

Planification de l'architecture Horizon 7

14 mars 2019

VMware Horizon 7 7.8



vmware®

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

<https://docs.vmware.com/fr/>

Les dernières mises à jour produit se trouvent également sur le site Web de VMware.

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2009–2019 VMware, Inc. Tous droits réservés. [Informations sur le copyright et les marques commerciales.](#)

Table des matières

Planification de l'architecture Horizon 7 5

1 Présentation de Horizon 7 6

Avantages de l'utilisation de Horizon 7 6

Fonctions d' Horizon 7 9

Comment les composants fonctionnent ensemble 12

Intégration et personnalisation d' Horizon 7 17

2 Planification d'une expérience d'utilisateur riche 24

Matrice de prise en charge des fonctionnalités pour Horizon Agent 24

Choisir un protocole d'affichage 25

Utilisation d'applications publiées 33

Utilisation d'Horizon Persona Management pour conserver des données et des paramètres
utilisateur 34

Utilisation de périphériques USB avec des applications et postes de travail distants 35

Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones 36

Utilisation des applications graphiques 3D 37

Diffusion multimédia sur un poste de travail distant 38

Impression à partir d'un poste de travail distant 38

Utilisation de l'authentification unique pour la connexion 39

Écrans et résolution d'écran 40

3 Gestion de pools de postes de travail et d'applications depuis un emplacement central 43

Avantages des pools de postes de travail 43

Avantages des pools d'applications 44

Réduction et gestion des exigences de stockage 45

Approvisionnement d'application 56

Utilisation de GPO Active Directory pour gérer des utilisateurs et des postes de travail 61

4 Recommandations sur la planification et les éléments de conception d'architecture pour les déploiements de postes de travail distants 63

Exigences de machine virtuelle pour les postes de travail distants 64

Horizon 7 Nœud ESXi 70

Pools de postes de travail pour des types de travailleurs spécifiques 71

Configuration de machine virtuelle de poste de travail 77

Configuration d'une machine virtuelle hôte RDS 78

Configuration d'une machine virtuelle vCenter Server et View Composer 79

Configuration maximale du Serveur de connexion Horizon et configuration de machine virtuelle	81
Clusters vSphere	84
Exigences de stockage et de bande passante	86
Blocs constitutifs Horizon 7	98
Espaces Horizon 7	98
Avantages à utiliser plusieurs vCenter Server dans un groupe	101

5 Planification des fonctions de sécurité 105

Comprendre les connexions client	105
Choisir une méthode d'authentification utilisateur	108
Restriction de l'accès aux postes de travail distants	113
Utilisation de paramètres de stratégie de groupe pour sécuriser des applications et postes de travail distants	114
Utilisation de Stratégies de carte à puce	115
Implémentation de meilleures pratiques pour sécuriser des systèmes client	115
Affectation de rôles d'administrateur	116
Préparation pour l'utilisation d'un serveur de sécurité	116
Comprendre les protocoles de communication	123

6 Présentation des étapes de configuration d'un environnement Horizon 7 132

Planification de l'architecture Horizon 7

Planification de l'architecture de Horizon 7 présente VMware Horizon™ 7. Il décrit ses principales fonctionnalités et options de déploiement et présente la façon dont les composants sont généralement configurés dans un environnement de production.

Ce guide répond aux questions suivantes :

- Le produit résout-il les problèmes pour lesquels vous avez besoin d'une solution ?
- Est-il envisageable et rentable de mettre en place cette solution dans votre entreprise ?

Les fonctionnalités et capacités de VMware Horizon 7 ne sont pas toutes disponibles dans toutes les éditions. Pour comparer les fonctionnalités de chaque édition, consultez

<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

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

Public cible

Ces informations sont destinées aux décideurs, architectes, administrateurs informatiques ou autres personnes qui veulent se familiariser avec les composants et les fonctions de ce produit. Ces informations permettent aux architectes et aux planificateurs de déterminer si Horizon 7 répond aux besoins de leur entreprise pour fournir de façon efficace et sécurisée des postes de travail et des applications Windows à leurs utilisateurs finaux. L'exemple d'architecture aide les planificateurs à comprendre les exigences matérielles et à quantifier les efforts nécessaires pour un déploiement à grande échelle.

Présentation de Horizon 7

Avec Horizon 7, les services informatiques peuvent exécuter des applications et des postes de travail distants dans le centre de données et fournir ces postes de travail et ces applications 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 centre de données.

Ce chapitre contient les rubriques suivantes :

- [Avantages de l'utilisation de Horizon 7](#)
- [Fonctions d'Horizon 7](#)
- [Comment les composants fonctionnent ensemble](#)
- [Intégration et personnalisation d'Horizon 7](#)

Avantages de l'utilisation de Horizon 7

Lorsque vous gérez des postes de travail d'entreprise avec Horizon 7, les avantages sont, entre autres, une fiabilité, une sécurité, une indépendance matérielle et une commodité améliorées.

Fiabilité et sécurité

Les applications et les postes de travail peuvent être centralisés par une intégration avec VMware vSphere® et la virtualisation des ressources de serveur, de stockage et de mise en réseau. Placer des systèmes d'exploitation de poste de travail et des applications sur un serveur dans le centre de données offre 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.
- La prise en charge RADIUS fournit une flexibilité lorsque vous choisissez des fournisseurs avec authentification à deux facteurs. Les fournisseurs pris en charge incluent RSA SecureID, VASCO DIGIPASS, SMS Passcode et SafeNet, entre autres.
- L'intégration avec VMware Identity Manager signifie que les utilisateurs ont accès à la demande à des postes de travail distants via le catalogue d'applications Web qu'ils utilisent pour accéder à des applications SaaS, Web et Windows. Dans un poste de travail distant, les utilisateurs peuvent également utiliser ce magasin d'applications personnalisées pour accéder à des applications.

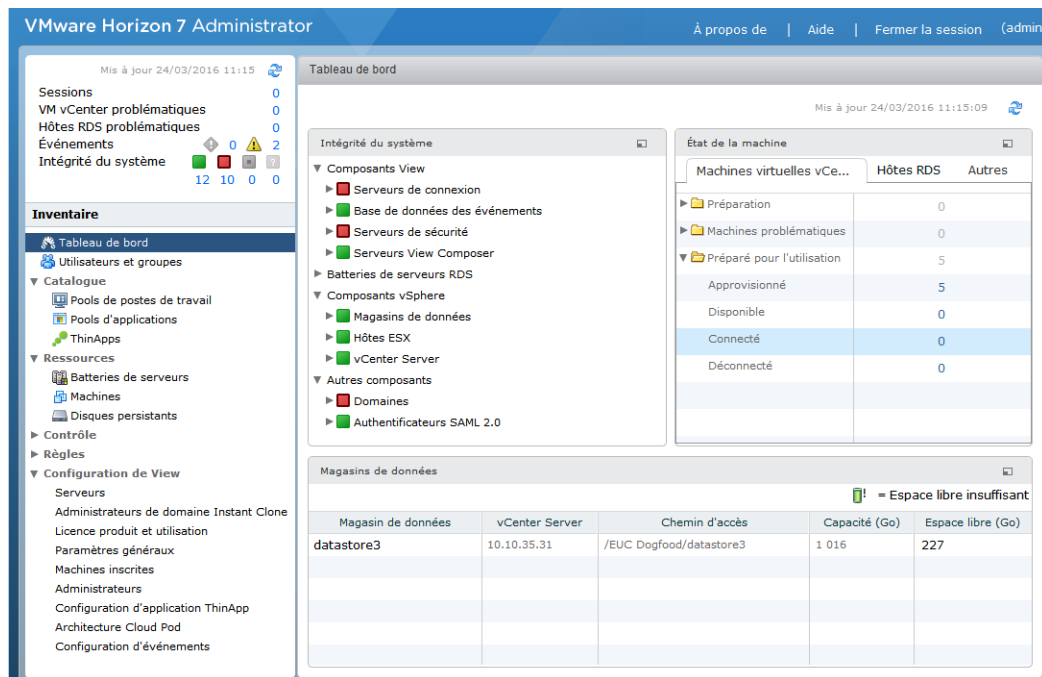
- La capacité d'approvisionner des postes de travail distants avec des comptes Active Directory créés au préalable répond aux exigences d'environnements Active Directory verrouillés qui ont des stratégies d'accès en lecture seule.
- Des sauvegardes de données peuvent être programmées sans se soucier de l'heure à laquelle les systèmes des utilisateurs peuvent être éteints.
- Les applications et postes de travail distants hébergés dans un centre de données subissent 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 hôtes des services Bureau à distance (RDS) Microsoft.

Commodité

La console de gestion unifiée est créée à des fins d'évolutivité pour que même les déploiements d'Horizon 7 les plus importants puissent être gérés efficacement à partir d'une seule interface de gestion. Des assistants et des tableaux de bord améliorent le workflow et facilitent la descente dans la hiérarchie pour afficher des détails ou pour modifier des paramètres. [Chiffre 1-1](#) montre un exemple de l'interface utilisateur basée sur un navigateur pour Horizon Administrator.

Chiffre 1-1. Console administrative affichant la vue du tableau de bord



Les autres fonctionnalités qui améliorent le confort d'utilisation sont les protocoles d'affichage à distance de VMware, PCoIP (PC over IP) et Blast Extreme. Ces protocoles d'affichage à distance délivrent 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, les protocoles d'affichage peuvent 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.

Facilité de gestion

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

L'utilisation de VMware vSphere pour héberger des postes de travail virtuels et des serveurs d'hôtes RDS offre 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.
- Grâce à l'intégration avec VMware Identity Manager, les responsables informatiques peuvent utiliser l'interface d'administration Web d'VMware Identity Manager pour surveiller les droits d'accès des utilisateurs et des groupes aux postes de travail distants.
- L'intégration à VMware App Volumes, un système de fourniture d'applications en temps réel, permet aux entreprises de fournir et de gérer des applications à grande échelle. Utilisez App Volumes pour lier des applications à des utilisateurs, des groupes ou des ordinateurs cibles, même lorsque les utilisateurs sont connectés à leur poste de travail. Il est également possible de provisionner, de fournir, de mettre à jour et de mettre hors service des applications en temps réel.
- Avec Horizon Persona Management, les postes de travail physiques et virtuels peuvent être gérés de façon centrale, y compris les profils d'utilisateur, les droits d'application, les stratégies, les performances et autres paramètres. Déployez Persona Management sur des postes de travail physiques avant de les convertir en postes de travail virtuels.
- Avec VMware User Environment Manager, les utilisateurs finaux obtiennent un poste de travail Windows personnalisé adapté à la situation de l'utilisateur, ce qui signifie que l'accès aux ressources informatiques requises se base sur des aspects tels que le rôle, le périphérique et l'emplacement.
- La gestion du stockage est simplifiée. Avec VMware vSphere, vous pouvez virtualiser des volumes et des systèmes de fichiers pour ne pas avoir à gérer des périphériques de stockage séparés.
- Avec vSphere 6.0 ou version ultérieure, vous pouvez utiliser Virtual Volumes (VVols). Cette fonctionnalité mappe les disques virtuels et leurs dérivés, clones, snapshots et répliques, directement à des objets nommés volumes virtuels sur un système de stockage. Ce mappage permet à vSphere de décharger des opérations de stockage intensives telles que la prise de snapshots, le clonage et la réplication sur le système de stockage. Par exemple, une opération de clonage qui mettait précédemment une heure s'exécute dorénavant en seulement quelques minutes à l'aide de Virtual Volumes.

- Avec vSphere 5.5 Update 1 ou version ultérieure, vous pouvez utiliser vSAN, qui virtualise les disques SSD et les disques durs locaux physiques disponibles sur les hôtes ESXi™ dans une banque de données unique partagée par tous les hôtes d'un cluster. Vous spécifiez une seule banque de données lors de la création d'un pool de postes de travail, et les différents composants, comme les fichiers, réplicas, données utilisateur et fichiers de système d'exploitation de la machine virtuelle sont placés sur des disques SSD ou des disques durs, selon les besoins.

Vous gérez les exigences du stockage de la machine virtuelle, comme la capacité, les performances et la disponibilité, sous la forme de profils de stratégie de stockage par défaut qui sont créés automatiquement lors de la création d'un pool de postes de travail.

- Avec Horizon 7 Storage Accelerator, la charge de stockage IOPS est considérablement réduite, ce qui permet de prendre en charge les connexions d'utilisateurs à des échelles plus grandes sans nécessiter de technologie de baie de stockage particulière.
- Si des postes de travail distants utilisent le format de disque à optimisation d'espace disponible avec vSphere 5.1 et version ultérieure, les données périmées ou supprimées dans un système d'exploitation invité sont automatiquement récupérées avec un processus d'effacement et de réduction.

Indépendance matérielle

Les applications publiées et les postes de travail distants sont indépendants du matériel. Par exemple, comme un poste de travail distant s'exécute sur un serveur dans le centre de données et qu'il n'est accessible que depuis un périphérique client, un poste de travail distant peut utiliser un système d'exploitation qui n'est peut-être pas compatible avec le matériel du périphérique client.

Les postes de travail distants s'exécutent sur des PC, des Mac, des clients légers, des PC reconvertis en clients légers, des tablettes et des téléphones. Les applications publiées s'exécutent sur un sous-ensemble de ces périphériques. Un nouveau support de périphérique est ajouté tous les trimestres.

Si vous utilisez la fonctionnalité HTML Access, les utilisateurs finaux peuvent ouvrir une application ou un poste de travail distant dans un navigateur, sans devoir installer d'application cliente sur le système ou le périphérique client.

Fonctions d' Horizon 7

Les fonctions incluses dans Horizon 7 comprennent la convivialité, la sécurité, le contrôle centralisé et l'évolutivité.

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

- Sur certains périphériques clients, imprimez à partir d'un poste de travail virtuel sur n'importe quelle imprimante locale ou en réseau définie sur le périphérique client. Cette 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.

- Sur la plupart des périphériques client, utilisez la fonctionnalité d'impression basée sur l'emplacement pour effectuer un mappage vers des imprimantes physiquement proches du système client. L'impression basée sur l'emplacement requiert que vous installiez des pilotes d'imprimante sur la machine virtuelle.
- La redirection de l'imprimante locale est conçue pour les cas d'utilisation suivants :
 - Des imprimantes connectées directement à des ports USB ou série sur le client
 - Des imprimantes spécialisées, telles que des imprimantes de code-barres et d'étiquettes, connectées au client
 - Des imprimantes réseau sur un réseau distant qui ne sont pas adressables à partir de la session virtuelle.
- Utilisation de plusieurs écrans. Avec les protocoles d'affichage PCoIP et Blast Extreme, la prise en charge de plusieurs moniteurs signifie que vous pouvez ajuster la résolution d'affichage et la rotation séparément pour chaque moniteur.
- Accès à des périphériques USB et autres connectés au périphérique local qui affiche votre poste de travail virtuel.

Vous pouvez spécifier à quels types de périphériques USB les utilisateurs sont autorisés à se connecter. Pour les périphériques composites qui contiennent plusieurs types de périphériques, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage, vous pouvez diviser le périphérique pour qu'un périphérique (par exemple, le périphérique d'entrée vidéo) soit autorisé mais pas l'autre (par exemple, le périphérique de stockage).

- Utilisez Horizon Persona Management pour conserver des paramètres et des données utilisateur entre des sessions même après l'actualisation ou la recomposition du poste de travail. Persona Management a la capacité de répliquer des profils d'utilisateur vers un magasin de profils distant (partage CIFS) à des intervalles configurables.

Vous pouvez également utiliser une version autonome de Persona Management sur des ordinateurs physiques et des machines virtuelles qui ne sont pas gérés par Horizon 7.

Horizon 7 offre les fonctions de sécurité suivantes (parmi d'autres) :

- Utilisez l'authentification à deux facteurs, telle que RSA SecurID ou RADIUS (Remote Authentication Dial-In User Service) ou des cartes à puce pour ouvrir une session.
- Utilisez des comptes Active Directory créés au préalable lorsque vous approvisionnez des applications et postes de travail distants dans des environnements qui ont des stratégies d'accès en lecture seule pour Active Directory.
- Utilisez le tunneling SSL/TLS pour garantir que toutes les connexions sont complètement cryptées.
- Utilisez VMware High Availability pour garantir le basculement automatique.

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, de hauts niveaux de disponibilité et un contrôle avancé de l'allocation des ressources pour vos applications et postes de travail distants.
- Utilisation de la fonctionnalité Horizon 7 Storage Accelerator pour prendre en charge les connexions d'utilisateurs à des échelles plus grandes avec les mêmes ressources de stockage. Cet Storage Accelerator utilise des fonctions dans la plate-forme vSphere 5 pour créer un cache mémoire hôte de lectures de bloc communes.
- Configuration du Serveur de connexion Horizon pour des connexions de broker entre les utilisateurs finaux et les applications et postes de travail distants auxquels 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.
- Utilisez la fonctionnalité Instant Clone, introduite dans Horizon 7, pour créer rapidement des images de poste de travail qui partagent des disques virtuels et la mémoire avec une image parente. Non seulement les Instant Clones disposent de l'optimisation d'espace des clones liés View Composer, mais ils éliminent également le besoin d'actualiser, de recomposer, de rééquilibrer, ce qui simplifie la gestion des correctifs et des mises à jour du système d'exploitation. Les Instant Clones éliminent complètement la période de maintenance des postes de travail.

Les fonctions suivantes fournissent une administration et une gestion centralisées :

- Utilisation de Microsoft Active Directory pour gérer l'accès à des applications et postes de travail distants et pour gérer des stratégies.
- Utilisation de Persona Management pour simplifier et rationaliser la migration entre postes de travail physiques et postes de travail virtuels.
- Utilisation de la console administrative Web pour gérer des applications et postes de travail distants depuis n'importe quel emplacement.
- Utilisation d'Horizon Administrator pour distribuer et gérer des applications empaquetées avec VMware ThinApp™.
- Utilisation d'un modèle, ou d'une image maître, pour créer et approvisionner rapidement des pools de postes de travail.
- Envoi de mises à jour et de correctifs à des postes de travail virtuels sans affecter les paramètres, les données ou les préférences utilisateur.
- Intégration dans VMware Identity Manager afin que les utilisateurs finaux puissent accéder aux postes de travail distants à l'aide du portail utilisateur sur le Web et utiliser également VMware Identity Manager à partir d'un navigateur d'un poste de travail distant.

