virtuelle	1
Capacité de disque système	20 Go (standard)

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

Élément	Exemple
Capacité des données utilisateur (sous forme de disque de données utilisateur ou de profil redirigé)	5 Go (point de départ)
Type d'adaptateur SCSI virtuel	Utilisez l'adaptateur par défaut, qui est LSI Logic
Adaptateur de réseau virtuel	Utilisez l'adaptateur par défaut, qui est dépendant du système d'exploitation

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

Vous installez vCenter 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 provisionner 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 et View Composer sur une machine physique, cet exemple utilise des machines virtuelles avec les spécifications répertoriées dans le Tableau 4-4. Le serveur ESX qui héberge ces machines virtuelles peuvent faire partie d'un cluster VMware HA pour se protéger contre les échecs du serveur physique.

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

Élément	Exemple
Système d'exploitation	Windows Server 2003 32 bits (avec le dernier Service Pack)
RAM	4 Go
CPU virtuelle	2
Capacité de disque système	20 Go
Type SCSI	LSI Logic (par défaut pour Windows Server 2003)
Adaptateur réseau	Réseau de VM (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, reportez-vous au document http://www.vmware.com/support/vi3/doc/vc_db_calculator.xls.

Configuration et nombre maximum de machines virtuelles dans Connection Server

Lorsque vous installez View Connection Server, l'interface utilisateur de View Administrator est également installée. Ce serveur requiert la même quantité 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 des machines virtuelles avec les spécifications répertoriées dans le Tableau 4-5. Le serveur ESX qui héberge ces machines virtuelles peuvent faire partie d'un cluster VMware HA pour se protéger contre les échecs du serveur physique.

Tableau 4-5. Exemple de machine virtuelle de Connection Server

Élément	Exemple
Système d'exploitation	Windows Server 2003 32 bits (avec le dernier Service Pack)
RAM	4 Go
CPU virtuelle	2 ou 4
Capacité de disque système	20 Go
Type SCSI	LSI Logic (par défaut pour Windows Server 2003)
Adaptateur réseau	Réseau de VM (par défaut)
1 carte réseau	1 Gigabit

Nombre de connexions maximum pour View Connection Server

Le Tableau 4-6 fournit des informations sur le nombre maximum de connexions simultanées auquel un déploiement VMware View peut s'adapter.

Tableau 4-6. 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	2 000
5 serveurs Connection Server	Connexion directe, RDP	5 000
3 serveurs Connection Server	Connexion par tunnel, RDP	2 000
1 serveur Connection Server	Connexion directe, PCoIP	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.

Nœud de VMware View

Un nœud est un serveur VMware ESX qui héberge des postes de travail de machine virtuelle dans un déploiement VMware View. Un nœud peut héberger 8 machines virtuelles par cœur et 64 machines virtuelles par LUN.

VMware View est plus rentable lorsque vous optimisez 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 ne sont pas limitées exagérément par des cœurs de CPU ou par la RAM.

En général, vous pouvez avoir 8 machines virtuelles par cœur de CPU, mais vous devez également prendre en considération les exigences de RAM physique. Après avoir estimé la quantité de RAM à allouer à chaque machine virtuelle, vous pouvez déterminer si une configuration de serveur ESX donnée est limitée par cœur ou par RAM. Si un serveur est limité par cœur, il contient trop de RAM lorsqu'il s'exécute au nombre maximum de machines virtuelles par cœur. Si un serveur est limité par RAM, la RAM physique est consommée avant que le nombre cible de machines virtuelles par cœur soit atteint.

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 30. Pour plus d'informations sur le calcul de la quantité de RAM requise par machine virtuelle, reportez-vous à la section « Allocation de mémoire à un système d'exploitation client », page 28. Prenez également en compte 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.

Les recommandations pour les composants de nœud ESX 3.5 dans le Tableau 4-7 sont spécifiques de VMware View. Pour plus d'informations générales sur les limites des hôtes ESX dans vSphere, consultez le document *VMware vSphere Configuration Maximums*.

Tableau 4-7. Exemple de nœud VMware View pour un serveur ESX

Élément	Exemple
Version ESX	ESX 3.5 U4 ou ESX 4.0 U1
Type de châssis	Lame ou rack
CPU	Quadricœur à 2 ou 4 sockets
Vitesse de CPU	3 GHz par cœur
RAM	128 Go
Port Ethernet	1 Gigabit
Machines virtuelles par cœur	8
Cœurs par nœud	8 pour ESX 3.5, 16 pour ESX 4.0 U1
Cartes réseau	4 (32 machines virtuelles par carte réseau)
Densité de stockage de poste de travail View, en machines virtuelles par LUN	64
Ports d'adaptateur Fiber Channel	0 ou plus

REMARQUE L'exécution de VMware View 3.x sur vSphere 4 n'est pas prise en charge.

Clusters vSphere

Les déploiements VMware View peuvent utiliser des clusters VMware HA pour se protéger contre les échecs du serveur physique. Comme chaque serveur ESX dans un cluster View héberge plus de 40 machines virtuelles et à cause des limites de View Composer, le cluster doit contenir au plus 8 serveurs, ou nœuds.