- Intégration à Mirage™ et Horizon FLEX™ pour gérer les postes de travail de machine virtuelle locaux afin de déployer et de mettre à jour les applications sur des postes de travail distants de clone complet dédiés sans remplacer les applications installées par l'utilisateur.

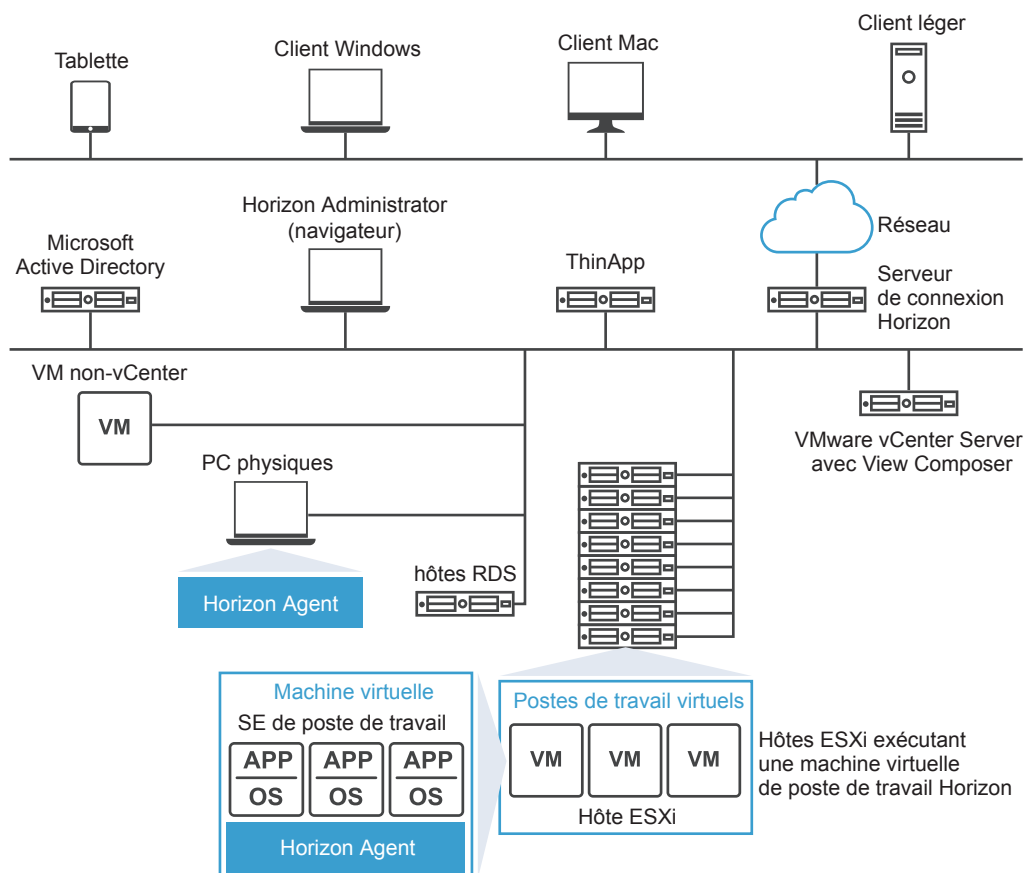
Comment les composants fonctionnent ensemble

Les utilisateurs finaux démarrent Horizon Client pour ouvrir une session sur le Serveur de connexion Horizon. Ce serveur, qui s'intègre à Active Directory de Windows, fournit un accès aux postes de travail distants hébergés sur un serveur VMware vSphere, un PC physique ou un hôte RDS Microsoft. Horizon Client fournit également un accès à des applications publiées sur un hôte RDS Microsoft.

Note Horizon 7 prend en charge des niveaux fonctionnels de domaine des services de domaine Active Directory (AD DS). Pour plus d'informations sur les niveaux fonctionnels de domaine des services AD DS pris en charge, consultez l'article de la base de connaissances de VMware <http://kb.vmware.com/kb/2150351>.

Chiffre 1-2 montre la relation entre les composants principaux d'un déploiement d'Horizon 7.

Chiffre 1-2. Exemple de haut niveau d'un environnement Horizon 7



Périphériques clients

Le principal avantage de l'utilisation d'Horizon 7 est que les applications et les postes de travail distants suivent l'utilisateur final quel que soit le périphérique ou l'emplacement. Les utilisateurs peuvent accéder à leur poste de travail virtuel personnalisé ou leur application distante depuis un ordinateur portable de l'entreprise, leur ordinateur personnel, un périphérique de client léger, un Mac, une tablette ou un téléphone.

Les utilisateurs finaux ouvrent Horizon Client pour afficher leurs applications et postes de travail distants. Les périphériques de client léger utilisent le logiciel Horizon 7 Thin Client et peuvent être configurés pour que la seule application pouvant être lancée par les utilisateurs directement sur le périphérique soit Horizon 7 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 Horizon 7 sur un poste de travail dynamique, vous pouvez utiliser un système d'exploitation plus récent, comme Windows 8.x, sur un matériel de poste de travail plus ancien.

Si vous utilisez la fonctionnalité HTML Access, les utilisateurs finaux peuvent ouvrir un poste de travail dans un navigateur, sans devoir installer d'application cliente sur le système ou le périphérique client.

Serveur de connexion Horizon

Ce service logiciel agit comme un broker pour les connexions client. Le Serveur de connexion Horizon authentifie les utilisateurs via Windows Active Directory et dirige la demande vers la machine virtuelle appropriée, le PC physique ou l'hôte Microsoft RDS.

Le Serveur de connexion fournit les fonctions de gestion suivantes :

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

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

En dehors du pare-feu d'entreprise, dans la zone DMZ, vous pouvez installer et configurer un Serveur de connexion en tant que serveur de sécurité ou installer un dispositif Unified Access Gateway. Des serveurs de sécurité et des dispositifs Unified Access Gateway dans la zone DMZ communiquent avec des Serveurs de connexion dans le pare-feu de l'entreprise. Les serveurs de sécurité et les dispositifs Unified Access Gateway vérifient que le seul trafic d'application et de poste de travail distant qui peut entrer dans le centre de données de l'entreprise est le trafic au nom d'un utilisateur dont l'authentification est renforcée. Les utilisateurs ne peuvent accéder qu'aux ressources dont l'accès leur est autorisé.

Des serveurs de sécurité offrent un sous-ensemble de fonctionnalités et ne doivent pas nécessairement se trouver dans un domaine Active Directory. Vous devez installer le Serveur de connexion dans un serveur Windows Server 2008 R2 ou Windows Server 2012 R2, de préférence sur une machine virtuelle VMware. Pour plus d'informations sur les dispositifs Unified Access Gateway, consultez *Déploiement et configuration d'Unified Access Gateway*.

Important Il est possible de créer une installation d'Horizon 7 sans utiliser le Serveur de connexion. Si vous installez le plug-in de connexion directe d'Horizon 7 Agent sur un poste de travail de machine virtuelle, le client peut se connecter directement à la machine virtuelle. Toutes les fonctionnalités de poste de travail distant, notamment PCoIP, HTML Access, RDP, redirection USB et la gestion de session fonctionnent de la même manière, comme si l'utilisateur s'était connecté via le Serveur de connexion. Pour plus d'informations, consultez *Administration du plug-in Agent Direct-Connection Horizon 7*.

Horizon Client

Le logiciel client permettant d'accéder à des applications et à des postes de travail distants peut s'exécuter sur une tablette, un téléphone, un PC ou un ordinateur portable Windows, Linux ou Mac, un client léger, etc.

Après avoir ouvert une session, les utilisateurs choisissent parmi une liste d'applications et de postes de travail distants 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 ou un autre jeton d'authentification à deux facteurs.

Un administrateur peut configurer Horizon Client pour autoriser les utilisateurs finaux à sélectionner un protocole d'affichage. Les protocoles incluent PCoIP, Blast Extreme et Microsoft RDP pour les postes de travail distants. La vitesse et la qualité d'affichage de PCoIP et Blast Extreme sont équivalentes à celle d'un PC physique.

Les fonctions diffèrent en fonction de l'instance d'Horizon Client que vous utilisez. Ce guide met l'accent sur Horizon Client pour Windows. Les types de client suivants ne sont pas décrits en détail dans ce guide :

- Détails sur Horizon Client pour les tablettes, les clients Linux et les clients Mac. Reportez-vous à la documentation d'Horizon Client à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

- Détails sur HTML Access Web client qui vous permet d'ouvrir un poste de travail distant à l'intérieur d'un navigateur. Aucune application Horizon Client n'est installée sur le système ou le périphérique client. Reportez-vous à la documentation d'Horizon Client à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.
- Divers clients légers et zéro 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 une application cliente officielle et il n'est pas pris en charge comme tel.

Portail Web utilisateur VMware Horizon

Depuis un navigateur Web sur un périphérique client, les utilisateurs finaux peuvent se connecter aux applications et postes de travail distants au moyen du navigateur, démarrer Horizon Client automatiquement s'il est installé ou télécharger le programme d'installation d'Horizon Client.

Lorsque vous ouvrez un navigateur et entrez l'URL d'une instance du Horizon Connection Server, la page Web qui s'affiche contient des liens vers le [site Téléchargements VMware](#) pour télécharger Horizon Client. Toutefois, les liens sur la page Web sont configurables. Par exemple, vous pouvez configurer les liens pour qu'ils pointent sur un serveur Web interne ou vous pouvez limiter quelles versions client sont disponibles sur votre propre Serveur de connexion.

Si vous utilisez la fonctionnalité HTML Access, la page Web affiche également un lien d'accès aux applications et aux postes de travail distants dans un navigateur pris en charge. Avec cette fonctionnalité, aucune application d'Horizon Client n'est installée sur le système ou le périphérique client. Pour plus d'informations, consultez la documentation d'Horizon Client à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Horizon Agent

Vous installez le service Horizon Agent sur l'ensemble des machines virtuelles, des systèmes physiques et des hôtes Microsoft RDS que vous utilisez comme sources pour les applications et les postes de travail distants. Sur des machines virtuelles, cet agent communique avec Horizon Client pour fournir des fonctionnalités comme le contrôle des connexions, l'impression virtuelle, Horizon Persona Management et l'accès à des périphériques USB connectés localement.

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

Vous pouvez installer l'agent avec une option pour l'authentification unique. Avec l'authentification unique, les utilisateurs sont invités à ouvrir une session uniquement lorsqu'ils se connectent au Serveur de connexion Horizon et ne sont pas invités une deuxième fois à se connecter à une application ou à un poste de travail distant.

Horizon Administrator

Cette application Web permet aux administrateurs de configurer le Serveur de connexion Horizon, de déployer et de gérer des applications et des postes de travail distants, de contrôler l'authentification utilisateur et de résoudre des problèmes d'utilisateur final.

Lorsque vous installez une instance du Serveur de connexion, l'application Horizon Administrator est également installée. Cette application permet aux administrateurs de gérer des instances du Serveur de connexion depuis n'importe où sans avoir à installer d'application sur leur ordinateur local.

View Composer

Vous pouvez installer ce service logiciel sur une instance de vCenter Server qui gère des machines virtuelles ou sur un serveur séparé. 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.

Vous pouvez également utiliser View Composer pour créer des batteries de serveurs automatisées d'hôtes RDS Microsoft de clone lié, qui fournissent des applications publiées aux utilisateurs finaux.

Bien que vous puissiez installer View Composer sur son propre hôte serveur, un service View Composer ne peut fonctionner qu'avec une seule instance de vCenter Server. De même, une instance de vCenter Server ne peut être associée qu'à un seul service View Composer.

Important View Composer est un composant facultatif. Si vous prévoyez de provisionner des Instant Clones, vous n'avez pas besoin d'installer View Composer.

vCenter Server

Ce service joue le rôle d'administrateur central des serveurs VMware ESXi qui sont connectés sur un réseau. vCenter Server fournit le point central pour la configuration, le provisionnement et la gestion de machines virtuelles dans le centre de données.

Outre l'utilisation de ces machines virtuelles en tant que sources des pools de postes de travail de machine virtuelle, vous pouvez utiliser des machines virtuelles pour héberger les composants de serveur d'Horizon 7, notamment des instances du Horizon Connection Server, des serveurs Active Directory, des hôtes RDS Microsoft et des instances de vCenter Server.

Vous pouvez installer View Composer sur le même serveur que vCenter Server ou sur un autre serveur. 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 pouvez installer vCenter Server comme un dispositif virtuel VMware ou installer vCenter Server dans un serveur Windows Server 2008 R2 ou un serveur Windows Server 2012 R2, de préférence sur une machine virtuelle VMware.

Intégration et personnalisation d' Horizon 7

Pour améliorer l'efficacité d'Horizon 7 dans votre entreprise, vous pouvez utiliser plusieurs interfaces pour intégrer Horizon 7 à des applications externes ou pour créer des scripts d'administration que vous pouvez exécuter depuis la ligne de commande ou en mode de traitement par lots.

Intégration à d'autres composants

Horizon 7 s'intègre à ces produits VMware.

VMware Cloud on AWS

VMware Cloud on AWS vous permet de créer des centres de données vSphere sur Amazon Web Services. Ces centres de données vSphere intègrent vCenter Server pour gérer votre centre de données, vSAN pour le stockage et VMware NSX pour la mise en réseau. Vous pouvez connecter un centre de données sur site à votre SDDC de Cloud et gérer les deux à partir d'une interface vSphere Client unique. À l'aide de votre compte AWS connecté, vous pouvez accéder à des services AWS, tels qu'EC2 et S3, à partir des machines virtuelles dans votre SDDC. Pour plus d'informations, consultez la documentation d'VMware Cloud on AWS à l'adresse <https://docs.vmware.com/fr/VMware-Cloud-on-AWS/index.html>.

À partir d'Horizon 7 version 7.5, vous pouvez déployer des clones complets d'Horizon 7 sur VMware Cloud on AWS. Par exemple, vous pouvez déployer un environnement Horizon 7 qu'Architecture Cloud Pod utilise entre des centres de données sur site et des instances de VMware Cloud on AWS. Cela permet à Horizon 7 de s'exécuter facilement sur un environnement de Cloud hybride et d'externaliser la gestion de l'infrastructure SDDC à VMware.

VMware Identity Manager

Vous pouvez intégrer VMware Identity Manager à Horizon 7 pour que les responsables informatiques et les utilisateurs profitent des avantages suivants :

- Les utilisateurs disposent d'un accès à la demande à des applications et des postes de travail distants via le portail utilisateur sur le Web qu'ils utilisent pour accéder à des applications SaaS, Web et Windows, avec la même fonction d'authentification unique.

Avec la fonctionnalité d'authentification unique réelle, les utilisateurs qui s'authentifient à l'aide de cartes à puce ou de l'authentification à deux facteurs peuvent accéder à leurs applications et postes de travail distants sans fournir d'informations d'identification Active Directory.

- Les utilisateurs finaux peuvent accéder à VMware Identity Manager sur le Web depuis un poste de travail distant pour les applications dont ils ont besoin.
- Si vous utilisez également HTML Access, les utilisateurs finaux peuvent ouvrir un poste de travail distant dans un navigateur, sans devoir installer d'application cliente sur le système ou le périphérique client.
- Les responsables informatiques peuvent utiliser la console d'administration de type navigateur d'VMware Identity Manager pour surveiller les droits d'accès des utilisateurs et des groupes sur les postes de travail distants.

VMware Mirage et Horizon FLEX

Vous pouvez utiliser Mirage et Horizon FLEX pour déployer et mettre à jour des applications sur des postes de travail distants de clone complet dédié sans remplacer les applications ou les données installées par l'utilisateur.

Mirage fournit une meilleure solution de poste de travail virtuel hors connexion que la fonctionnalité Mode local qui était précédemment incluse dans Horizon 7. Mirage inclut les fonctionnalités de sécurité et de gestion pour les postes de travail hors connexion :

- Chiffre la machine virtuelle installée localement et empêche l'utilisateur de modifier les paramètres de machine virtuelle qui affectent l'intégrité du conteneur sécurisé.
- Fournit des stratégies, notamment l'expiration, disponibles dans VMware Fusion™ Professional et VMware® Player Plus™, qui sont comparables aux stratégies fournies avec la fonctionnalité Mode local précédente. Fusion Pro et Player Plus sont inclus dans Mirage.
- Élimine pour les utilisateurs le besoin de restituer ou d'emprunter leurs postes de travail pour recevoir des mises à jour.
- Permet aux administrateurs d'utiliser la fonctionnalité de superposition, les fonctionnalités de sauvegarde et le portail de fichiers de Mirage.

VMware App Volumes

VMware App Volumes est un système de fourniture d'applications et de gestion des utilisateurs intégré et unifié pour Horizon 7 et d'autres environnements virtuels. Les applications et les données gérées par App Volumes sont conservées dans des VMDK ou VHD spécialisés appelés AppStacks, qui sont liés à chaque session d'utilisateur Windows lors de la connexion ou du redémarrage. Cette stratégie garantit que les applications et les données les plus récentes sont fournies à l'utilisateur. App Volumes fournit également un conteneur différent pour les applications et les

paramètres persistants installés par l'utilisateur appelé volume accessible en écriture, qui est également chargé lors de la connexion ou du redémarrage. Le profil d'utilisateur et les paramètres de stratégie peuvent également être gérés à l'aide de la plate-forme App Volumes.

VMware User Environment Manager

Vous pouvez utiliser la fonctionnalité Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des fonctionnalités de redirection USB, d'impression virtuelle, de redirection du Presse-papiers, de redirection du lecteur client et de protocole d'affichage PCoIP sur des postes de travail distants spécifiques. User Environment Manager permet au service informatique de contrôler les paramètres que les utilisateurs peuvent personnaliser. De plus, il mappe les paramètres d'environnement, tels que les réseaux et les imprimantes basées sur l'emplacement. Avec Stratégies de carte à puce, vous pouvez créer des stratégies qui ne prennent effet que si certaines conditions sont respectées. Par exemple, vous pouvez configurer une stratégie qui désactive la fonctionnalité de redirection du lecteur client si un utilisateur se connecte à un poste de travail distant depuis l'extérieur du réseau d'entreprise.

VMware Unified Access Gateway

Unified Access Gateway fonctionne comme une passerelle sécurisée pour les utilisateurs qui veulent accéder à des applications et des postes de travail distants depuis l'extérieur du pare-feu d'entreprise.

Unified Access Gateway est un dispositif installé dans une zone démilitarisée (DMZ). Utilisez Unified Access Gateway pour vous assurer que le trafic entrant dans le centre de données d'entreprise est effectué uniquement pour le compte d'un utilisateur distant à authentification élevée. Vous pouvez utiliser des dispositifs Unified Access Gateway au lieu de serveurs de sécurité Horizon 7. Pour plus d'informations, consultez la documentation Unified Access Gateway.