VMware vSphere et vCenter fournissent un ensemble complet de fonctionnalités 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 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 non persistant peut avoir différentes exigences d'objectif de point de récupération (RPO) qu'un pool persistant. Pour un pool non persistant, 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 4-1. Exemple de configuration de cluster

Les paramètres répertoriés dans le Tableau 4-8 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 4-8. Exemple de cluster HA

Élément	Exemple
Nœuds (serveurs ESX)	8 (y compris un 1 nœud de secours)
Type de cluster	DRS (Distributed Resource Scheduler)/HA
Composant de réseau	Réseau de cluster ESX 3.5 ou 4 standard
Ports commutés	48 GigE gérés pour ESX 3.5 ou 80 pour ESX 4

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 1 000 utilisateurs comprend des serveurs physiques, une infrastructure VMware vSphere, des serveurs VMware View, un stockage partagé et 1 000 postes de travail de machines virtuelles. Vous pouvez inclure jusqu'à cinq blocs constitutifs dans un groupe View.

Tableau 4-9. Exemple de bloc constitutif de View sur le réseau local

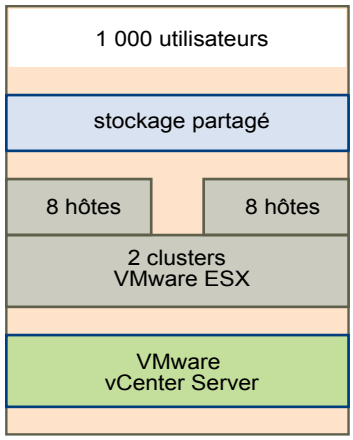
Élément	Exemple
Clusters vSphere	2 (avec 8 hôtes ESX dans chaque cluster)
Commutateur de réseau à 48 ports	1
Composant de stockage de réseau partagé	1
vCenter Server avec View Composer	1 (peut être exécuté dans le bloc lui-même)
Base de données	MS 2005 SQL Server ou serveur de base de données Oracle (peut être exécuté dans le bloc lui-même)
Composant de stockage partagé	1 (avec 64 machines virtuelles par LUN)
Réseaux	3 (un réseau Ethernet 1 Gbit pour chaque réseau de gestion, réseau de stockage et réseau VMotion)

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

Ces informations ont été prises dans le guide *VMware View WAN Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*.

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 de stockage sont l'une des raisons principales pour lesquelles les entreprises adoptent la technologie de virtualisation. 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, la décision d'utiliser View Composer a le plus d'impact sur la planification du stockage. 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 de données utilisateur 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 de données utilisateur 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 22.

Exemple 4-2. Exemple de stockage

Comme exemple de stockage, le Tableau 4-10 répertorie les composants de stockage publiés dans le guide *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*. Ce tableau montre une configuration de stockage requise pour un bloc constitutif de View qui peut contenir 1 000 utilisateurs.

Tableau 4-10. Exemple de configuration de stockage EMC NS20FC

Élément	Nombre
Celerra NS20FC avec une baie principale CLARiiON CX3-10F	1
Cache en écriture CLARiiON	259 Mo
Configurations X-Blade 20	2

Tableau 4-10. Exemple de configuration de stockage EMC NS20FC (suite)

Élément	Nombre
CPU 2,8 GHz Pentium IV	2
RAM à double débit de données (266 MHz)	4
Ports Fibre Channel pour connectivité de stockage principal	2
Ports Ethernet 10/100/1000 BaseT	4
Disques Fibre Channel 300 Go/15K 2/4-Go	30

Exemples de matériel pour blocs constitutifs et groupes View

L'infrastructure virtuelle d'un groupe de blocs constitutifs de VMware View réside sur des serveurs physiques. VMware a utilisé des châssis de serveur lame pour valider son architecture de bloc constitutif, mais vous pouvez utiliser n'importe quel type de serveur avec les mêmes spécifications matérielles.

Exemple 4-3. Matériel d'infrastructure de VMware View

Le matériel semblable à celui indiqué dans le Tableau 4-11 peut héberger des composants d'infrastructure pour un bloc constitutif de View. Les composants d'infrastructure incluent des serveurs de machine virtuelle qui hébergent Active Directory, DNS, DHCP, des instances de View Connection Server, vCenter avec View Composer et la base de données de vCenter.

Tableau 4-11. Exemple de matériel pour un bloc constitutif avec des composants d'infrastructure

Élément	Nombre
Châssis de lame à 16 fentes	1
Serveurs lame	4
Processeur quadricœur 2,66 GHz	4
RAM	32 Go
Lecteur SAS 72 Go	1
Adaptateurs Gb Ethernet Broadcom	4

Sur les 4 serveurs lame, 2 sont destinés aux clients de charge, 1 à une instance de View Connection Server et 1 à Active Directory, DNS et DHCP.

Exemple 4-4. Matériel hébergeant des postes de travail VMware View

Le matériel semblable à celui indiqué dans le Tableau 4-12 peut héberger les postes de travail virtuels d'un bloc constitutif de View qui contient 1 000 utilisateurs.