Intégration avec un logiciel de conférence vidéo largement répandu

Vous pouvez utiliser ces logiciels de conférence audio et vidéo avec Horizon 7.

Redirection d'URL Flash

La diffusion de contenus Flash directement à partir d'Adobe Media Server vers les points de terminaison client réduit la charge sur l'hôte ESXi du centre de données, supprime les routages supplémentaires via le centre de données et réduit la bande passante nécessaire pour diffuser simultanément des événements vidéo en direct sur plusieurs points de terminaison client.

La fonctionnalité de redirection d'URL Flash utilise un JavaScript incorporé dans le HTML d'une page Web par l'administrateur de celle-ci. Chaque fois qu'un utilisateur de poste de travail virtuel clique sur le lien de l'URL désigné à partir d'une page Web, JavaScript intercepte et redirige le fichier ShockWave (SWF) à partir de la session du poste de travail virtuel au point de terminaison client. Le point de terminaison ouvre alors un projecteur VMware Flash local à l'extérieur de la session de poste de travail virtuel et lance la lecture du flux multimédia en local.

Note Avec la redirection d'URL Flash, le flux de multidiffusion ou de monodiffusion est redirigé vers les périphériques clients qui pourraient être en dehors du pare-feu de votre organisation. Vos clients doivent avoir accès au serveur Web d'Adobe hébergeant le fichier Shockwave Flash (SWF) qui initie les flux de multidiffusion ou de monodiffusion. Si nécessaire, configurez votre pare-feu pour ouvrir les ports appropriés afin de permettre aux périphériques client d'accéder à ce serveur.

Cette fonctionnalité n'est disponible que sur certains types de clients. Pour savoir si cette fonctionnalité est prise en charge sur un type de client particulier, consultez la matrice de prise en charge des fonctionnalités incluse dans le document « Utilisation de VMware Horizon Client » pour le type spécifique de poste de travail ou d'appareil mobile client. Allez sur <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Microsoft Lync 2013

Vous pouvez utiliser un client Microsoft Lync 2013 sur des postes de travail distants pour participer à des appels VoIP (Voice over IP) de communications unifiées et de conversation vidéo avec des périphériques audio et vidéo USB certifiés Lync. Il n'est plus nécessaire de disposer d'un téléphone IP dédié.

Cette architecture requiert l'installation d'un client Microsoft Lync 2013 sur le poste de travail distant et d'un plug-in VDI Microsoft Lync sur le point de terminaison du client Windows 7 ou 8. Les clients peuvent utiliser le client Microsoft Lync 2013 pour les fonctions de présence, de messagerie instantanée, de conférence Web et Microsoft Office.

À chaque appel VoIP ou de conversation vidéo Lync, le plug-in VDI Lync décharge tout le traitement multimédia du serveur de centre de données vers le point de terminaison du client, et code tout le multimédia en codecs audio et vidéo optimisés pour Lync. Cette architecture optimisée est hautement évolutive, entraîne une utilisation réduite de la bande passante réseau et fournit une livraison de données multimédia point à point avec la prise en charge de VoIP et de la vidéo en temps réel haute qualité. Pour

plus d'informations, consultez le Livre blanc sur VMware Horizon 6 et Microsoft Lync 2013, à l'adresse <http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf>.

Note L'enregistrement audio n'est pas encore pris en charge. Cette intégration est prise en charge uniquement avec le protocole d'affichage PCoIP ou Blast Extreme.

Skype Entreprise

Un utilisateur final peut passer des appels audio et vidéo optimisés avec Skype Entreprise à l'intérieur d'un poste de travail virtuel sans affecter négativement l'infrastructure virtuelle et sans surcharger le réseau. Tout le traitement multimédia a lieu sur la machine cliente plutôt que dans le poste de travail virtuel lors des appels audio et vidéo Skype.

Le logiciel Pack de virtualisation pour Skype Entreprise est installé par défaut dans le cadre des programmes d'installation d'Horizon Client pour Windows (4.6 et versions ultérieures), d'Horizon Client pour Linux (4.6 et versions ultérieures) et d'Horizon Client pour Mac (4.7 et versions ultérieures). Un administrateur Horizon doit également installer le pack de virtualisation VMware pour la fonctionnalité Skype Entreprise sur le poste de travail virtuel lors de l'installation d'Horizon Agent. Pour plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7*. Pour configurer Skype Entreprise, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Intégration d' Horizon 7 avec un logiciel de Business Intelligence

Vous pouvez configurer le Serveur de connexion Horizon pour enregistrer des événements dans une base de données Microsoft SQL Server ou Oracle.

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

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

Pour plus d'informations, reportez-vous au document *Intégration d'Horizon 7*.

Vous pouvez également générer des événements Horizon 7 au format Syslog pour qu'un logiciel d'analyse puisse accéder aux données d'événement. Si vous activez la journalisation d'événements basée sur des fichiers, les événements sont accumulés dans un fichier journal local. Si vous spécifiez un partage de fichiers, les fichiers journaux sont déplacés dans ce partage. Pour plus d'informations, reportez-vous au document *Installation d'Horizon 7*.

Utilisation de cmdlets Horizon PowerCLI pour créer des scripts d'administration

Vous pouvez utiliser des cmdlets Horizon PowerCLI avec VMware PowerCLI. Utilisez les cmdlets Horizon PowerCLI pour effectuer diverses tâches d'administration sur les composants Horizon.

Pour plus d'informations sur les cmdlets Horizon PowerCLI, consultez le document *Référence sur les cmdlets VMware PowerCLI* (contenu en anglais).

Pour plus d'informations sur les spécifications de l'API afin de créer des fonctions et des scripts avancés à utiliser avec Horizon PowerCLI, reportez-vous à la référence d'API View dans le [Centre pour développeurs VMware](#).

Pour plus d'informations sur les exemples de scripts que vous pouvez utiliser pour créer vos propres scripts Horizon PowerCLI, reportez-vous à la [Communauté Horizon PowerCLI sur GitHub](#).

Vous pouvez utiliser les applets de commande d'Horizon PowerCLI pour effectuer diverses tâches d'administration sur des composants Horizon 7.

- Créez et mettez à jour des pools de postes de travail.
- Configurez plusieurs étiquettes de réseau pour augmenter considérablement le nombre d'adresses IP affectées à des machines virtuelles dans un pool.
- Ajoutez des ressources de centre de données à une machine virtuelle complète ou à un pool de clone lié.
- Effectuez des opérations de rééquilibrage, d'actualisation ou de recomposition sur des postes de travail de clone lié.
- Échantillonnez l'utilisation de postes de travail ou de pools de postes de travail spécifiques dans le temps.
- Interrogez la base de données des événements.
- Interrogez l'état des services.

Modification des données de configuration LDAP dans Horizon 7

Lorsque vous utilisez Horizon Administrator pour modifier la configuration d'Horizon 7, les données LDAP appropriées dans le référentiel sont mises à jour. Le Serveur de connexion Horizon stocke ses informations de configuration dans un référentiel compatible avec LDAP. Par exemple, si vous ajoutez un pool de postes de travail, le Serveur de connexion stocke des informations sur les utilisateurs, les groupes d'utilisateurs et les droits dans LDAP.

Vous pouvez utiliser des outils de ligne de commande VMware et Microsoft pour exporter et importer des données de configuration LDAP dans des fichiers LDIF (LDAP Data Interchange Format) depuis et vers Horizon 7. Ces commandes sont destinées aux administrateurs avancés qui souhaitent utiliser des scripts pour mettre à jour des données de configuration sans utiliser Horizon Administrator ou Horizon PowerCLI.

Vous pouvez utiliser des fichiers LDIF pour effectuer plusieurs tâches.

- Transférer des données de configuration entre des instances du Serveur de connexion.
- Définir un grand nombre d'objets Horizon 7, tels que des pools de postes de travail, et ajouter ces objets à vos instances du Serveur de connexion sans utiliser Horizon Administrator ou Horizon PowerCLI.
- Sauvegarder une configuration pour que vous puissiez restaurer l'état d'une instance du Serveur de connexion.

Pour plus d'informations, reportez-vous au document *Intégration d'Horizon 7*.

Utilisation de la commande vdmadmin

Vous pouvez utiliser l'interface de ligne de commande `vdmadmin` pour effectuer diverses tâches d'administration sur une instance du Serveur de connexion. Vous pouvez utiliser `vdmadmin` pour effectuer des tâches d'administration qui ne sont pas possibles depuis l'interface utilisateur d'Horizon Administrator ou qui doivent être exécutées automatiquement depuis des scripts.

Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.

Planification d'une expérience d'utilisateur riche

2

Horizon 7 fournit l'environnement de poste de travail familial et personnalisé que tous les utilisateurs finaux attendent. Par exemple, sur certains systèmes client, 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.

Horizon 7 inclut plusieurs fonctions que vous pouvez vouloir rendre disponibles à vos utilisateurs finaux. Avant de décider quelles fonctions utiliser, vous devez comprendre les limites et les restrictions de chaque fonction.

Ce chapitre contient les rubriques suivantes :

- [Matrice de prise en charge des fonctionnalités pour Horizon Agent](#)
- [Choisir un protocole d'affichage](#)
- [Utilisation d'applications publiées](#)
- [Utilisation d'Horizon Persona Management pour conserver des données et des paramètres utilisateur](#)
- [Utilisation de périphériques USB avec des applications et postes de travail distants](#)
- [Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones](#)
- [Utilisation des applications graphiques 3D](#)
- [Diffusion multimédia sur un poste de travail distant](#)
- [Impression à partir d'un poste de travail distant](#)
- [Utilisation de l'authentification unique pour la connexion](#)
- [Écrans et résolution d'écran](#)

Matrice de prise en charge des fonctionnalités pour Horizon Agent

Lorsque vous décidez du protocole d'affichage et des fonctionnalités à rendre disponibles pour les utilisateurs finaux, utilisez les informations suivantes pour identifier les systèmes d'exploitation d'agent (application et poste de travail distants) prenant en charge la fonctionnalité.

Les types et éditions des systèmes d'exploitation client pris en charge dépendent de la version de Windows. Pour obtenir les mises à jour de la liste de systèmes d'exploitation Windows 10 pris en charge, consultez l'article de la base de connaissances de VMware <http://kb.vmware.com/kb/2149393>. Pour les systèmes d'exploitation Windows autres que Windows 10, consultez l'article de la base de connaissances de VMware <http://kb.vmware.com/kb/2150295>.

Pour voir la liste des fonctionnalités d'expérience à distance prises en charge sur les systèmes d'exploitation Windows sur lesquels Horizon Agent est installé, consultez l'article <http://kb.vmware.com/kb/2150305> de la base de connaissances de VMware.

Note Pour plus d'informations sur les fonctionnalités prises en charge sur les différents types de périphériques clients, reportez-vous à la documentation de Horizon Client à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

En outre, plusieurs partenaires VMware offrent des périphériques clients léger et zéro pour les déploiements d'Horizon 7. Les fonctions disponibles pour chaque périphérique de client léger ou zéro 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 clients légers et zéro, reportez-vous au [Guide de compatibilité VMware](#), disponible sur le site Web de VMware.

Choisir un protocole d'affichage

Un protocole d'affichage fournit aux utilisateurs finaux une interface graphique sur une application ou un poste de travail distant qui réside dans le centre de données. En fonction du type de périphérique client que vous possédez, vous pouvez choisir entre Blast Extreme et PCoIP (PC-over-IP), fourni par VMware, ou Microsoft RDP (Remote Desktop Protocol).

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.

Note Pour certains types de clients, les protocoles d'affichage à distance PCoIP et RDP ne sont pas utilisés. Par exemple, si vous utilisez le client HTML Access, disponible avec la fonctionnalité HTML Access, le protocole Blast Extreme est utilisé plutôt que PCoIP ou RDP. De même, si vous utilisez un poste de travail Linux distant, Blast Extreme est utilisé.

VMware Blast Extreme

Optimisé pour le cloud mobile, VMware Blast Extreme prend en charge la plus large gamme de périphériques clients compatibles avec H.264. De tous les protocoles d'affichage, VMware Blast est celui qui offre la consommation de CPU la plus faible pour une durée de vie de la batterie plus longue sur les périphériques mobiles. VMware Blast Extreme peut compenser une augmentation de la latence ou une réduction de la bande passante et peut exploiter les transports réseau TCP et UDP.

Le protocole d'affichage VMware Blast peut être utilisé pour des applications publiées et pour des postes de travail distants qui utilisent des machines virtuelles ou des postes de travail à session partagée sur un hôte RDS. L'hôte RDS peut être une machine physique ou une machine virtuelle. Le protocole d'affichage VMware Blast ne fonctionne pas sur un ordinateur physique mono-utilisateur, à l'exception de l'édition Entreprise de Windows 10 RS4 et versions ultérieures.

Note Les films et les applications TV ne sont pas pris en charge pour les ordinateurs physiques exécutant Windows 10 RS4.

Fonctionnalités de VMware Blast Extreme

Les fonctionnalités clés de VMware Blast Extreme incluent les éléments suivants :

- Les utilisateurs à l'extérieur du pare-feu d'entreprise peuvent utiliser ce protocole avec le réseau privé virtuel (VPN) d'entreprise ou établir une connexion chiffrée et sécurisée avec un serveur de sécurité ou un dispositif Access Point dans la zone DMZ de l'entreprise.
- Le cryptage AES (Advanced Encryption Standard) 128 bits est pris en charge et est activé par défaut. Vous pouvez toutefois modifier le chiffrement de clé de cryptage sur AES-256.
- Les connexions à partir de tous les types d'appareils clients.
- Les contrôles d'optimisation pour la réduction de l'utilisation de bande passante sur les réseaux LAN et WAN.
- Les compteurs de performances affichés à l'aide de PerfMon sur les agents Windows fournissent une représentation précise de l'état actuel du système qui s'actualise également à un rythme constant pour les éléments suivants :
 - Session Blast
 - Imagerie
 - Audio
 - CDR
 - USB : les compteurs USB affichés à l'aide de PerfMon sur les agents Windows sont valides si le trafic USB est configuré pour utiliser VVC (VMware Virtual Channel).
 - Skype Entreprise : les compteurs sont uniquement destinés au trafic de contrôle.
 - Presse-papiers
 - RTAV
 - Fonctionnalités de redirection de port série et de scanner
 - Impression virtuelle
 - HTML5 MMR
 - Windows Media MMR : les compteurs de performances s'affichent uniquement si vous avez configuré cette fonctionnalité pour utiliser VVC (VMware Virtual Channel).

- Continuité du réseau pendant une perte momentanée de réseau sur les clients Windows.
- Les couleurs 32 bits sont prises en charge pour les affichages virtuels.
- Les polices ClearType sont prises en charge.
- Redirection audio avec réglage dynamique de la qualité audio pour les réseaux locaux et les réseaux étendus.
- Audio/vidéo en temps réel pour l'utilisation de webcams et de microphones sur certains types de clients.
- Copier-coller de texte et, sur certains clients, d'images entre le système d'exploitation client et un poste de données distant ou une application publiée. Pour d'autres types de clients, seul le copier-coller de texte brut est pris en charge. Vous ne pouvez pas copier et coller des objets système comme des dossiers et des fichiers entre des systèmes.
- Plusieurs écrans sont pris en charge pour certains types de client. Sur certains clients, il est possible d'utiliser jusqu'à quatre moniteurs avec une résolution pouvant atteindre 2 560 x 1 600 par écran ou jusqu'à trois moniteurs avec une résolution 4K (3 840 x 2 160) pour les postes de travail distants Windows 7 dont l'option Aero est désactivée. La rotation d'affichage et l'ajustement automatique sont également pris en charge.

Lorsque la fonctionnalité 3D est activée, jusqu'à deux moniteurs peuvent être pris en charge avec une résolution pouvant atteindre 1 920 x 1 200 ou un moniteur avec une résolution 4K (3 840 x 2 160).

- La redirection USB est prise en charge pour certains types de client.
- La redirection MMR est prise en charge pour certains systèmes d'exploitation clients Windows et certains systèmes d'exploitation de postes de travail distants (sur lesquels Horizon Agent est installé).
- Les connexions à des machines physiques sans moniteur sont prises en charge avec les cartes graphiques NVIDIA. Pour de meilleures performances, utilisez une carte graphique prenant en charge le codage H.264.

Si vous disposez d'un GPU discret de complément et d'un GPU intégré, le système d'exploitation peut être défini par défaut sur le GPU intégré. Pour résoudre ce problème, vous pouvez désactiver ou supprimer le périphérique dans le Gestionnaire de périphériques. Si le problème persiste, vous pouvez installer le pilote graphique WDDM pour le GPU intégré ou désactiver le GPU intégré dans le BIOS système. Consultez la documentation de votre système pour savoir comment désactiver le GPU intégré.



Attention La désactivation du GPU intégré peut entraîner une perte d'accès future à des fonctionnalités, telles que l'accès de la console à la configuration BIOS ou au chargeur de démarrage NT.

Pour plus d'informations sur les périphériques clients prenant en charge des fonctionnalités VMware Blast Extreme spécifiques, accédez à <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Wake-on-LAN

Wake-on-LAN est pris en charge pour les machines physiques avec l'édition Entreprise de Windows 10 RS4 et versions ultérieures. Avec cette fonctionnalité, les utilisateurs peuvent réveiller des machines physiques lors de la connexion avec Horizon Connection Server. La fonctionnalité Wake-on-LAN présente les conditions préalables suivantes :

- Wake-on-LAN (WoL) n'est pris en charge que dans les environnements IPv4.
- La machine physique doit être configurée pour se réveiller lors de la réception de paquets Wake-on-LAN lorsque Wake-on-LAN est activé dans les paramètres du BIOS, ainsi que dans les paramètres de carte réseau.
- Le port de destination 9 est utilisé pour les paquets WoL provenant du Serveur de connexion.
- Les paquets WoL sont des paquets de diffusion dirigés par adresse IP qui doivent être en mesure d'atteindre Horizon Agent lorsqu'ils sont envoyés depuis Horizon Connection Server. Wake-on-LAN fonctionne dans les scénarios suivants :
 - Le Serveur de connexion et Horizon Agent sur la machine physique se trouvent sur le même sous-réseau dans un environnement LAN.
 - Tous les routeurs entre le Serveur de connexion et Horizon Agent sont configurés pour autoriser le paquet de diffusion dirigé par adresse IP pour le sous-réseau cible de la machine physique que vous voulez réveiller.

Note La fonctionnalité Wake-on-LAN ne prend pas en charge les pools d'attribution flottante d'un agent Windows 10 physique. Le paquet WoL n'est envoyé qu'à des pools d'attribution dédiée autorisés avec un utilisateur particulier.

Paramètres de système d'exploitation client recommandés

1 Go ou plus de RAM et un CPU double sont recommandés pour lire des vidéos haute définition, en mode plein écran ou formatées à 720p ou plus. Pour utiliser vDGA (Virtual Dedicated Graphics Acceleration) pour les applications graphiques intensives telles que les applications CAO, une capacité de 4 Go de RAM est requise.

Exigences de qualité vidéo

Vidéo formatée à 480p

Vous pouvez lire une vidéo à 480p ou moins à des résolutions natives lorsque le poste de travail distant dispose d'une seule CPU virtuelle. Si vous voulez lire la vidéo en Flash haute définition ou en mode plein écran, le poste de travail requiert un CPU virtuel double. Même avec un poste de travail de CPU virtuel double, les vidéos formatées à 360p lues en mode plein écran peuvent être décalées par rapport au son, en particulier sur les clients Windows.

Vidéo formatée à 720p

Vous pouvez lire une vidéo à 720p à des résolutions natives lorsque le poste de travail distant dispose d'une CPU virtuelle double. Les performances peuvent être affectées si vous lisez des vidéos à 720p en haute définition ou en mode plein écran.

Vidéo formatée à 1 080p

Si le poste de travail distant dispose d'une CPU virtuelle double, vous pouvez lire une vidéo formatée à 1 080p, bien que la taille d'écran du lecteur multimédia puisse nécessiter une diminution.

rendu 3D

Vous pouvez configurer des postes de travail distants pour utiliser des graphiques à accélération matérielle ou logicielle. La fonctionnalité graphique à accélération logicielle vous permet d'exécuter des applications DirectX 9 et OpenGL 2.1 sans nécessiter de GPU physique. Les fonctionnalités graphiques à accélération matérielle permettent aux machines virtuelles de partager les GPU physiques sur un hôte vSphere ou de dédier un GPU physique à un seul poste de travail virtuel.

Pour les applications 3D, deux écrans maximum sont pris en charge et la résolution d'écran maximale est 1 920 x 1 200. Le système d'exploitation invité sur les postes de travail distants doit être Windows 7 ou version ultérieure.

Pour plus d'informations sur les fonctionnalités 3D, reportez-vous à [Utilisation des applications graphiques 3D](#).

Exigences matérielles des systèmes client

Pour plus d'informations sur les exigences en termes de processeur et de mémoire pour le type spécifique de poste de travail ou de périphérique client mobile, accédez à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

PCoIP

PCoIP (PC-over-IP) offre une expérience de poste de travail optimisée pour fournir une application publiée ou l'intégralité de l'environnement d'un poste de travail distant, y compris des applications, des images, du contenu audio et vidéo, à un grand nombre d'utilisateurs sur le réseau local ou sur le réseau étendu. PCoIP peut compenser une augmentation de la latence ou une réduction de la bande passante pour garantir que les utilisateurs peuvent rester productifs quelles que soient les conditions du réseau.

Le protocole d'affichage PCoIP peut être utilisé pour des applications publiées et des postes de travail distants qui utilisent des machines virtuelles, des machines physiques qui contiennent des cartes d'hôte Teradici ou des postes de travail à session partagée sur un hôte RDS.

Fonctions de PCoIP

Les fonctions clés de PCoIP incluent :

- Les utilisateurs à l'extérieur du pare-feu d'entreprise peuvent utiliser ce protocole avec le réseau privé virtuel (VPN) de votre entreprise ou établir une connexion chiffrée et sécurisée avec un serveur de sécurité ou un dispositif Access Point dans la zone DMZ de l'entreprise.
- Le cryptage AES (Advanced Encryption Standard) 128 bits est pris en charge et est activé par défaut. Vous pouvez toutefois modifier le chiffrement de clé de cryptage sur AES-256.
- Les connexions à partir de tous les types d'appareils clients.
- Les contrôles d'optimisation pour la réduction de l'utilisation de bande passante sur les réseaux LAN et WAN.
- Les couleurs 32 bits sont prises en charge pour les affichages virtuels.
- Les polices ClearType sont prises en charge.
- Redirection audio avec réglage dynamique de la qualité audio pour les réseaux locaux et les réseaux étendus.
- Audio/vidéo en temps réel pour l'utilisation de webcams et de microphones sur certains types de clients.
- Copier-coller de texte et, sur certains clients, d'images entre le système d'exploitation client et un poste de données distant ou une application publiée. Pour d'autres types de clients, seul le copier-coller de texte brut est pris en charge. Vous ne pouvez pas copier et coller des objets système comme des dossiers et des fichiers entre des systèmes.
- Plusieurs écrans sont pris en charge pour certains types de client. Sur certains clients, il est possible d'utiliser jusqu'à 4 moniteurs avec une résolution pouvant atteindre 2 560 x 1 600 par écran ou jusqu'à 3 moniteurs de résolution 4K (3 840 x 2 160) pour les postes de travail à distance Windows 7 dont l'option Aero est désactivée. La rotation d'affichage et l'ajustement automatique sont également pris en charge.

Lorsque la fonction 3D est activée, jusqu'à deux moniteurs peuvent être pris en charge avec une résolution allant jusqu'à 1 920 x 1 200 ou un moniteur avec une résolution 4K (3 840 x 2 160).

- La redirection USB est prise en charge pour certains types de client.
- La redirection MMR est prise en charge pour certains systèmes d'exploitation clients Windows et certains systèmes d'exploitation de postes de travail distants (sur lesquels Horizon Agent est installé).

Pour plus d'informations sur les systèmes d'exploitation de postes de travail qui prennent en charge des fonctionnalités PCoIP spécifiques, reportez-vous à [Matrice de prise en charge des fonctionnalités pour Horizon Agent](#).

Pour plus d'informations sur les périphériques client prenant en charge des fonctions PCoIP spécifiques, allez sur <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Paramètres de système d'exploitation client recommandés

1 Go ou plus de RAM et un CPU double sont recommandés pour lire des vidéos haute définition, en mode plein écran ou formatées à 720p ou plus. Pour utiliser vDGA (Virtual Dedicated Graphics Acceleration) pour les applications graphiques intensives telles que les applications CAO, une capacité de 4 Go de RAM est requise.

Exigences de qualité vidéo

Vidéo formatée à 480p	Vous pouvez lire une vidéo à 480p ou moins à des résolutions natives lorsque le poste de travail distant dispose d'une seule CPU virtuelle. Si vous voulez lire la vidéo en Flash haute définition ou en mode plein écran, le poste de travail requiert un CPU virtuel double. Même avec un poste de travail de CPU virtuel double, les vidéos formatées à 360p lues en mode plein écran peuvent être décalées par rapport au son, en particulier sur les clients Windows.
Vidéo formatée à 720p	Vous pouvez lire une vidéo à 720p à des résolutions natives lorsque le poste de travail distant dispose d'une CPU virtuelle double. Les performances peuvent être affectées si vous lisez des vidéos à 720p en haute définition ou en mode plein écran.
Vidéo formatée à 1 080p	Si le poste de travail distant dispose d'une CPU virtuelle double, vous pouvez lire une vidéo formatée à 1 080p, bien que la taille d'écran du lecteur multimédia puisse nécessiter une diminution.
Rendu 3D	Vous pouvez configurer des postes de travail distants pour utiliser des graphiques à accélération matérielle ou logicielle. La fonctionnalité graphique à accélération logicielle vous permet d'exécuter des applications DirectX 9 et OpenGL 2.1 sans nécessiter de GPU physique. Les fonctionnalités graphiques à accélération matérielle permettent aux machines virtuelles de partager les GPU (graphical processing unit) physiques sur un hôte vSphere ou de dédier une GPU physique à un seul poste de travail de machine virtuelle.

Pour les applications 3D, jusqu'à deux moniteurs sont pris en charge et la résolution d'écran maximale est de 1 920 x 1 200. Le système d'exploitation invité sur les postes de travail de machines virtuelles doivent exécuter Windows 7 ou version ultérieure.

Pour plus d'informations sur les fonctionnalités 3D, reportez-vous à [Utilisation des applications graphiques 3D](#).

Exigences matérielles des systèmes client

Pour plus d'informations sur les exigences de processeur et de mémoire, reportez-vous au document « Utilisation de VMware Horizon Client » pour le type spécifique de poste de travail ou d'appareil mobile client. Allez sur <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Microsoft RDP

Remote Desktop Protocol est le même protocole multicanal que de nombreuses personnes utilisent déjà pour accéder à leur ordinateur professionnel depuis leur ordinateur à domicile. La Connexion Bureau à distance Microsoft utilise RDP pour transmettre des données.

Microsoft RDP est un protocole d'affichage pris en charge par les postes de travail distants utilisant les machines virtuelles, les machines physiques ou les postes de travail en session partagée sur un hôte RDS. (Seuls les protocoles d'affichage PCoIP et VMware Blast sont pris en charge pour les applications publiées.) Microsoft RDP fournit les fonctions suivantes :

- RDP 7 offre une prise en charge de plusieurs écrans, pour 16 écrans maximum.
- Vous pouvez copier et coller du texte et des objets système, tels que des dossiers et des fichiers, entre le système local et le poste de travail distant.
- Les couleurs 32 bits sont prises en charge pour les affichages virtuels.
- RDP prend en charge le cryptage 128 bits.
- Les utilisateurs à l'extérieur du pare-feu d'entreprise peuvent utiliser ce protocole avec le réseau privé virtuel (VPN) de votre entreprise, ou bien ils peuvent établir une connexion cryptée et sécurisée avec un serveur de sécurité View dans la zone DMZ de l'entreprise.

Pour prendre en charge les connexions TLSv1.1 et TLSv1.2 à Windows 7 et Windows Server 2008 R2, vous devez appliquer le correctif Microsoft KB3080079.

Exigences matérielles des systèmes client

Pour plus d'informations sur les exigences de processeur et de mémoire, reportez-vous au document « Utilisation de VMware Horizon Client » pour le type spécifique de système client. Allez sur <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Note Les périphériques 3.x clients mobiles utilisent uniquement le protocole d'affichage PCoIP. Les clients 4.x clients mobiles utilisent uniquement le protocole d'affichage PCoIP ou VMware Blast.

Utilisation d'applications publiées

Vous pouvez utiliser Horizon Client pour accéder en toute sécurité aux applications Windows publiées, en plus des postes de travail distants.

Avec cette fonctionnalité, après le lancement d'Horizon Client et l'ouverture de session sur un serveur Horizon 7, les utilisateurs voient toutes les applications publiées qu'ils ont le droit d'utiliser, en plus des postes de travail distants. La sélection d'une application ouvre une fenêtre pour cette application sur le périphérique client local, et l'application se présente et se comporte comme si elle était installée localement.

Par exemple, sur un ordinateur client Windows, si vous réduisez la fenêtre d'application, un élément pour cette application subsiste dans la barre des tâches et il se présente exactement comme s'il avait été installé sur l'ordinateur Windows local. Vous pouvez également créer un raccourci pour l'application qui apparaîtra sur votre poste de travail client, tout comme les raccourcis des applications localement installées.

Le déploiement d'applications publiées de cette manière peut être préférable au déploiement de postes de travail distants complets dans les conditions suivantes :

- Si une application est configurée avec une architecture à plusieurs niveaux, dans laquelle les composants fonctionnent mieux s'ils sont géographiquement rapprochés, l'utilisation d'applications publiées constitue une bonne solution.

Par exemple, lorsqu'un utilisateur accède à une base de données à distance, si de grandes quantités de données doivent être transmises sur le réseau étendu, les performances s'en trouvent généralement affectées. Avec les applications publiées, toutes les parties de l'application peuvent résider dans le même centre de données que la base de données, ce trafic est donc isolé et seules les mises à jour d'écran sont envoyées sur le réseau étendu.

- À partir d'un appareil mobile, l'accès à une application individuelle est plus simple que l'ouverture d'un poste de travail Windows distant et l'accès à l'application.

Pour utiliser cette fonctionnalité, vous installez les applications sur un hôte Microsoft RDS. À cet égard, les applications publiées par Horizon 7 fonctionnent de la même façon que les autres solutions d'accès à distance aux applications. Les applications publiées par Horizon 7 sont fournies à l'aide du protocole d'affichage Blast Extreme ou PCoIP, pour une expérience utilisateur optimisée.

Utilisation d'Horizon Persona Management pour conserver des données et des paramètres utilisateur

Vous pouvez utiliser Horizon Persona Management avec des postes de travail distants et avec des ordinateurs physiques et des machines virtuelles qui ne sont pas gérés par Horizon 7. Persona Management conserve les modifications que les utilisateurs apportent à leurs profils. Les profils d'utilisateur comportent plusieurs informations générées par l'utilisateur.

- Des données spécifiques de l'utilisateur et des paramètres de poste de travail, ce qui permet à l'utilisateur de voir toujours la même apparence de poste de travail quel que soit le poste de travail sur lequel il ouvre une session.
- Des données et des paramètres d'application. Par exemple, ces paramètres permettent à des applications de se souvenir de la position des barres d'outils et des préférences.
- Des entrées de registre de Windows configurées par des applications utilisateur.

Pour faciliter ces capacités, Persona Management requiert que le stockage sur un partage CIFS soit égal ou supérieur à la taille du profil local de l'utilisateur.

Minimisation des durées d'ouverture et de fermeture de session

Persona Management minimise le temps nécessaire pour ouvrir et fermer une session sur des postes de travail. Lors de l'ouverture de session, par défaut, Horizon 7 télécharge uniquement les fichiers dont Windows a besoin, tels que les fichiers de registre utilisateur. Horizon 7 récupère les modifications récentes dans le profil sur le poste de travail distant et les copie sur le référentiel distant à des intervalles réguliers.

Avec Persona Management, vous pouvez éviter d'apporter des modifications à Active Directory pour avoir un profil géré. Pour configurer Gestion de persona, vous spécifiez un référentiel central, sans modifier les propriétés de l'utilisateur dans Active Directory. Avec ce référentiel central, vous pouvez gérer le profil d'un utilisateur dans un environnement sans affecter les machines physiques sur lesquelles les utilisateurs peuvent également ouvrir une session.

Avec Persona Management, si vous provisionnez des postes de travail avec des applications VMware ThinApp, les données de sandbox ThinApp peuvent également être stockées dans le profil d'utilisateur. Ces données peuvent suivre l'utilisateur mais n'affectent pas significativement les heures d'ouverture de session. Cette stratégie fournit une meilleure protection contre la perte ou la corruption de données.

Options de configuration

Vous pouvez configurer des personas Horizon 7 à plusieurs niveaux : un poste de travail distant unique, un pool de postes de travail, une UO ou tous les postes de travail distants de votre déploiement. Vous pouvez également utiliser une version autonome de Persona Management sur des ordinateurs physiques et des machines virtuelles qui ne sont pas gérés par Horizon 7.

En définissant des stratégies de groupe (des GPO), vous disposez d'un contrôle granulaire des fichiers et des dossiers à inclure dans un persona. Vous pouvez spécifier si vous voulez inclure le dossier des paramètres locaux, quels fichiers se chargent lors de la connexion, quels fichiers se téléchargent en arrière-plan une fois l'utilisateur connecté et quels fichiers dans le persona d'un utilisateur sont gérés avec la fonctionnalité de profils itinérants Windows au lieu de Persona Management.

Comme avec les profils itinérants de Windows, vous pouvez configurer la redirection de dossiers. Vous pouvez rediriger les dossiers suivants vers un partage de réseau.

Contacts	Mes documents	Jeux sauvegardés
Cookies	Ma musique	Recherches
Poste de travail	Mes images	Menu Démarrer
Téléchargements	Mes vidéos	Éléments de démarrage
Favoris	Voisinage réseau	Modèles
Historique	Voisinage imprimante	Fichiers Internet temporaires
Liens	Éléments récents	

Limites

Persona Management présente les limites et restrictions suivantes :

- Cette fonctionnalité n'est pas prise en charge sur les pools de postes de travail de clone instantané.
- Vous devez disposer d'une licence Horizon 7 qui inclut le composant Persona Management.
- Persona Management requiert un partage CIFS (Common Internet File System).
- Cette fonctionnalité n'est pas prise en charge pour une utilisation avec un disque persistant sur les pools de postes de travail de clone lié Windows 10.

Utilisation de périphériques USB avec des applications et postes de travail distants

Les administrateurs peuvent configurer l'utilisation des périphériques USB, tels que des clés USB, des caméras, des périphériques VoIP (voice-over-IP) et des imprimantes, à partir d'un poste de travail virtuel. Cette fonctionnalité est appelée redirection USB. Un poste de travail virtuel peut recevoir jusqu'à 128 périphériques USB.

Vous pouvez également rediriger certains périphériques USB connectés localement pour les utiliser dans des applications et des postes de travail publiés. Pour plus d'informations sur les types spécifiques de périphériques pris en charge, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Lorsque vous utilisez cette fonctionnalité dans des pools de postes de travail qui sont déployés sur des machines mono-utilisateur, la plupart des périphériques USB raccordés au système client local deviennent disponibles à partir d'un poste de travail distant. Vous pouvez même vous connecter à un iPad et le gérer depuis un poste de travail distant. Par exemple, vous pouvez synchroniser votre iPad avec l'application iTunes installée sur votre poste de travail distant. Sur certains périphériques clients, comme les ordinateurs Windows et Mac, les périphériques USB sont répertoriés dans un menu d'Horizon Client. Vous utilisez le menu pour connecter et déconnecter les périphériques.

Dans la plupart des cas, vous ne pouvez pas utiliser simultanément un périphérique USB sur votre système client et sur votre poste de travail distant. Seuls quelques types de périphériques USB peuvent être partagés entre un poste de travail distant et l'ordinateur local. Ces périphériques sont notamment les lecteurs de carte à puce et les périphériques d'interface utilisateur, tels que les claviers et les dispositifs de pointage.

Les administrateurs peuvent spécifier les types de périphériques USB auxquels les utilisateurs finaux sont autorisés à se connecter. Pour les périphériques composites qui contiennent plusieurs types de périphériques, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage, sur certains systèmes clients, les administrateurs peuvent diviser le périphérique pour qu'un périphérique (par exemple, le périphérique d'entrée vidéo) soit autorisé mais pas l'autre (par exemple, le périphérique de stockage).