Tableau 4-12. Exemple de matériel pour un bloc constitutif de VMware View

Élément	Nombre
Châssis de lame à 16 fentes	1 pour 2 blocs constitutifs
Serveurs lame	16 (8 pour chaque cluster)
Processeur quadricœur 2,66 GHz	4
RAM	64 Go (32 Go pour chaque cluster)
Lecteur SAS 72 Go	2
Adaptateurs Gb Ethernet Broadcom	12 (6 pour chaque cluster)

Tableau 4-12. Exemple de matériel pour un bloc constitutif de VMware View (suite)

Élément	Nombre
Modules en liaison montante Gigabit à 4 ports	12 (6 pour chaque cluster)
Commutateur de cœur de réseau Cisco 6500	1

Les composants d'infrastructure et les postes de travail View font partie des clusters VMware HA pour les protéger des échecs du serveur physique.

Ces informations ont été prises dans le guide *VMware View WAN Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*.

Considérations de bande passante pour un bloc constitutif de View

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 pour la configuration de serveur. Vous devez également prendre en compte les effets du matériel de consolidation de port.

Pics de charges de travail

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 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.

Trafic de l'affichage

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.

Prise en charge WAN

Pour les réseaux WAN (Wide-Area Network), vous devez prendre en compte les contraintes de bande passante et les problèmes de latence.

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.

Tableau 4-13. Support pour les bureaux de petite taille ou de taille moyenne avec l'optimisation WAN

Élément	Petit bureau	Bureau de taille moyenne
Nombre d'utilisateurs	Jusqu'à 15	Jusqu'à 100
Type de lien	T1	10 Mbit/s

Tableau 4-13. Support pour les bureaux de petite taille ou de taille moyenne avec l'optimisation WAN (suite)

Élément	Petit bureau	Bureau de taille moyenne
Bande passante	1,544 Mbit/s	10 Mbit/s
Latence	Jusqu'à 100 ms	Jusqu'à 100 ms

Les utilisateurs qui accèdent à un poste de travail View avec le protocole d'affichage RDP depuis chez eux avec une ligne DSL ou un modem câble ne peuvent pas utiliser l'optimisation WAN. Dans ce cas, le réseau peut contenir entre 3 et 5 utilisateurs.

Ces informations ont été prises dans le guide *VMware View WAN Reference Architecture*.

Groupe VMware View

Un groupe VMware View comporte cinq blocs constitutifs de 1 000 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 4-14 répertorie les composants d'un groupe View.

Tableau 4-14. Exemple de groupe VMware View

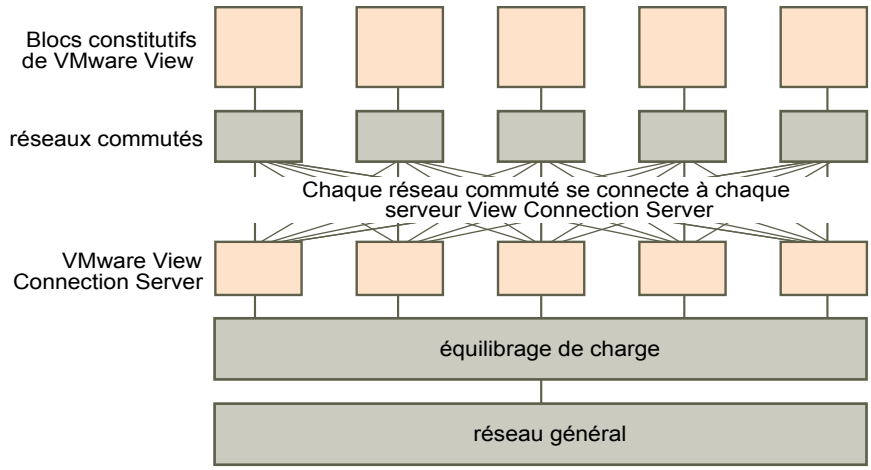
Élément	Nombre
Blocs constitutifs de View	5
View Connection Server	5 (un pour chaque bloc constitutif)
View Security Server	2 à 5 (avec équilibrage de charge dans la zone DMZ)
Module Ethernet 10 Gb	1
Commutateur de cœur de réseau modulaire	1
Module d'équilibrage de charge	1
VPN pour WAN	1 (facultatif)
Accélérateur WAN si RDP est utilisé	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 5 000 postes de travail View



Planification des fonctions de sécurité 5

View Manager offre une sécurité réseau renforcée pour protéger les données d'entreprise sensibles. Pour plus de sécurité, vous pouvez intégrer View Manager 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.

View Manager comporte un certificat SSL auto-signé par défaut que les clients peuvent utiliser lorsqu'ils se connectent à un hôte View Connection Server. Par défaut, les clients sont présentés avec leur propre certificat SSL auto-signé lorsqu'ils visitent une page sécurisée telle que View Administrator.

Vous pouvez utiliser le certificat SSL par défaut à des fins de test. Comme il n'est pas approuvé par les clients et qu'il ne possède pas le nom correct du service, vous devez remplacer le certificat SSL par défaut. Vous pouvez créer votre propre certificat auto-signé, obtenir un certificat signé auprès d'une autorité de certification ou utiliser un certificat SSL que vous possédez déjà.

- Connexions client par tunnel avec Microsoft RDP page 44

  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 44

  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 View Connection Server. Ce type de connexion est appelé connexion client directe.