La fonctionnalité de redirection USB n'est disponible que sur certains types de clients. Pour savoir si cette fonctionnalité est prise en charge sur un client particulier, consultez la matrice de prise en charge des fonctionnalités incluse dans le document d'installation et de configuration d'Horizon Client pour ce client.

Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones

La fonctionnalité Audio/vidéo en temps réel vous permet d'utiliser une webcam ou un microphone du système client local sur un poste de travail distant ou une application publiée. La fonctionnalité Audio/vidéo en temps réel est compatible avec les applications de conférence standard et les applications vidéo basées sur navigateur. Elle prend en charge les webcams standards, les périphériques audio USB et l'entrée audio analogique.

Les utilisateurs finaux peuvent utiliser Skype, Webex, Google Hangouts et d'autres applications de conférence en ligne sur leurs postes de travail distants. Cette fonctionnalité redirige les données vidéo et audio vers la machine de l'agent avec une bande passante beaucoup plus faible que celle utilisée par la redirection USB. Avec l'Audio/Vidéo en temps réel, les images de webcam et l'entrée audio sont codées sur le client, puis sont envoyées à la machine de l'agent. Sur la machine de l'agent, une webcam et microphone virtuels peuvent décoder et lire le flux de données, que l'application tierce peut utiliser.

Aucune configuration spéciale n'est requise, bien que les administrateurs puissent définir des stratégies de groupe côté agent et les clés de registre pour configurer la fréquence et la résolution d'images, ou désactiver la fonctionnalité. Par défaut, la résolution est de 320 x 240 pixels à 15 images par seconde. Le cas échéant, les administrateurs peuvent également utiliser les paramètres de configuration côté client afin de définir la webcam ou le périphérique audio préférés.

Note Cette fonctionnalité n'est disponible que sur certains types de clients. Pour savoir si cette fonctionnalité est prise en charge sur un type de client particulier, consultez la matrice de prise en charge des fonctionnalités incluse dans le document d'installation et de configuration pour le type spécifique de poste de travail ou de périphérique client mobile.

Utilisation des applications graphiques 3D

Les fonctionnalités graphiques accélérées par le matériel et par les logiciels disponibles dans le protocole d'affichage Blast Extreme ou PCoIP permettent aux utilisateurs de postes de travail distants d'exécuter des applications 3D allant de Google Earth à de la CAO et d'autres applications consommant beaucoup de ressources graphiques.

NVIDIA GRID vGPU (accélération matérielle GPU partagée)

Disponible dans vSphere 6.0 et versions ultérieures, cette fonctionnalité permet de partager une GPU (Graphical Processing Unit) physique sur un hôte ESXi entre plusieurs machines virtuelles. Utilisez cette fonctionnalité si vous avez besoin de graphiques de workstation haut de gamme accélérés par le matériel.

GPU multi-utilisateur AMD utilisant vDGA

Disponible avec vSphere 6.0 et versions ultérieures, cette fonctionnalité permet à plusieurs machines virtuelles de partager un GPU AMD en faisant apparaître le GPU sous la forme de plusieurs périphériques de relais PCI. Cette fonctionnalité offre des profils 3D souples accélérés par le matériel allant des exécutants de tâches 3D légères aux utilisateurs graphiques expérimentés de stations de travail haut de gamme.

vDGA (Virtual Dedicated Graphics Acceleration)

Disponible dans vSphere 5.5 Update 2 et versions ultérieures, cette fonctionnalité dédie un seul GPU physique sur un hôte ESXi à une machine virtuelle unique. Utilisez cette fonctionnalité si vous avez besoin de graphiques de workstation haut de gamme accélérés par le matériel.

Note Certaines cartes Intel vDGA requièrent une version spécifique de vSphere 6. Consultez la liste de compatibilité matérielle VMware à l'adresse <http://www.vmware.com/resources/compatibility/search.php>. De plus, pour Intel vDGA, le GPU intégré Intel est utilisé à la place de GPU discrets, comme c'est le cas avec d'autres fournisseurs.

vSGA (Virtual Shared Graphics Acceleration)

Disponible dans vSphere 5.5 Update 2 et versions ultérieures, cette fonctionnalité permet à plusieurs machines virtuelles de partager les GPU physiques sur des hôtes ESXi. Vous pouvez utiliser des applications 3D pour la conception, la modélisation et le multimédia.

Soft 3D

Les graphiques à accélération logicielle, disponibles dans vSphere 5.5 Update 2 et versions ultérieures, vous permettent d'exécuter des applications DirectX 9 et OpenGL 2.1 sans nécessiter de GPU physique. Utilisez cette fonctionnalité pour les applications 3D moins exigeantes, comme les thèmes Windows Aero, Microsoft Office 2010 et Google Earth.

NVIDIA GRID vGPU et vDGA sont maintenant également pris en charge dans les applications publiées exécutées sur des hôtes RDS Microsoft.

Important Pour plus d'informations sur les divers choix et exigences du rendu 3D, consultez le [livre blanc VMware](#) sur l'accélération graphique, le [Guide de déploiement NVIDIA GRID vGPU de VMware Horizon 6.1](#) et le [Guide de l'utilisateur de NVIDIA GRID vGPU](#).

Diffusion multimédia sur un poste de travail distant

La fonctionnalité Windows Media MMR (redirection multimédia), pour postes de travail et clients Windows 7 et Windows 8/8.1, permet la lecture haute-fidélité sur des ordinateurs clients Windows lorsque les fichiers multimédias sont diffusés en continu sur un poste de travail distant.

Avec MMR, le flux multimédia est traité, c'est-à-dire décodé, sur le système client Windows. Le système client effectue la lecture du contenu multimédia, déchargeant ainsi la demande sur l'hôte ESXi. Les formats multimédias pris en charge sur le Lecteur multimédia Windows sont pris en charge ; par exemple : M4V ; MOV ; MP4 ; WMP ; MPEG-4 Part 2 ; WMV 7, 8 et 9 ; WMA ; AVI ; ACE ; MP3 ; WAV.

Note Vous devez ajouter le port MMR en tant qu'exception à votre logiciel de pare-feu. Le port par défaut pour MMR est 9427.

Impression à partir d'un poste de travail distant

La fonctionnalité d'impression virtuelle permet aux utilisateurs finaux sur certains systèmes clients d'utiliser des imprimantes locales ou réseau à partir d'un poste de travail distant sans avoir à installer de pilotes d'imprimante supplémentaires sur le système d'exploitation du poste de travail distant. La fonctionnalité d'impression basée sur l'emplacement vous permet de mapper des postes de travail distants à l'imprimante la plus proche du périphérique client de point de terminaison.

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

La redirection de l'imprimante locale est conçue pour les cas d'utilisation suivants :

- Des imprimantes connectées directement à des ports USB ou série sur le périphérique client
- Des imprimantes spécialisées, telles que des imprimantes de code-barres et d'étiquettes, connectées au client
- Des imprimantes réseau sur un réseau distant qui ne sont pas adressables à partir de la session virtuelle.

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

L'impression basée sur l'emplacement permet aux services informatiques de mapper des postes de travail distants à l'imprimante la plus proche du périphérique client de point de terminaison. Par exemple, lorsqu'un médecin passe de chambre en chambre dans un hôpital, chaque fois qu'il imprime un document, le travail d'impression est envoyé à l'imprimante la plus proche. Pour utiliser cette fonction, il n'est pas nécessaire que les bons pilotes d'imprimante soient installés sur le poste de travail distant.

Note Ces fonctionnalités d'impression ne sont disponibles que sur certains types de clients. Pour savoir si une fonctionnalité d'impression est prise en charge sur un type de client particulier, consultez la matrice de prise en charge des fonctionnalités incluse dans le guide d'installation et de configuration pour le type spécifique de poste de travail ou de périphérique client mobile. Accédez à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Utilisation de l'authentification unique pour la connexion

La fonctionnalité d'authentification unique permet aux utilisateurs finaux de n'entrer qu'une seule fois les informations d'identification de connexion Active Directory.

Si vous n'utilisez pas la fonction d'authentification unique, les utilisateurs finaux doivent ouvrir une session deux fois. Ils sont d'abord invités à fournir leurs informations d'identification Active Directory pour se connecter au Serveur de connexion Horizon, puis à leur poste de travail distant. 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.

Pour les postes de travail distants, cette fonctionnalité inclut une bibliothèque de liens dynamiques de fournisseur d'informations d'identification.

authentification unique réelle

Avec la fonctionnalité d'authentification unique réelle, les utilisateurs n'ont plus à fournir les informations d'identification Active Directory. Lorsque des utilisateurs sont connectés à VMware Identity Manager avec une méthode non-AD (par exemple, authentification RSA SecurID ou RADIUS), ils ne sont plus invités à entrer également leurs informations d'identification Active Directory pour utiliser une application ou un poste de travail distant.

Si un utilisateur s'authentifie avec des cartes à puce ou des informations d'identification Active Directory, la fonctionnalité d'authentification unique réelle n'est pas nécessaire, mais vous pouvez configurer l'authentification unique réelle pour qu'elle soit utilisée même dans ce cas. Ensuite, les informations d'identification AD que l'utilisateur fournit sont ignorées et l'authentification unique réelle est utilisée.

L'authentification unique réelle fonctionne en générant un certificat unique de courte durée pour le processus de connexion de Windows. Vous devez configurer une autorité de certification, si vous n'en avez pas déjà une, et un serveur d'inscription de certificat afin de générer des certificats de courte durée au nom de l'utilisateur. Vous installez le serveur d'inscription en exécutant le programme d'installation du Serveur de connexion et en sélectionnant l'option Serveur d'inscription.

L'authentification unique réelle sépare l'authentification (en validant l'identité d'un utilisateur) de l'accès (comme à un poste de travail ou une application Windows). Les informations d'identification d'utilisateur sont sécurisées par un certificat numérique. Aucun mot de passe n'est archivé ou transféré dans le centre de données. Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.

Écrans et résolution d'écran

Vous pouvez étendre un poste de travail distant sur plusieurs moniteurs. Si vous disposez d'un moniteur haute résolution, vous pouvez afficher l'application ou le poste de travail distant en pleine résolution.

Vous pouvez sélectionner le mode Tous les moniteurs pour afficher un poste de travail distant sur plusieurs moniteurs. Si vous utilisez le mode Tous les moniteurs et que vous cliquez sur le bouton Réduire, lorsque vous agrandissez la fenêtre, celle-ci repasse en mode Tous les moniteurs. De la même façon, si vous utilisez le mode Plein écran et que vous réduisez la fenêtre, lorsque vous agrandissez la fenêtre, celle-ci repasse en mode Plein écran sur un écran.

Utilisation de tous les moniteurs dans une configuration à plusieurs moniteurs

Quel que soit le protocole d'affichage, vous pouvez utiliser plusieurs moniteurs avec un poste de travail distant. Lorsque vous configurez Horizon Client pour qu'il utilise tous les moniteurs, si vous agrandissez la fenêtre d'une application, la fenêtre passe en plein écran sur le seul moniteur qui la contient.

Horizon Client prend en charge les configurations de moniteur suivantes :

- Si vous utilisez deux moniteurs, il n'est pas nécessaire qu'ils soient dans le même mode. Par exemple, si vous utilisez un ordinateur portable connecté à un moniteur externe, le moniteur externe peut être en mode portrait ou en mode paysage.

- Les moniteurs peuvent être placés côte à côte, associés deux par deux ou empilés verticalement, seulement si vous utilisez deux moniteurs et si la hauteur totale est inférieure à 4 096 pixels.
- Pour utiliser la fonction de rendu 3D, vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP. Vous pouvez utiliser deux moniteurs maximum, avec une résolution maximale de 1 920 x 1 200. Pour une résolution de 4K (3 840 x 2 160), un seul moniteur est pris en charge.
- Avec le protocole d'affichage VMware Blast ou PCoIP, la résolution d'écran de poste de travail distant de 4K (3 840 x 2 160) est prise en charge. Le nombre d'écrans 4K pris en charge dépend de la version matérielle de la machine virtuelle de poste de travail et de la version de Windows.

Version du matériel	Version Windows	Nombre d'écrans 4K pris en charge
10 (compatible avec ESXi 5.5.x)	7, 8, 8.x, 10	1
11 (compatible avec ESXi 6.0)	7 (fonction de rendu 3D désactivée et Windows Aero désactivé)	3
11	7 (fonction de rendu 3D activée)	1
11	8, 8.x, 10	1
13 ou 14	8, 8.x, 10	3
13 ou 14	8, 8.x, 10 (fonction de rendu 3D activée)	1

- Si vous disposez de Microsoft RDP 7, vous pouvez utiliser un maximum de 16 moniteurs pour afficher un poste de travail distant.
- Si vous utilisez le protocole d'affichage Microsoft RDP, Connexion Bureau à distance Microsoft (RDC) 6.0 ou version ultérieure doit être installé sur le poste de travail distant.

Utilisation d'un écran dans une configuration à plusieurs écrans

Si vous disposez de plusieurs moniteurs, mais que vous voulez qu'Horizon Client utilise uniquement l'un d'entre eux, vous pouvez choisir qu'une fenêtre de poste de travail distant s'ouvre dans un mode qui n'est pas Tous les moniteurs. Par défaut, la fenêtre est ouverte sur le moniteur principal. Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Utilisation du mode haute résolution

Sur certains types de clients, lorsque vous utilisez le protocole d'affichage VMware Blast ou PCoIP, Horizon Client prend également en charge les résolutions très élevées pour les systèmes clients avec des affichages haute résolution. L'option pour activer le mode haute résolution s'affiche uniquement si le système client prend en charge les affichages haute résolution.

Le codage du matériel est activé par défaut une fois que vGPU est configuré dans la machine virtuelle. Le codage du matériel est activé pour toutes les configurations à plusieurs moniteurs prises en charge, à ceci près que les profils vGPU utilisant moins de 1 Go de mémoire vidéo utiliseront le décodeur logiciel en raison de restrictions de mémoire NVENC. Reportez-vous à la section *NVENC nécessite au moins 1 Go de mémoire tampon de trame* dans <https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vmware/index.html>

Gestion de pools de postes de travail et d'applications depuis un emplacement central

3

Vous pouvez créer des pools qui comprennent un, des centaines ou des milliers de postes de travail distants. Comme source de postes de travail, vous pouvez utiliser des machines virtuelles, des machines physiques et des hôtes des services Bureau à distance Windows (RDS). Créez une machine virtuelle unique comme image de base pour permettre à Horizon 7 de générer un pool de postes de travail distants à partir de cette image. Vous pouvez également créer des pools d'applications qui permettent aux utilisateurs d'accéder à distance à des applications.

Ce chapitre contient les rubriques suivantes :

- [Avantages des pools de postes de travail](#)
- [Avantages des pools d'applications](#)
- [Réduction et gestion des exigences de stockage](#)
- [Approvisionnement d'application](#)
- [Utilisation de GPO Active Directory pour gérer des utilisateurs et des postes de travail](#)

Avantages des pools de postes de travail

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

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

- Un système physique comme un PC de poste de travail physique.
- Une machine virtuelle hébergée sur un hôte ESXi et gérée par vCenter Server
- Une machine virtuelle s'exécutant sur une plate-forme de virtualisation autre que vCenter Server qui prend en charge Horizon Agent.
- Un poste de travail basé sur une session sur un hôte RDS. Pour plus d'informations sur la création de pools de postes de travail à partir d'un hôte RDS, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

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

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

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

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

Pools d'affectation dédiée

Un poste de travail distant particulier est attribué à chaque utilisateur. Les utilisateurs reviennent au même poste de travail à chaque ouverture de session. Les pools d'affectation dédiée requièrent une relation poste de travail/utilisateur un-à-un. Par exemple, un pool de 100 postes de travail est nécessaire pour un groupe de 100 utilisateurs.

Pools d'affectation flottante

L'utilisation de pools d'affectation flottante vous permet également de créer un pool de postes de travail qui peut être utilisé par des groupes d'utilisateurs. Par exemple, un pool de 100 postes de travail peut être utilisé par 300 utilisateurs s'ils travaillent en groupe de 100 utilisateurs à la fois. Le poste de travail distant est supprimé et recréé après chaque utilisation de façon facultative, offrant ainsi un environnement hautement contrôlé.

Avantages des pools d'applications

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

Les pools d'applications offrent plusieurs avantages importants :

- **Accessibilité**

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

- **Indépendance des périphériques**

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

- **Contrôle d'accès**

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

- **Déploiement accéléré**

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

- **Gérabilité**

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

- **Sécurité et conformité réglementaire**

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

- **Réduction du coût**

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

Réduction et gestion des exigences de stockage

Le déploiement de postes de travail sur des machines virtuelles gérées par vCenter Server offre toutes les performances de stockage qui étaient auparavant réservées aux serveurs virtualisés. L'utilisation d'Instant Clones ou de clones liés View Composer en tant que machines de poste de travail améliore les économies de stockage, car toutes les machines virtuelles dans un pool partagent un disque virtuel avec une image de base.

- **Gestion du stockage avec vSphere**

vSphere vous permet de virtualiser des volumes de disque et des systèmes de fichiers pour que vous puissiez gérer et configurer le stockage sans vous soucier de l'emplacement de stockage physique des données.

- **Utilisation de VMware vSAN pour le stockage hautes performances et la gestion basée sur les stratégies**

VMware VMware vSAN est une couche de stockage définie par logiciel, disponible avec vSphere 5.5 Update 2 ou une version ultérieure, qui virtualise les disques de stockage physiques disponibles sur un cluster d'hôtes vSphere. Vous spécifiez une seule banque de données lors de la création d'un pool de postes de travail automatisé ou d'une batterie de serveurs automatisée, et les différents composants, comme les fichiers, réplicas, données utilisateur et fichiers de système d'exploitation de la machine virtuelle sont placés sur des disques SSD ou des disques durs appropriés.

- **Utilisation de Virtual Volumes pour un stockage centré sur une machine virtuelle et une gestion basée sur la stratégie**

Avec Virtual Volumes (VVols), disponible dans vSphere 6.0 ou version ultérieure, une machine virtuelle individuelle, pas la banque de données, devient une unité de gestion de stockage. Le matériel de stockage obtient le contrôle sur le contenu, la disposition et la gestion d'un disque virtuel.

- **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 %.

- **Réduction des exigences de stockage avec des Instant Clones**

La fonctionnalité d'Instant Clones exploite la technologie vSphere vmFork (disponible avec vSphere 6.0U1 et versions ultérieures) afin de suspendre une image de base en cours d'exécution, ou une machine virtuelle parente, et de créer et personnaliser rapidement un pool de postes de travail virtuels.