- Connexions client de View Client with Offline Desktop page 45

  View Client with Offline Desktop est une fonction expérimentale qui offre aux utilisateurs mobiles la possibilité de désactiver une instance clonée de certains types de poste 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 View Manager 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 47.

Les clients qui utilisent les protocoles d'affichage PCoIP ou HP RGS n'utilisent pas la connexion par tunnel. Pour plus d'informations, reportez-vous à la section « Connexions client directes avec PCoIP et HP RGS », page 44.

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 View Connection Server. Ce type de connexion est appelé connexion client directe.

Avec des connexions client directes, une connexion HTTPS est toujours faite entre le client et l'hôte 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.

Si les clients utilisent les protocoles d'affichage PCoIP ou HP RGS, vous devez activer les connexions client directes.

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. Pour plus d'informations, reportez-vous à la section « Connexions client par tunnel avec Microsoft RDP », page 44.

Connexions client de View Client with Offline Desktop

View Client with Offline Desktop est une fonction expérimentale qui offre aux utilisateurs mobiles la possibilité de désactiver une instance clonée de certains types de poste de travail View sur leur ordinateur local.

View Client with Offline Desktop prend en charge les communications par tunnel et hors tunnel pour les transferts de données sur réseau local. Avec les communications par tunnel, tout le trafic est routé via l'hôte 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 système client Offline Desktop et la machine virtuelle de poste de travail View.

Les données hors ligne 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

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

- Authentification Active Directory page 45

  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.

- Authentification RSA SecurID page 46

  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 46

  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 47

  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 la commande `vdmadmin` pour configurer le filtrage de domaines, qui limite les domaines qu'une instance de View Connection Server ou qu'un serveur de sécurité recherche, et qu'il affiche aux utilisateurs. Pour plus d'informations, consultez la note technique *Command-Line Tool for View Manager*.

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.

View Manager 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).

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.

Chaque système client qui utilise l'authentification par carte à puce doit posséder un lecteur de carte à puce compatible avec Windows et des pilotes d'application spécifiques du produit.

L'authentification par carte à puce n'est prise en charge que par View Client. Elle n'est pas prise en charge par View Client with Offline Desktop, View Portal ni View Administrator.

L'authentification par carte à puce n'est pas prise en charge pour les clients qui utilisent le protocole d'affichage PCoIP.

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 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.

Remarque Lorsque l'authentification par carte à puce est requise, l'authentification échoue pour les utilisateurs qui cochent la case **[Se connecter en tant qu'utilisateur actuel]** . Ces utilisateurs doivent s'authentifier de nouveau avec leur carte à puce et leur code PIN lorsqu'ils ouvrent une session sur un poste de travail View.

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 démilitarisée (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 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 54.

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 local.

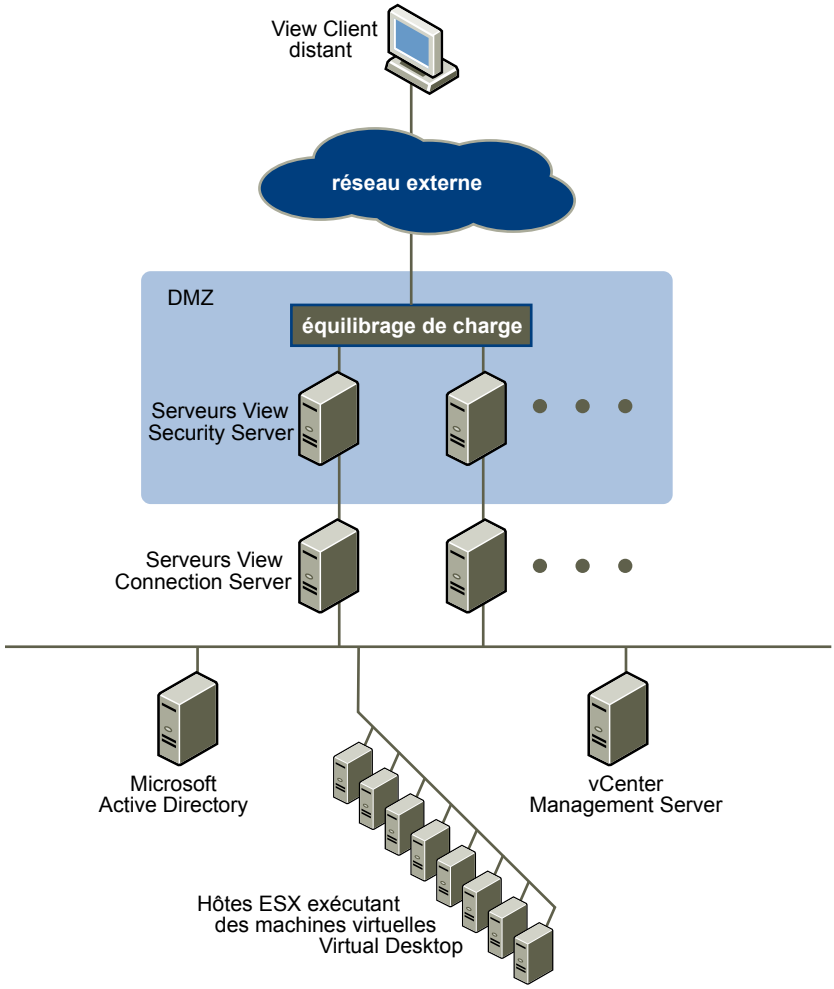
Les clients View qui utilisent PCoIP peuvent se connecter à des serveurs de sécurité View, mais les sessions PCoIP avec le poste de travail virtuel ignorent le serveur de sécurité. PCoIP utilise le protocole UDP (User Datagram Protocol) pour la diffusion audio et vidéo. Les serveurs de sécurité ne prennent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

Topologies de serveur de sécurité

Vous pouvez implémenter plusieurs topologies de serveur de sécurité différentes.

La topologie illustrée dans la Figure 5-1 montre un environnement hautement disponible qui comprend deux serveurs de sécurité avec équilibre de charge dans une zone DMZ. Les serveurs de sécurité communiquent avec deux instances de View Connection Server dans le réseau interne.

Figure 5-1. Serveurs de sécurité avec équilibre de charge dans une zone DMZ

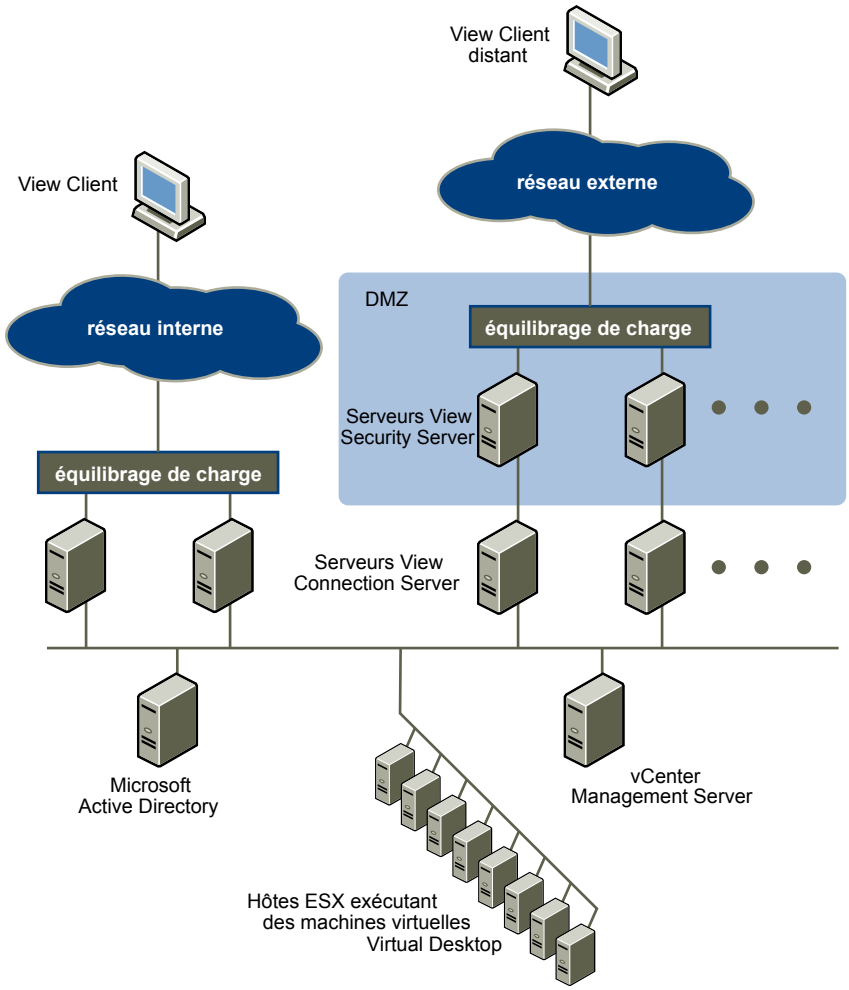


Lorsque des utilisateurs distants se connectent à un serveur de sécurité, ils doivent s'authentifier avant de pouvoir accéder à des postes de travail View. Avec des règles de pare-feu adéquates des deux côtés de la zone DMZ, cette topologie est appropriée pour accéder à des postes de travail View à partir 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 5-2 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 5-2. 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 fonctionne avec des solutions d'équilibrage de charge tierces standard. View Connection Server ne fournit pas sa propre fonctionnalité d'équilibrage de charge.