Gestion du stockage avec vSphere

vSphere vous permet de virtualiser des volumes de disque et des systèmes de fichiers pour que vous puissiez gérer et configurer le stockage sans vous soucier de l'emplacement de stockage physique des données.

Les baies Fibre Channel SAN, iSCSI SAN et NAS sont des technologies de stockage largement utilisées et prises en charge par vSphere pour répondre à différents besoins de stockage de centre de données. Les baies de stockage sont connectées à et partagées entre des groupes de serveurs via des réseaux de stockage. Cette configuration permet l'agrégation des ressources de stockage et fournit plus de flexibilité dans leur approvisionnement aux machines virtuelles.

Fonctionnalités compatibles avec vSphere 5.5 Update 2 ou version ultérieure

Avec vSphere 5.5 Update 2 ou version ultérieure, vous pouvez utiliser vSAN, qui virtualise les disques SSD et les disques durs locaux physiques disponibles sur les hôtes ESXi dans une banque de données unique partagée par tous les hôtes d'un cluster. vSAN fournit un stockage haute performance avec une gestion basée sur la stratégie, de sorte que vous pouvez spécifier une seule banque de données lors de la création d'un pool de postes de travail, et que les différents composants, comme les fichiers, les réplicas, les données utilisateur et les fichiers du système d'exploitation de la machine virtuelle sont placés sur des disques SSD ou sur des disques durs appropriés.

vSAN vous permet également de gérer le stockage et les performances du stockage de la machine virtuelle et en utilisant des profils de stratégie de stockage. Si la stratégie devient non conforme en raison d'un hôte, d'un disque, d'une panne réseau ou de changements de charge de travail, vSAN reconfigure les données des machines virtuelles affectées et optimise l'utilisation des ressources dans le cluster. Vous pouvez déployer un pool de postes de travail sur un cluster contenant jusqu'à 20 hôtes ESXi.

Tout en prenant en charge les fonctionnalités VMware qui nécessitent un stockage partagé, tel que VMware HA, vMotion et DRS, vSAN élimine le besoin d'un stockage partagé externe et simplifie les activités de configuration de stockage et d'approvisionnement de machines virtuelles.

Important La fonctionnalité vSAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performances. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie. Pour plus d'informations sur vSAN dans vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware vSAN*.

Note vSAN est compatible avec la fonctionnalité View Storage Accelerator, mais pas avec la fonctionnalité de format de disque à optimisation d'espace qui récupère de l'espace disque en effaçant et en réduisant les disques.

Avec vSphere 5.5 Update 2 ou version ultérieure, vous pouvez utiliser les fonctionnalités suivantes :

- Avec la fonction View Storage Accelerator, vous pouvez configurer des hôtes ESXi pour mettre en cache des données de disque de machine virtuelle.

L'utilisation de ce cache de lecture basé sur le contenu (CBRC) peut réduire le nombre d'opérations d'E/S par seconde et améliorer les performances au cours des tempêtes de démarrage, lorsque plusieurs machines démarrent et exécutent des analyses antivirus en même temps. Au lieu de lire tout le système d'exploitation depuis le système de stockage encore et encore, un hôte peut lire des blocs de données communes depuis le cache.

- Si des postes de travail distants utilisent le format de disque à optimisation d'espace disponible avec vSphere 5.1 et version ultérieure, les données périmées ou supprimées dans un système d'exploitation invité sont automatiquement récupérées avec un processus d'effacement et de réduction.

- Les disques de réplica doivent être stockés sur des magasins de données VMFS5 ou supérieur ou sur des magasins de données NFS. Si vous stockez les réplicas sur une version VMFS antérieure à VMFS5, un cluster peut contenir 8 hôtes au maximum. Les disques du système d'exploitation et les disques persistants peuvent être stockés sur des magasins de données NFS ou VMFS.

Fonctionnalités compatibles avec vSphere 6.0 ou version ultérieure

Avec vSphere 6.0 ou version ultérieure, vous pouvez utiliser Virtual Volumes (VVols). Cette fonctionnalité mappe les disques virtuels et leurs dérivés, clones, snapshots et réplicas, directement à des objets nommés volumes virtuels sur un système de stockage. Ce mappage permet à vSphere de décharger des opérations de stockage intensives telles que la prise de snapshots, le clonage et la réplication sur le système de stockage.

La fonctionnalité Virtual Volumes vous permet également de gérer le stockage et les performances du stockage de la machine virtuelle dans vSphere. Ces profils de stratégie de stockage déterminent les services de stockage utilisés au niveau de chaque machine virtuelle. Ce type de provisionnement granulaire augmente le degré d'utilisation de la capacité. Vous pouvez déployer un pool de postes de travail sur un cluster contenant jusqu'à 32 hôtes ESXi.

Note Virtual Volumes est compatible avec la fonctionnalité View Storage Accelerator, mais pas avec la fonctionnalité de format de disque à optimisation d'espace qui récupère de l'espace disque en effaçant et en réduisant les disques.

Note Les Instant Clones ne prennent pas en charge Virtual Volumes.

Utilisation de VMware vSAN pour le stockage hautes performances et la gestion basée sur les stratégies

VMware VMware vSAN est une couche de stockage définie par logiciel, disponible avec vSphere 5.5 Update 2 ou une version ultérieure, qui virtualise les disques de stockage physiques disponibles sur un cluster d'hôtes vSphere. Vous spécifiez une seule banque de données lors de la création d'un pool de postes de travail automatisé ou d'une batterie de serveurs automatisée, et les différents composants, comme les fichiers, réplicas, données utilisateur et fichiers de système d'exploitation de la machine virtuelle sont placés sur des disques SSD ou des disques durs appropriés.

vSAN met en œuvre une approche à la gestion du stockage basée sur les stratégies. Lorsque vous utilisez vSAN, Horizon 7 définit les exigences du stockage de la machine virtuelle, comme la capacité, les performances et la disponibilité, sous la forme de profils de stratégie de stockage par défaut et les déploie automatiquement pour des postes de travail virtuels sur vCenter Server. Les stratégies sont appliquées automatiquement et individuellement par disque (objets vSAN) et conservées tout au long du cycle de vie du poste de travail virtuel. Le stockage est approvisionné et configuré automatiquement selon les stratégies affectées. Vous pouvez modifier ces stratégies dans vCenter. Horizon crée des stratégies vSAN pour des pools de postes de travail de clone lié, des pools de postes de travail d'Instant Clone, des pools de postes de travail de clone complet ou une batterie de serveurs automatisée par cluster Horizon.

Vous pouvez activer le chiffrement d'un cluster vSAN afin de chiffrer toutes les données au repos dans la banque de données vSAN. Le chiffrement vSAN est disponible avec vSAN 6.6 ou version ultérieure. Pour plus d'informations sur le chiffrement d'un cluster vSAN, consultez la documentation de *VMware vSAN*.

Chaque machine virtuelle maintient sa stratégie, quel que soit son emplacement physique dans le cluster. Si la stratégie devient non conforme en raison d'une panne d'hôte, de disque, de réseau ou à la suite de modifications dans la charge de travail, vSAN reconfigure les données des machines virtuelles affectées et des équilibrages de charge pour satisfaire les stratégies de chaque machine virtuelle.

Tout en prenant en charge les fonctionnalités VMware qui nécessitent un stockage partagé, tel que VMware HA, vMotion et DRS, vSAN élimine le besoin d'une infrastructure de stockage partagé externe et simplifie les activités de configuration de stockage et d'approvisionnement de machines virtuelles.

Important La fonctionnalité vSAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport à la fonctionnalité disponible avec vSphere 5.5 Update 2. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie. De plus, VMware vSAN 6.0 prend en charge une architecture entièrement flash qui utilise des périphériques basés sur le flash pour la mise en cache et le stockage persistant.

Exigences et limitations

La fonctionnalité vSAN présente les limitations suivantes lors d'une utilisation dans un déploiement Horizon 7 :

- Cette version ne prend pas en charge l'utilisation de la fonctionnalité de format de disque à optimisation d'espace d'Horizon 7 qui récupère de l'espace en effaçant et en réduisant les disques.
- vSAN ne prend pas en charge la fonctionnalité VCAI (View Composer Array Integration), car vSAN n'utilise pas les périphériques NAS.

Note vSAN est compatible avec la fonctionnalité View Storage Accelerator. vSAN fournit une couche de mise en cache sur les disques SSD, et la fonctionnalité View Storage Accelerator fournit un cache basé sur le contenu qui réduit les opérations d'E/S et améliore les performances lors des tempêtes de démarrage.

La fonctionnalité vSAN a les exigences suivantes :

- vSphere 5.5 Update 2 ou une version ultérieure.
- Matériel approprié. Par exemple, VMware recommande une carte réseau 10 Gbits/s et au moins un disque SSD et un disque dur pour chaque nœud constituant la capacité. Pour obtenir des informations spécifiques, reportez-vous au [Guide de compatibilité VMware](#).
- Un cluster d'au moins trois hôtes ESXi. Il vous faut suffisamment d'hôtes ESXi pour recevoir votre installation, même si vous utilisez deux hôtes ESXi avec un cluster étendu vSAN. Pour plus d'informations, reportez-vous au document *Configurations maximales pour vSphere*.
- Capacité de disque SSD correspondant au moins à 10 pour cent de la capacité du disque dur.

- Suffisamment de disques durs pour recevoir votre installation. Ne dépassez pas le seuil de 75 % de l'utilisation sur un disque magnétique.

Pour plus d'informations sur les conditions requises de vSAN, reportez-vous à « Utilisation de vSAN » dans le document *Stockage de vSphere 5.5 Update 2*. Pour vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware vSAN*. Pour obtenir des instructions sur le dimensionnement et la conception des composants clés des infrastructures de postes de travail virtuels Horizon 7 pour VMware vSAN, consultez le livre blanc à l'adresse <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

Utilisation de Virtual Volumes pour un stockage centré sur une machine virtuelle et une gestion basée sur la stratégie

Avec Virtual Volumes (VVols), disponible dans vSphere 6.0 ou version ultérieure, une machine virtuelle individuelle, pas la banque de données, devient une unité de gestion de stockage. Le matériel de stockage obtient le contrôle sur le contenu, la disposition et la gestion d'un disque virtuel.

Avec Virtual Volumes, des conteneurs de stockage abstraits remplacent les volumes de stockage traditionnels basés sur des LUN ou des partages NFS. Virtual Volumes mappe les disques virtuels et leurs dérivés, clones, snapshots et réplicas, directement à des objets nommés volumes virtuels sur un système de stockage. Avec ce mappage, vSphere peut décharger des opérations de stockage intensives telles que la prise de snapshots, le clonage et la réplication sur le système de stockage. Par exemple, une opération de clonage qui mettait précédemment une heure s'exécute dorénavant en seulement quelques minutes à l'aide de Virtual Volumes.

Important L'un des principaux avantages de Virtual Volumes est la possibilité d'utiliser la gestion basée sur des stratégies de logiciel (SPBM). Cependant, pour cette version, Horizon 7 ne crée pas les stratégies de stockage granulaire que crée vSAN. En revanche, vous pouvez définir une stratégie de stockage global par défaut dans vCenter Server qui s'appliquera à toutes les banques de données Virtual Volume.

Virtual Volumes offre les avantages suivants :

- Virtual Volumes gère la décharge d'un certain nombre d'opérations sur le matériel de stockage. Ces opérations incluent la prise de snapshots, le clonage et Storage DRS.
- Avec Virtual Volumes, vous pouvez utiliser des services de stockage avancés qui incluent notamment la réplication, le chiffrement, la déduplication et la compression sur des disques virtuels individuels.
- Virtual Volumes prend en charge diverses fonctionnalités vSphere telles que vMotion, Storage vMotion, snapshots, clones liés, Flash Read Cache et DRS.
- Vous pouvez utiliser Virtual Volumes avec des baies de stockage qui prennent en charge la technologie VAAI (vSphere APIs for Array Integration).

Exigences et limitations

La fonctionnalité Virtual Volumes présente les limitations suivantes lors d'une utilisation dans un déploiement Horizon 7 :

- Cette version ne prend pas en charge l'utilisation de la fonctionnalité de format de disque à optimisation d'espace d'Horizon 7 qui récupère de l'espace en effaçant et en réduisant les disques.
- Virtual Volumes ne prend pas en charge l'utilisation de View Composer Array Integration (VCAI).
- Les banques de données Virtual Volumes ne sont pas prises en charge pour les pools de postes de travail d'Instant Clone.

Note Virtual Volumes est compatible avec la fonctionnalité View Storage Accelerator. vSAN fournit une couche de mise en cache sur les disques SSD, et la fonctionnalité View Storage Accelerator fournit un cache basé sur le contenu qui réduit les opérations d'E/S et améliore les performances lors des tempêtes de démarrage.

La fonctionnalité Virtual Volumes impose la configuration requise suivante :

- vSphere 6.0 ou version ultérieure.
- Matériel approprié. Certains fournisseurs de stockage sont responsables de l'apport de fournisseurs de stockage pouvant s'intégrer avec vSphere et apporter la prise en charge de Virtual Volumes. Chaque fournisseur de stockage doit être certifié par VMware et correctement déployé.
- Tous les disques virtuels que vous provisionnez sur une banque de données virtuelle doivent être un multiple entier de 1 Mo.

Virtual Volumes est une fonctionnalité vSphere 6.0. Pour plus d'informations sur les conditions requises, la fonctionnalité, l'arrière-plan et la configuration requise pour l'installation, reportez-vous aux rubriques sur Virtual Volumes dans le document *vSphere Storage*.

Réduction des exigences de stockage avec View Composer

Comme View Composer crée des images de poste de travail qui partagent des disques virtuels avec une image de base, vous pouvez réduire la capacité de stockage requise de 50 à 90 %.

View Composer utilise une image de base, ou une machine virtuelle parente, et crée un pool de 2,000 machines virtuelles de clone lié maximum. Chaque clone lié agit comme un poste de travail indépendant, avec un nom d'hôte et une adresse IP uniques. Pourtant le clone lié requiert beaucoup moins de stockage.

Clones réplica et liés sur le même magasin de données

Lorsque vous créez un pool de postes de travail de clone lié ou une batterie de serveurs d'hôtes RDS Microsoft, un clone complet est d'abord créé à partir de la machine virtuelle parente. Le clone complet, ou réplica, et ses clones liés peuvent être placés sur le même magasin de données, ou LUN (Logical Unit Number). Si nécessaire, vous pouvez utiliser la fonctionnalité de rééquilibrage pour déplacer le réplica et les pools de postes de travail de clone lié d'un LUN vers un autre ou des pools de postes de travail de clone lié vers une banque de données vSAN ou d'une banque de données vSAN vers un LUN.

Clones réplica et liés sur des magasins de données différents

Vous pouvez également placer des réplicas et des clones liés View Composer sur des magasins de données séparés avec différentes caractéristiques de performance. Par exemple, vous pouvez stocker les machines virtuelles réplicas sur un disque électronique. Les disques électroniques ont une capacité de stockage faible et des performances de lecture élevées. En général, ils prennent en charge des dizaines de milliers d'E/S par seconde (IOPS). Vous pouvez stocker des clones liés sur des magasins de données sur des supports de rotation traditionnels. Ces disques sont moins performants, mais ils sont moins chers et fournissent une plus grande capacité de stockage. Ils sont donc adaptés pour le stockage des nombreux clones liés d'un pool volumineux. Les configurations de stockage étagées peuvent être utilisées pour gérer de façon rentable les scénarios d'E/S intensifs tels que le redémarrage simultané de plusieurs machines virtuelles ou l'exécution d'analyses antivirus programmées.

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

Si vous utilisez des banques de données vSAN ou des banques de données Virtual Volumes, vous ne pouvez pas sélectionner manuellement différentes banques de données pour les réplicas ou clones liés. Comme les fonctionnalités de vSAN et de Virtual Volumes placent automatiquement les objets sur le type de disque approprié et mettent en cache toutes les opérations d'E/S, il n'est pas nécessaire d'utiliser la hiérarchisation des réplicas pour les banques de données vSAN et Virtual Volumes.

Disques supprimables pour fichiers d'échange et temporaires

Lorsque vous créez un pool de clone lié ou une batterie de serveurs, vous pouvez également configurer de façon facultative un disque virtuel supprimable séparé pour stocker les fichiers d'échange et temporaires du système d'exploitation invité qui sont générés au cours de sessions utilisateur. Quand une machine virtuelle est mise hors tension, le disque pouvant être supprimé est supprimé. L'utilisation de disques supprimables peut économiser de l'espace de stockage en ralentissant la croissance des clones liés et en réduisant l'espace utilisé par les machines virtuelles désactivées.

Disques persistants pour postes de travail dédiés

Lorsque vous créez des pools de postes de travail d'affectation dédiée, View Composer peut également créer de façon facultative un disque virtuel persistant séparé pour chaque poste de travail virtuel. Le profil Windows et les données d'application de l'utilisateur final sont enregistrés sur le disque persistant. Lorsqu'un clone lié est actualisé, recomposé ou rééquilibré, le contenu du disque virtuel persistant est conservé. VMware vous recommande de conserver les disques persistants View Composer sur un magasin de données séparé. Vous pouvez ensuite sauvegarder l'ensemble de LUN qui conserve les disques persistants.

Magasins de données locaux pour postes de travail flottants sans état

Des postes de travail de clone lié peuvent être stockés sur des magasins de données locaux, qui sont des disques de secours internes sur des hôtes ESXi. Le stockage local offre des avantages tels que du matériel peu coûteux, un approvisionnement de machine virtuelle rapide, des opérations d'alimentation haute performance et une gestion simple. Toutefois, l'utilisation du stockage local limite les options de configuration de l'infrastructure vSphere qui sont à votre disposition. L'utilisation du stockage local est utile dans certains environnements, mais n'est pas appropriée dans d'autres.

Note Les limites décrites dans cette section ne s'appliquent pas aux banques de données vSAN qui utilisent également les disques de stockage local, mais nécessitent un matériel spécifique, comme décrit dans la section précédente à propos de vSAN.

L'utilisation de banques de données locales fonctionnera mieux si les postes de travail distants de votre environnement sont sans état. Par exemple, vous pouvez utiliser des magasins de données locaux si vous déployez des kiosques ou des stations de classe et de formation sans état.