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

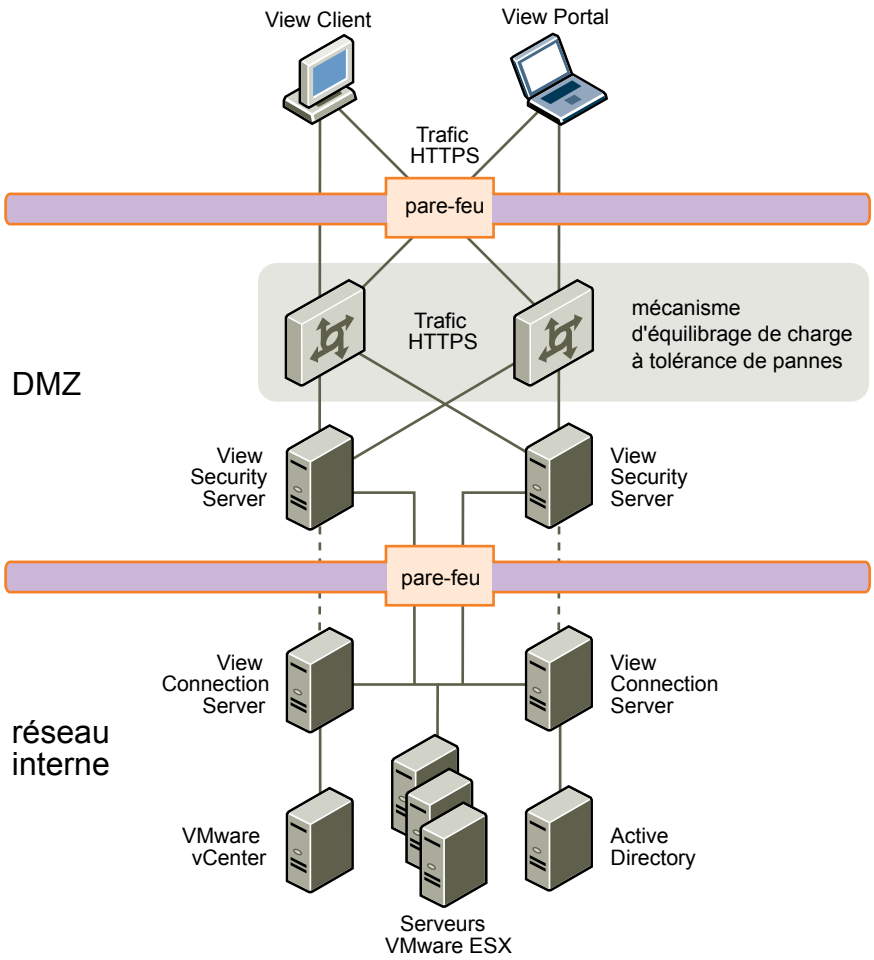
Un déploiement de serveur de sécurité basé sur une zone DMZ doit comporter deux pare-feu.

- 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 5-3 montre un exemple de configuration qui comporte des pare-feu frontal et principal.

Figure 5-3. Topologie de double pare-feu

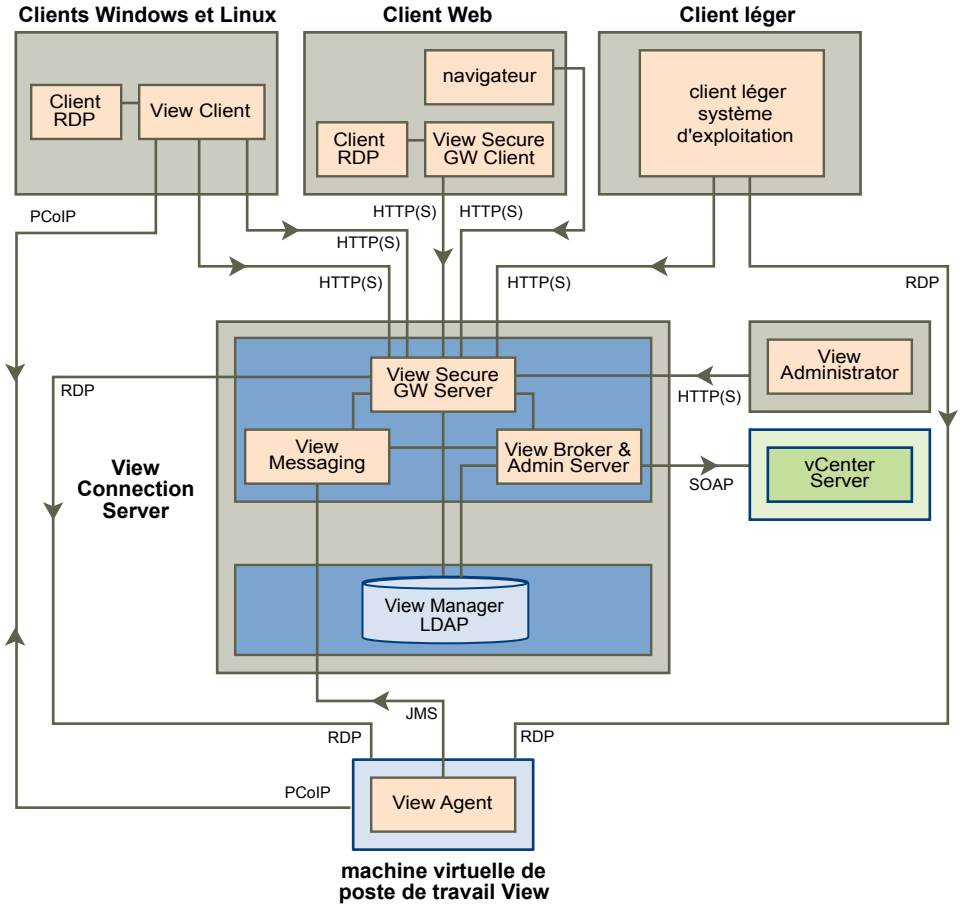


Composants View Manager et protocoles

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

La Figure 5-4 illustre les rapports entre composants View Manager, y compris les protocoles que chaque composant utilise pour la communication, lorsqu'un serveur de sécurité n'est pas configuré.

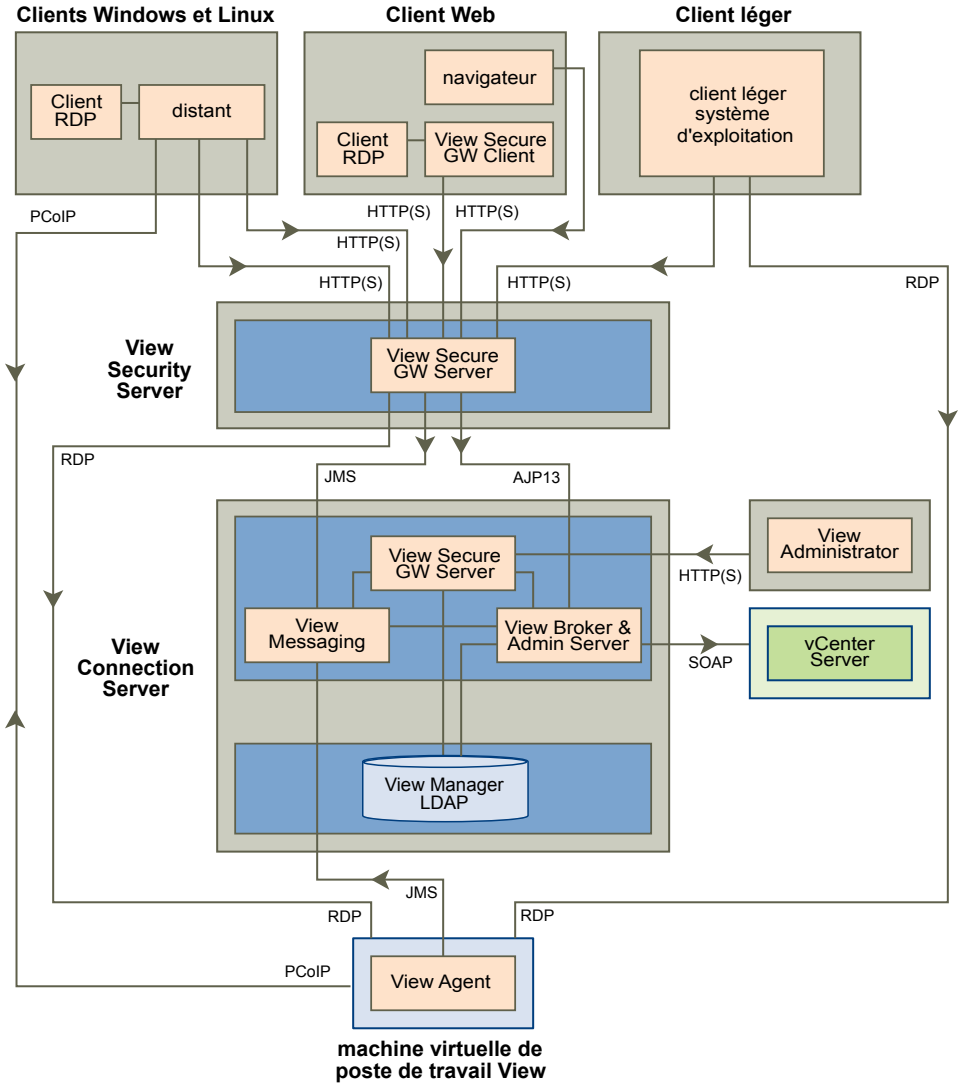
Figure 5-4. Composants View Manager et protocoles sans serveur Security Server



Pour connaître les ports par défaut utilisés pour chaque protocole, reportez-vous au Tableau 5-1.

La Figure 5-5 illustre les rapports entre le serveur de sécurité et tous les autres composants View Manager, notamment les protocoles que chaque composant utilise pour la communication, lorsqu'un serveur de sécurité est configuré.

Figure 5-5. Composants View Manager et protocoles avec un serveur Security Server



Le Tableau 5-1 répertorie les ports par défaut utilisés pour chaque protocole.

Tableau 5-1. 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 5-1. Ports par défaut (suite)

Protocole	Port
SOAP	Port TCP 80 ou 443
PCoIP	Port TCP 50002 depuis View Client vers le poste de travail View. PCoIP utilise également le port UDP 50002 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 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 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 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 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 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.

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

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 5-2 résume les règles de pare-feu frontal.

Tableau 5-2. 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 5-3 résume les règles de pare-feu principal.

Tableau 5-3. 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 la communication 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.

Comme les pare-feu ne sont généralement pas utilisés entre les instances View Connection Server d'un groupe, ces ports TCP ne sont pas décrits ici.

Règles de pare-feu générales pour les composants View Manager

Dans toute configuration de pare-feu, des ports TCP doivent être ouverts pour autoriser le trafic entre certains composants View Manager.

Pour connaître les règles spécifiques des implémentations de serveur de sécurité, reportez-vous à la section « Règles de pare-feu pour serveurs de sécurité basés sur une zone DMZ », page 54.

Règles de pare-feu pour View Agent

Le Tableau 5-4 répertorie les ports TCP ouverts sur le pare-feu par le programme d'installation de View Agent. Les ports sont des ports TCP entrants sauf mention contraire. Reportez-vous à la section « Composants View Manager et protocoles », page 50 pour plus d'informations sur les protocoles.