Si vous prévoyez de profiter des avantages du stockage local, vous devez examiner attentivement les limites suivantes :

- Vous ne pouvez pas utiliser VMotion, VMware High Availability (HA) ou vSphere Distributed Resource Scheduler (DRS).
- Vous ne pouvez pas utiliser l'opération de rééquilibrage View Composer pour équilibrer les charges de machines virtuelles sur un pool de ressources.
- Vous ne pouvez pas stocker un réplica View Composer et des clones liés sur des magasins de données séparés et, en fait, VMware recommande de les stocker sur le même volume.

Si vous gérez l'utilisation du disque local en contrôlant le nombre de machines virtuelles et leur croissance du disque, et si vous utilisez des affectations flottantes et effectuez régulièrement des opérations d'actualisation et de suppression, vous pouvez réussir à déployer des clones liés sur des magasins de données locaux.

Pour plus d'informations, consultez le chapitre sur la création de pools de postes de travail dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Réduction des exigences de stockage avec des Instant Clones

La fonctionnalité d'Instant Clones exploite la technologie vSphere vmFork (disponible avec vSphere 6.0U1 et versions ultérieures) afin de suspendre une image de base en cours d'exécution, ou une machine virtuelle parente, et de créer et personnaliser rapidement un pool de postes de travail virtuels.

Les Instant Clones partagent les disques virtuels avec la machine virtuelle parente au moment de la création, mais également la mémoire du parent. Chaque Instant Clone agit comme un poste de travail indépendant, avec un nom d'hôte et une adresse IP uniques. Pourtant l'Instant Clone requiert beaucoup moins de stockage. Les Instant Clones réduisent la capacité de stockage requise de 50 à 90 %. Les exigences de mémoire globale sont également réduites au moment de la création des clones. Pour plus d'informations sur les exigences de stockage et les limites de dimensionnement, consultez l'article de la base de connaissances de VMware <https://kb.vmware.com/kb/2150348>.

À partir d'Horizon 7 version 7.8, les Instant Clones prennent en charge les fonctionnalités TRIM et UNMAP de vSphere pour les banques de données vSAN.

Réplica et Instant Clones sur la même banque de données

Lorsque vous créez un pool de postes de travail d'Instant Clone, un clone complet est d'abord créé depuis la machine virtuelle maître. Le clone complet, ou réplica, et ses clones liés peuvent être placés sur le même magasin de données, ou LUN (Logical Unit Number).

Réplica et Instant Clones sur des banques de données différentes

Vous pouvez également placer des réplicas d'Instant Clone et des Instant Clones sur des banques de données séparées avec différentes caractéristiques de performance. Par exemple, vous pouvez stocker les machines virtuelles réplicas sur un disque électronique. Les disques électroniques ont une capacité de stockage faible et des performances de lecture élevées. En général, ils prennent en charge des dizaines de milliers d'E/S par seconde (IOPS).

Vous pouvez stocker des Instant Clones sur des banques de données sur des supports de rotation traditionnels. Ces disques sont moins performants, mais ils sont moins chers et fournissent une plus grande capacité de stockage. Ils sont donc adaptés pour le stockage des nombreux Instant Clones d'un pool volumineux. Les configurations de stockage étagées peuvent être utilisées pour gérer de façon rentable les scénarios d'E/S intensifs tels que l'exécution simultanée d'analyses antivirus programmées.

Si vous utilisez des banques de données vSAN, vous ne pouvez pas sélectionner manuellement différentes banques de données pour les réplicas ou les Instant Clones. Comme vSAN place automatiquement les objets sur le type de disque approprié et met en cache toutes les opérations d'E/S, il n'est pas nécessaire d'utiliser la hiérarchisation des réplicas pour les banques de données vSAN. Les pools d'Instant Clone sont pris en charge sur les banques de données vSAN.

Stockage d'Instant Clones sur des banques de données locales

Des machines virtuelles d'Instant Clone peuvent être stockées sur des banques de données locales, qui sont des disques de rechange internes sur des hôtes ESXi. Le stockage local offre des avantages tels que du matériel peu coûteux, un approvisionnement de machine virtuelle rapide, des opérations d'alimentation haute performance et une gestion simple. Cependant, l'utilisation du stockage local limite les options de configuration de l'infrastructure vSphere qui sont à votre disposition. L'utilisation du stockage local est utile dans certains environnements Horizon 7, mais n'est pas appropriée dans d'autres.

Note Les limites décrites dans cette section ne s'appliquent pas aux banques de données vSAN qui utilisent également des disques de stockage local, mais nécessitent un matériel spécifique.

L'utilisation de banques de données locales fonctionnera mieux si les postes de travail Horizon 7 dans votre environnement sont sans état. Par exemple, vous pouvez utiliser des magasins de données locaux si vous déployez des kiosques ou des stations de classe et de formation sans état.

Vous pouvez envisager l'utilisation de banques de données locales si vos machines virtuelles disposent d'attributions flottantes, ne sont pas dédiées à des utilisateurs finaux individuels et peuvent être supprimées ou actualisées à intervalles réguliers, par exemple lors de la déconnexion d'un utilisateur. Cette approche vous permet de contrôler l'utilisation des disques sur chaque banque de données locale sans devoir déplacer les machines virtuelles entre des banques de données ni effectuer un équilibrage de charge entre celles-ci.

Toutefois, vous devez tenir compte des restrictions qu'impose l'utilisation de banques de données locales sur votre déploiement de postes de travail ou de batterie de serveurs Horizon 7 :

- Vous ne pouvez pas utiliser vMotion pour gérer des volumes virtuels.
- Vous ne pouvez pas utiliser VMware High Availability.
- Vous ne pouvez pas utiliser vSphere Distributed Resource Scheduler (DRS).

Si vous déployez des Instant Clones sur un seul hôte ESXi avec une banque de données locale, vous devez configurer un cluster contenant cet hôte ESXi unique. Si vous disposez d'un cluster de deux ou plusieurs hôtes ESXi avec des banques de données locales, sélectionnez la banque de données locale à partir de chacun des hôtes du cluster. Dans le cas contraire, la création d'Instant Clone échoue. Ce comportement diffère de celui des banques de données locales avec des clones liés de View Composer.

- Vous ne pouvez pas stocker un réplica et des Instant Clones sur des banques de données séparées.
- Si vous sélectionnez des disques dur rotatifs locaux, les performances risquent de ne pas correspondre à celles d'une baie de stockage disponible sur le marché. Les disques durs rotatifs locaux et une baie de stockage peuvent avoir une capacité similaire, mais les disques durs rotatifs locaux n'offrent pas le même débit qu'une baie de stockage. Le débit est directement proportionnel au nombre de piles. Si vous sélectionnez des disques SSD (solid-state disks) directement raccordés, les performances sont susceptibles de dépasser celles de nombreuses baies de stockage.

- Si vous prévoyez de tirer parti des avantages du stockage local, vous devez soigneusement envisager les conséquences de ne pas disposer de vMotion, High Availability, DRS et autres fonctionnalités disponibles. Si vous gérez l'utilisation du disque local en contrôlant le nombre de disques de machines virtuelles et leur croissance, et si vous utilisez des attributions flottantes et effectuez régulièrement des opérations d'actualisation et de suppression, vous pouvez réussir à déployer des Instant Clones sur des banques de données locales.
- La prise en charge de la banque de données locale pour les Instant Clones est disponible pour les postes de travail virtuels et les postes de travail publiés.

Différences entre les Instant Clones et les clones liés View Composer

Comme les Instant Clones peuvent être créés beaucoup plus rapidement que les clones liés, les fonctionnalités suivantes de clones liés ne sont plus nécessaires lorsque vous provisionnez un pool d'Instant Clones :

- Les pools d'Instant Clone ne prennent pas en charge la configuration d'un disque virtuel supprimable séparé pour stocker les fichiers d'échange et temporaires du système d'exploitation invité. Chaque fois qu'un utilisateur se déconnecte d'un poste de travail d'Instant Clone, View supprime automatiquement le clone, puis provisionne et met sous tension un autre Instant Clone en fonction de la dernière image de système d'exploitation disponible pour le pool. Les fichiers d'échange et temporaires des systèmes d'exploitation invités sont automatiquement supprimés lors de l'opération de déconnexion.
- Les pools d'Instant Clone ne prennent pas en charge la création d'un disque virtuel persistant séparé pour chaque poste de travail virtuel. Vous pouvez plutôt stocker le profil Windows et les données d'application de l'utilisateur final sur des disques accessibles en écriture utilisateur App Volumes. Le disque accessible en écriture utilisateur de l'utilisateur final est lié à un poste de travail d'Instant Clone lorsque l'utilisateur final se connecte. De plus, des disques accessibles en écriture utilisateur peuvent être utilisés pour conserver des applications installées par l'utilisateur.
- Comme les postes de travail d'Instant Clone ont une durée de vie courte, les Instant Clones ne prennent pas en charge le format de disque à optimisation d'espace (SE sparse), avec son processus d'effacement et de réduction.
- Les pools de postes de travail d'Instant Clone sont compatibles avec Storage vMotion. Les pools de postes de travail de clone lié de View Composer ne sont pas compatibles avec Storage vMotion.

Approvisionnement d'application

Avec Horizon 7, vous disposez de plusieurs options concernant le provisionnement d'application : vous pouvez utiliser des techniques de provisionnement d'application traditionnelles, fournir des applications publiées plutôt qu'un poste de travail distant, distribuer des modules d'applications créés avec VMware ThinApp, déployer des applications dans le cadre d'une image de base View Composer ou d'Instant Clone ou lier des applications à l'aide d'App Volumes.

- **Déploiement d'applications individuelles à l'aide d'un hôte RDS**

Vous pouvez choisir de fournir aux utilisateurs finaux des applications publiées plutôt que des postes de travail distants. Les applications publiées individuelles peuvent être plus simples à utiliser sur un petit périphérique mobile.

- **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.

- **Déploiement d'applications et de mises à jour système avec des clones instantanés**

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

- **Gestion d'applications VMware ThinApp dans Horizon Administrator**

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

- **Déploiement et gestion d'applications à l'aide d'App Volumes**

VMware App Volumes offre une autre manière de gérer des applications en virtualisant des applications au-dessus du système d'exploitation. En utilisant cette stratégie, les applications, les fichiers de données, les paramètres, les intergiciels et les configurations agissent comme des conteneurs superposés distincts.

- **Utilisation de processus existants ou de VMware Mirage pour l'approvisionnement d'application**

Avec Horizon 7, vous pouvez continuer d'utiliser les techniques d'approvisionnement d'application que votre entreprise utilise actuellement et vous pouvez utiliser Mirage. 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 individuelles à l'aide d'un hôte RDS

Vous pouvez choisir de fournir aux utilisateurs finaux des applications publiées plutôt que des postes de travail distants. Les applications publiées individuelles peuvent être plus simples à utiliser sur un petit périphérique mobile.

Les utilisateurs finaux peuvent accéder à des applications Windows publiées en utilisant la même instance d'Horizon Client que celle qu'ils ont précédemment utilisée pour accéder aux postes de travail distants, et ils utilisent le même protocole d'affichage Blast Extreme ou PCoIP.

Pour fournir une application publiée, vous installez l'application sur un hôte RDS (Remote Desktop Session) Microsoft. Un ou plusieurs hôtes RDS constituent une batterie à partir de laquelle les administrateurs créent des pools d'applications de la même manière qu'ils créent des pools de postes de travail. Pour connaître les recommandations de dimensionnement de la batterie de serveurs, consultez l'article de la base de connaissances de VMware <http://kb.vmware.com/kb/2150348>.

L'utilisation de cette stratégie simplifie l'ajout, la suppression et la mise à jour des applications, l'ajout ou la suppression de droits d'accès utilisateurs aux applications, et l'attribution d'accès à partir de n'importe quel périphérique ou réseau à des batteries d'applications centralisées ou distribuées.

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

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

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

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

Note Comme vous pouvez également utiliser View Composer pour créer des batteries de serveur d'hôtes RDS Microsoft de clone lié, la fonction de recomposition vous permet de mettre à jour le système d'exploitation invité et des applications sur des hôtes RDS.

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

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

Déploiement d'applications et de mises à jour système avec des clones instantanés

Comme les pools de postes de travail de clone instantané 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 fonctionnalité d'image de transfert vous permet d'apporter des modifications à la machine virtuelle parente, de prendre un snapshot du nouvel état et d'envoyer la nouvelle version de l'image à tous les utilisateurs et postes de travail au fur et à mesure. Avec les mises à jour propagées, le temps d'arrêt lié à la maintenance de pool peut être réduit. Lorsqu'un utilisateur se déconnecte d'un poste de travail virtuel de clone instantané, Horizon 7 supprime le clone instantané et en crée un à partir de la dernière version de l'image. Ce nouveau clone est prêt pour le prochain utilisateur qui se connecte.

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

Gestion d'applications VMware ThinApp dans Horizon Administrator

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

VMware ThinApp fournit la virtualisation d'application en découplant une application du système d'exploitation sous-jacent et de ses bibliothèques et cadre, et en groupant l'application dans un seul fichier exécutable appelé module d'application. Vous pouvez utiliser Horizon Administrator pour distribuer des applications VMware ThinApp sur des postes de travail et sur des pools.

Important Si, au lieu de distribuer des applications ThinApp en les affectant à des postes de travail et à des pools, vous préférez affecter des applications ThinApp à des utilisateurs et à des groupes Active Directory, vous pouvez utiliser VMware Identity Manager.

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

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

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

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

Déploiement et gestion d'applications à l'aide d'App Volumes

VMware App Volumes offre une autre manière de gérer des applications en virtualisant des applications au-dessus du système d'exploitation. En utilisant cette stratégie, les applications, les fichiers de données, les paramètres, les intergiciels et les configurations agissent comme des conteneurs superposés distincts.

Ces conteneurs sont appelés piles d'applications (AppStacks) lorsqu'ils sont en mode lecture seule ou volumes accessibles en écriture lorsqu'ils sont en mode écriture-lecture. Les administrateurs peuvent utiliser App Volumes Manager pour créer des AppStacks et attribuer des droits d'application et pour fournir des AppStacks provisionnés au système ou à un utilisateur ou un groupe. Les applications fournies par App Volumes semblent être installées nativement et elles suivent les utilisateurs à travers les sessions et les périphériques. Les administrateurs peuvent mettre à jour ou remplacer les applications en temps réel et supprimer une application attribuée immédiatement, alors que l'utilisateur est toujours connecté ou lors de la prochaine connexion ou du prochain redémarrage.

Pour plus d'informations, consultez la documentation de VMware App Volumes, disponible à l'adresse <https://docs.vmware.com/fr/VMware-App-Volumes/index.html>.

Utilisation de processus existants ou de VMware Mirage pour l'approvisionnement d'application

Avec Horizon 7, vous pouvez continuer d'utiliser les techniques d'approvisionnement d'application que votre entreprise utilise actuellement et vous pouvez utiliser Mirage. 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 distants exactement au même moment, vous pouvez voir des pointes dans l'utilisation du processeur et l'E/S de stockage. Ces pics de charges de travail peuvent avoir des effets visibles sur les performances des postes de travail. Il est recommandé de planifier les mises à jour d'application au cours des heures creuses et d'échelonner les mises à jour sur les postes de travail si cela est possible. Vous devez également vérifier que votre solution de stockage est conçue pour prendre en charge de telles charges de travail.

Si votre entreprise autorise les utilisateurs à installer des applications, vous pouvez toujours utiliser vos stratégies actuelles, mais vous ne pouvez pas bénéficier des fonctions de View Composer, telles que l'actualisation et la recomposition du poste de travail. Avec View Composer, si une application n'est pas virtualisée ou incluse dans le profil ou les paramètres de données de l'utilisateur, cette application est

ignorée lorsqu'une opération d'actualisation, de recomposition ou de rééquilibrage de View Composer se produit. Dans de nombreux cas, cette possibilité de contrôler quelles applications sont installées est un avantage. Les postes de travail View Composer sont facilement pris en charge car ils sont conservés avec une configuration connue.

Si des utilisateurs ont des exigences précises pour installer leurs propres applications et pour que ces applications durent tout le cycle de vie du poste de travail distant, au lieu d'utiliser View Composer pour le provisionnement d'application, vous pouvez utiliser des Instant Clones avec App Volumes. Une autre solution consiste à créer des postes de travail dédiés de clone complet, à autoriser les utilisateurs à installer des applications, puis à utiliser Mirage pour gérer et mettre à jour les postes de travail sans remplacer les applications installées par l'utilisateur.

Important De plus, utilisez Mirage pour gérer les postes de travail et leurs applications hors ligne installés localement. Pour en savoir plus, consultez la page [Documentation sur Mirage](#).

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

Horizon 7 comporte de nombreux modèles d'administration ADMX de stratégie de groupe pour centraliser la gestion et la configuration de composants Horizon 7 et de postes de travail distants.

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
- Configuration du Serveur de connexion
- Configuration d'Horizon Client
- Configuration d'Horizon 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 d'Horizon Administrator. Vous pouvez également utiliser des GPO pour définir des stratégies non disponibles depuis l'interface utilisateur. Pour obtenir la liste complète et la description des paramètres disponibles dans les modèles d'administration ADMX, reportez-vous à *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Utilisation de stratégies de carte à puce

Vous pouvez également utiliser Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des fonctionnalités de redirection USB, d'impression virtuelle, de redirection du Presse-papiers, de redirection du lecteur client et de protocole d'affichage PCoIP sur des postes de travail distants spécifiques. Cette fonctionnalité requiert User Environment Manager.

Avec Stratégies de carte à puce, vous pouvez créer des stratégies qui ne prennent effet que si certaines conditions sont respectées. Par exemple, vous pouvez configurer une stratégie qui désactive la fonctionnalité de redirection du lecteur client si un utilisateur se connecte à un poste de travail distant depuis l'extérieur du réseau d'entreprise.

En général, les paramètres de stratégie Horizon que vous configurez pour les fonctionnalités de poste de travail distant dans User Environment Manager remplacent les paramètres de clé de registre et de stratégie de groupe équivalents.

Recommandations sur la planification et les éléments de conception d'architecture pour les déploiements de postes de travail distants

4

Une conception d'architecture d'Horizon 7 classique utilise une stratégie d'espace. Les définitions d'espace peuvent varier en fonction de la configuration matérielle, des versions logicielles d'Horizon 7 et de vSphere utilisées, et d'autres facteurs de conception spécifiques de l'environnement.