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

Protocole	Ports
RDP	3389
Redirection USB	32111
MMR	9427
PCoIP	50002 (TCP et UDP)
HP RGS	42966

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

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

Si vous utilisez un modèle de machine virtuelle en tant que source de poste 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 règle 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 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 Offline Desktop

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

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.

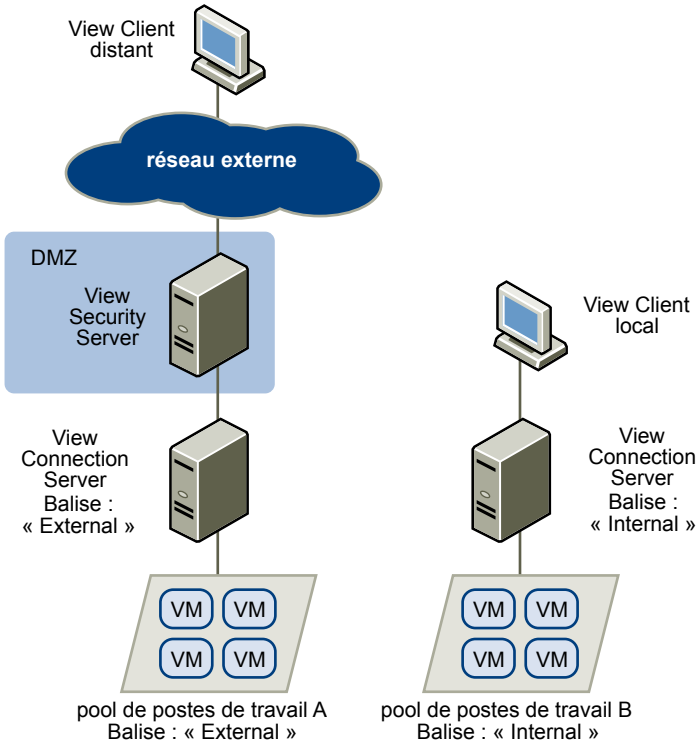
Avec des autorisations limitées, vous affectez une ou plusieurs balises à une instance de View Connection Server. Ensuite, lorsque vous configurez un poste de travail ou un pool de postes de travail, vous sélectionnez les balises des instances de View Connection Server que vous voulez rendre capables d'accéder au poste de travail ou 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 postes de travail et aux pools de postes de travail qui ont au moins une balise correspondante ou qui n'ont aucune balise.

Par exemple, votre déploiement 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 postes de travail et aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs internes.
- Affectez la balise « External » aux postes de travail et aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs externes.

Les utilisateurs externes ne peuvent pas voir les postes de travail et 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 postes de travail et 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 5-6 illustre cette configuration.

Figure 5-6. 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 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.

Présentation des étapes de configuration d'un environnement VMware View

6

La liste de vérification Installation et configuration de View décrit les étapes de haut niveau pour la création d'un déploiement View, indique dans quel ordre les réaliser et précise les documents fournissant les instructions y relatives.

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

Étape	Tâche
1	Configurez les utilisateurs et les groupes administrateur requis dans Active Directory. Instructions : *Guide d'administration de VMware View Manager* et la documentation de vSphere
2	(Facultatif) Installez et configurez des serveurs VMware ESX et vCenter Server Instructions : documentation de vSphere, calendrier de lancement de la documentation
3	(Facultatif) Installez View Composer sur vCenter Server. Instructions : *Guide d'administration de VMware View Manager*
4	Installez View Connection Server. Instructions : *Guide d'administration de VMware View Manager*
5	Copiez les modèles GPO Active Directory de la machine View Connection Server sur le serveur Active Directory et importez-les. Instructions : *Guide d'administration de VMware View Manager*
6	Effectuez une configuration initiale de View Connection Server. Instructions : *Guide d'administration de VMware View Manager*
7	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. Installez les applications de votre choix ou des applications VMware ThinApp. Instructions : documentation vSphere, calendrier de lancement de la documentation et le guide *Windows XP Deployment Guide* pour VMware View
8	Installez View Agent sur les machines virtuelles et physiques que vous voulez utiliser comme sources de postes de travail. Instructions : *Guide d'administration de VMware View Manager*
9	Créez un poste de travail View individuel ou un pool de postes de travail View, ou les deux. Instructions : *Guide d'administration de VMware View Manager*
19	Autorisez des utilisateurs ou des groupes d'utilisateurs ou les deux sur les postes de travail. Instructions : *Guide d'administration de VMware View Manager*
11	Définissez des règles de poste de travail. Instructions : *Guide d'administration de VMware View Manager*
12	Installez View Client sur des machines d'utilisateurs ou indiquez-leur d'utiliser View Portal pour installer les composants requis. Instructions : *Guide d'administration de VMware View Manager*

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

Étape	Tâche
13	Demandez à des utilisateurs d'accéder à leurs postes de travail View. Instructions : *Guide d'administration de VMware View Manager*
14	Gérez et contrôlez les utilisateurs et les postes de travail. Instructions : *Guide d'administration de VMware View Manager*

Index