Les exemples dans ce document illustrent une conception évolutive standard que vous pouvez adapter à l'environnement de votre entreprise et à des exigences spéciales. Ce chapitre inclut des détails clés sur la configuration requise en termes de mémoire, de CPU, de capacité de stockage, de composants réseau et de matériel pour permettre aux architectes et aux planificateurs informatiques de visualiser concrètement tous les éléments impliqués dans le déploiement d'une solution Horizon 7.

Important Ce chapitre n'aborde pas les rubriques suivantes :

Conception de l'architecture pour les applications hébergées	Un espace Horizon 7 peut prendre en charge des batteries de serveurs d'hôtes RDS Microsoft, où chaque batterie de serveurs contient des hôtes RDS. Pour plus d'informations, consultez le document <i>Configuration d'applications et de postes de travail publiés dans Horizon 7</i> . Si vous prévoyez d'utiliser des machines virtuelles pour les hôtes RDS, voir aussi Configuration d'une machine virtuelle hôte RDS .
Conception d'architecture pour le plug-in de connexion directe d'Horizon 7 Agent	Lorsque ce plug-in est en cours d'exécution sur un poste de travail de machine virtuelle distant, le client peut se connecter directement à la machine virtuelle. Toutes les fonctionnalités de poste de travail distant, notamment PCoIP, HTML Access, RDP, redirection USB, et la gestion de session fonctionnent de la même manière, comme si l'utilisateur s'était connecté via Serveur de connexion View. Pour plus d'informations, consultez <i>Administration du plug-in Agent Direct-Connection Horizon 7</i> .

Ce chapitre contient les rubriques suivantes :

- [Exigences de machine virtuelle pour les postes de travail distants](#)
- [Horizon 7 Nœud ESXi](#)
- [Pools de postes de travail pour des types de travailleurs spécifiques](#)
- [Configuration de machine virtuelle de poste de travail](#)
- [Configuration d'une machine virtuelle hôte RDS](#)
- [Configuration d'une machine virtuelle vCenter Server et View Composer](#)
- [Configuration maximale du Serveur de connexion Horizon et configuration de machine virtuelle](#)
- [Clusters vSphere](#)

- [Exigences de stockage et de bande passante](#)
- [Blocs constitutifs Horizon 7](#)
- [Espaces Horizon 7](#)
- [Avantages à utiliser plusieurs vCenter Server dans un groupe](#)

Exigences de machine virtuelle pour les postes de travail distants

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

- [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.

- [Estimation des exigences de mémoire pour les postes de travail de machine virtuelle](#)

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

- [Estimation des exigences de CPU pour les postes de travail de machine virtuelle](#)

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.

- [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.

Planification en fonction des types de travailleurs

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

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

Travailleurs

Les travailleurs et les travailleurs administratifs effectuent des tâches répétitives dans un petit nombre d'applications, habituellement sur un ordinateur stationnaire. Les applications ne sont généralement pas gourmandes en mémoire et en CPU comme celles utilisées par les travailleurs du savoir. Les travailleurs qui ont des horaires spécifiques

peuvent tous ouvrir une session sur leurs postes de travail virtuels en même temps. Les travailleurs comprennent les analystes de centre d'appels, les employés du commerce de détail, les employés travaillant en 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.

Utilisateurs de kiosque

Ces utilisateurs doivent partager un poste de travail qui se trouve dans un lieu public. Parmi les utilisateurs de kiosque, on trouve des étudiants utilisant un ordinateur partagé dans une salle de classe, des infirmières dans un poste de garde et des ordinateurs utilisés pour la recherche d'emploi et le recrutement. Ces postes de travail requièrent une ouverture de session automatique. L'authentification peut être effectuée via certaines applications si nécessaire.

Estimation des exigences de mémoire pour les postes de travail de machine virtuelle

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

Si l'allocation de RAM est trop faible, l'E/S de stockage peut être affectée négativement car il se produit trop d'échange Windows. 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 Windows excessif, qui peut générer une E/S causant des dégradations importantes des performances et augmentant la charge d'E/S de stockage.

- VMware ESXi prend en charge des algorithmes de gestion de ressource de mémoire sophistiqués, comme le partage transparent de page et le gonflage de mémoire, qui peuvent réduire significativement la RAM physique nécessaire pour prendre en charge une allocation de RAM invitée 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 l'hôte ESXi, définissez des valeurs non nulles pour les paramètres de réservation de RAM. Réserver un peu de RAM garantit que les postes de travail en veille mais utilisés ne sont jamais complètement délogés sur le disque. Cela peut également réduire l'espace de stockage consommé par les fichiers d'échange d'ESXi. Cependant, des paramètres de réservation supérieurs affectent votre capacité à surcharger la mémoire sur un hôte ESXi et peuvent affecter les opérations de maintenance de VMotion.

Impact du dimensionnement de la RAM sur le stockage

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

fichier d'échange de Windows

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

Pour les Instant Clones, les fichiers d'échange et temporaires des systèmes d'exploitation invités sont automatiquement supprimés lors de l'opération de déconnexion, ils n'ont donc pas le temps de devenir trop volumineux. Chaque fois qu'un utilisateur se déconnecte d'un poste de travail d'Instant Clone, Horizon supprime le clone, puis provisionne et met sous tension un autre Instant Clone en fonction de la dernière image de système d'exploitation disponible pour le pool.

Fichier de mise en veille prolongée de Windows pour ordinateurs portables

Ce fichier peut évaluer 100 % de la RAM du client. Vous pouvez supprimer ce fichier en toute sécurité, car il n'est pas requis dans les déploiements d'Horizon.

Fichier d'échange d'ESXi

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 invitée sont réservés et que la RAM invitée est de 2 Go, le fichier d'échange d'ESXi est de 1 Go. Ce fichier peut être stocké sur la banque de données locale sur l'hôte ou le cluster ESXi.

Fichier de suspension d'ESXi

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 ou Blast Extreme

En plus de la mémoire système, une machine virtuelle requiert également une petite quantité de RAM sur l'hôte ESXi pour la surcharge vidéo. Cette exigence de taille VRAM dépend de la résolution d'affichage et du nombre de moniteurs configurés pour les utilisateurs finaux. [Tableau 4-1](#) répertorie la quantité de RAM supplémentaire requise pour diverses configurations. Les quantités de mémoire répertoriées dans les colonnes complètent la quantité de mémoire requise pour d'autres fonctionnalités de PCoIP ou de Blast Extreme.

Tableau 4-1. Capacité supplémentaire d'affichage du client PCoIP ou Blast Extreme

Standard de résolution d'affichage	Largeur, en pixels	Hauteur, en pixels	Surcharge avec 1 écran	Surcharge avec 2 écrans	Surcharge avec 3 écrans	Surcharge avec 4 écrans
VGA	640	480	1,20 Mo	3,20 Mo	4,80 Mo	5,60 Mo
WXGA	1 280	800	4 Mo	12,50 Mo	18,75 Mo	25 Mo
1 080 p	1 920	1 080	8 Mo	25,40 Mo	38 Mo	50,60 Mo
WQXGA	2 560	1 600	16 Mo	60 Mo	84,80 Mo	109,60 Mo
UHD (4K)	3 840	2 160	32 Mo	78 Mo	124 Mo	Non pris en charge

Pour calculer la configuration système requise, les valeurs de VRAM doivent être ajoutées à la RAM système de base pour la machine virtuelle. La capacité supplémentaire de mémoire est automatiquement calculée et configurée lorsque vous spécifiez le nombre maximal de moniteurs et sélectionnez la résolution d'affichage dans Horizon Administrator.

Si vous utilisez la fonction de rendu 3D et sélectionnez Soft3D ou vSGA, vous pouvez effectuer le recalcul à l'aide des valeurs de VRAM supplémentaires dans un contrôle Horizon Administrator afin de configurer la VRAM pour des invités 3D. Pour d'autres types d'accélération graphique, outre Soft3D et vSGA, vous pouvez également spécifier la quantité exacte de VRAM si vous choisissez de gérer VRAM à l'aide de vSphere Client.

Par défaut, la configuration à plusieurs moniteurs correspond à la topologie d'hôte. Une surcharge supplémentaire est précalculée pour plus de 2 moniteurs afin de s'adapter à des schémas de topologie supplémentaires. Si un écran noir s'affiche au démarrage d'une session de poste de travail distant, vérifiez que les valeurs pour le nombre de moniteurs et la résolution d'affichage, qui sont définies dans Horizon Administrator, correspondent au système hôte, ou ajustez manuellement la quantité de mémoire en sélectionnant **Gérer à l'aide de vSphere Client** dans Horizon Administrator, puis définissez la valeur de mémoire vidéo totale sur le maximum de 128 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 consiste à allouer 1 Go aux postes de travail Windows 7 (ou version ultérieure) 32 bits et 2 Go aux postes de travail Windows 7 (ou version ultérieure) 64 bits. Si vous souhaitez utiliser l'une des fonctionnalités de graphiques à accélération matérielle pour les charges de travail 3D, VMware vous recommande de prévoir 2 CPU virtuelles et 4 Go de RAM. 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 de machine virtuelle

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.

Les exigences de CPU varient en fonction du type de travailleur. Au cours de la phase pilote, utilisez un outil de contrôle des performances, tel que Perfmon dans la machine virtuelle, esxtop dans ESXi ou des outils de contrôle des performances de vCenter Server pour comprendre les niveaux d'utilisation de CPU moyen et maximal pour ces groupes de travailleurs. Utilisez également les recommandations suivantes :

- Les développeurs de logiciel ou autres utilisateurs expérimentés avec des besoins en haute performance peuvent avoir des exigences de CPU beaucoup plus élevées que les travailleurs du savoir et les travailleurs. Les CPU virtuelles doubles ou quadruples sont recommandées pour les machines virtuelles Windows 7 64 bits qui exécutent des tâches nécessitant beaucoup de ressources, telles que l'utilisation d'applications de CAD, la lecture de vidéos HD ou l'utilisation de résolutions d'écran 4K.
- Les CPU virtuelles simples sont en général recommandées pour d'autres cas.

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

- Utilisez des Instant Clones ou des clones liés 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.
- Utilisez un antivirus compatible avec l'API VMware vShield. Par exemple, cette API a été intégrée dans VMware vCloud[®] Networking and Security 5.1 et version ultérieure.

Comme approche de dimensionnement initial informelle, pour commencer, supposez que chaque machine virtuelle requiert 1/8 à 1/10 d'un cœur de CPU comme puissance de calcul minimale garantie. Prévoyez pour cela un pilotage qui utilise 8 à 10 machines virtuelles par cœur. Par exemple, si vous partez du principe que vous utilisez 8 machines virtuelles par cœur et que vous possédez un hôte ESXi à 8 cœurs et 2 sockets, vous pouvez héberger 128 machines virtuelles sur le serveur au cours de la phase pilote. Contrôlez l'utilisation de CPU totale sur l'hôte au cours de cette période et vérifiez qu'elle ne dépasse rarement une marge de sécurité telle que 80 % pour laisser assez de hauteur aux pics.

Choisir la taille de disque système appropriée

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

Comme l'espace disque du centre de données 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.
- Désactivez les services Windows tels que le service Indexeur, le service Défragmenteur et les points de restauration. Pour plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7*.
- 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, un disque persistant View Composer ou App Volumes pour le contenu créé par les utilisateurs et les applications installées par les utilisateurs.
- Si vous utilisez vSphere 5.1 ou version ultérieure, activez la récupération d'espace pour vCenter Server et pour les pools de postes de travail de clone lié.

Si des postes de travail de machine virtuelle utilisent le format de disque à optimisation d'espace disponible avec vSphere 5.1 ou version ultérieure, les données périmées ou supprimées dans un système d'exploitation invité sont automatiquement récupérées avec un processus d'effacement et de réduction.

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

- Le fichier de suspension ESXi équivaut à la quantité de RAM allouée à la machine virtuelle.
- Par défaut, le fichier d'échange de Windows équivaut à 150 % de la RAM.
- Les fichiers journaux peuvent contenir jusqu'à 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 grandissent avec le temps, mais vous pouvez contrôler cette croissance en programmant des opérations d'actualisation de View Composer, en définissant une stratégie de surcharge de stockage pour des pools de postes de travail de machine virtuelle, et en redirigeant les fichiers d'échange et temporaires Windows sur un disque non persistant séparé.

Si vous utilisez des Instant Clones, les fichiers .vmdk croissent avec le temps pendant une session de connexion. Dès qu'un utilisateur se déconnecte, le poste de travail d'Instant Clone est automatiquement supprimé et un Instant Clone est créé et prêt pour le prochain utilisateur qui se connecte. Avec ce processus, le poste de travail est actualisé effectivement et reprend sa taille d'origine.

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

Horizon 7 Nœud ESXi

Un nœud est un hôte unique VMware ESXi qui héberge des postes de travail de machine virtuelle dans un déploiement d'Horizon 7.

Horizon 7 est plus rentable lorsque vous optimisez le taux de consolidation, qui est le nombre de postes de travail hébergés sur un hôte ESXi. Bien que de nombreux facteurs affectent la sélection de serveur, si vous effectuez une optimisation uniquement pour le prix d'acquisition, vous devez trouver des configurations de serveur qui ont un équilibre approprié de puissance de traitement et de mémoire.

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

- De façon générale, prenez en considération la capacité de calcul en termes de 8 ou 10 postes de travail virtuels par cœur de CPU. Pour plus d'informations sur le calcul des exigences de CPU pour chaque machine virtuelle, reportez-vous à la section [Estimation des exigences de CPU pour les postes de travail de machine virtuelle](#).
- Pensez à la capacité de mémoire en termes de RAM de poste de travail virtuel, de RAM d'hôte et de taux de surcharge. Bien que vous puissiez avoir entre 8 et 10 postes de travail virtuels par cœur de CPU, si des postes de travail virtuels disposent de 1 Go ou plus de RAM, vous devez également faire attention aux exigences de RAM physique. Pour plus d'informations sur le calcul de la quantité de RAM requise par machine virtuelle, reportez-vous à la section [Estimation des exigences de mémoire pour les postes de travail de machine virtuelle](#).

Notez également que les coûts de RAM physique ne sont pas linéaires et que, dans certaines situations, il peut être rentable d'acheter davantage de serveurs de plus petite taille qui n'utilisent pas de puces DIMM coûteuses. Dans d'autres cas, la densité de rack, la connectivité de stockage, la facilité de gestion et d'autres considérations font de la réduction du nombre de serveurs dans un déploiement un meilleur choix.

- Dans Horizon 7, la fonctionnalité View Storage Accelerator est activée par défaut, ce qui permet à des hôtes ESXi 5.5 Update 2 et version ultérieure de mettre en cache des données de disque de machine virtuelle communes. View Storage Accelerator peut améliorer les performances et réduire le besoin de bande passante d'E/S de stockage supplémentaire pour gérer des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus. Cette fonction requiert 1 Go de RAM par hôte ESXi.
- Enfin, prenez en considération des exigences de cluster et de basculement. Pour plus d'informations, reportez-vous à la section [Déterminer des exigences de haute disponibilité](#).

Pour plus d'informations sur les spécifications des hôtes ESXi dans vSphere, consultez le document *Configurations maximales pour VMware vSphere*.

Pools de postes de travail pour des types de travailleurs spécifiques

Horizon 7 offre de nombreuses fonctionnalités qui vous aident à conserver de l'espace de stockage et à réduire la puissance de traitement requise pour plusieurs cas d'utilisation. La plupart de ces fonctions sont disponibles en tant que paramètres de pool.

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

Images de poste de travail sans état

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

Images de poste de travail avec état

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

Il existe deux façons de créer des images de poste de travail sans état dans Horizon 7 :

- Vous pouvez créer des pools d'attribution flottante ou des pools d'attribution dédiée de machines virtuelles d'Instant Clone. La redirection de dossiers et les profils itinérants peuvent éventuellement être utilisés pour stocker des données utilisateur.
- Vous pouvez utiliser View Composer pour créer des pools à attribution flottante ou dédiée de machines virtuelles de clone lié. La redirection de dossiers et les profils itinérants peuvent éventuellement être utilisés pour stocker des données utilisateur ou configurer des disques persistants afin de conserver les données utilisateur.

Il existe plusieurs façons de créer des images de poste de travail avec état dans Horizon 7 :

- Vous pouvez créer des clones complets ou des machines virtuelles complètes. Certains fournisseurs de stockage disposent de solutions de stockage rentables pour les clones complets. Ces fournisseurs possèdent souvent leurs propres pratiques et utilitaires d'approvisionnement. Si vous faites appel à l'un de ces fournisseurs, vous devrez peut-être créer un pool d'affectation dédiée manuel.
- Vous pouvez créer des pools de machines virtuelles d'Instant Clone ou de clone lié et utiliser des volumes accessibles en écriture utilisateur App Volumes pour attacher des données utilisateur et des applications installées par l'utilisateur.

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

■ **Pools pour travailleurs**

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

- **Pools pour travailleurs du savoir et utilisateurs expérimentés**

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

- **Pools pour utilisateurs de kiosque**

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

Pools pour travailleurs

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

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

Pour les pools de postes de travail d'Instant Clone, utilisez les paramètres de pool suivants :

- Pour les pools d'Instant Clone, pour optimiser l'utilisation des ressources, utilisez le provisionnement à la demande pour accroître ou réduire le pool en fonction de l'utilisation. Veillez à spécifier suffisamment de postes de travail de rechange pour répondre à la fréquence de connexion.
- Pour les pools de postes de travail d'Instant Clone, Horizon 7 supprime automatiquement l'Instant Clone dès qu'un utilisateur se déconnecte. Un Instant Clone est créé et prêt pour la connexion du prochain utilisateur, ce qui actualise effectivement le poste de travail à chaque déconnexion.

Pour les pools de postes de travail de clone lié de View Composer, utilisez les paramètres de pool suivants :

- Pour les pools de postes de travail View Composer, déterminez quelle action, le cas échéant, exécuter lorsque les utilisateurs se déconnectent. Les disques croissent avec le temps. Vous pouvez conserver l'espace disque en actualisant le poste de travail à son état d'origine lorsque des utilisateurs ferment leur session. Vous pouvez également définir un planning pour l'actualisation périodique des postes de travail. Par exemple, vous pouvez programmer l'actualisation quotidienne, hebdomadaire ou mensuelle des postes de travail.

- Le cas échéant, et si vous utilisez des pools de clones liés View Composer, envisagez de stocker les postes de travail sur des banques de données ESXi locales. Cette stratégie peut offrir des avantages tels que du matériel peu coûteux, un approvisionnement de machine virtuelle rapide, des opérations d'alimentation haute performance et une gestion simple. Pour voir une liste des limites, consultez [Magasins de données locaux pour postes de travail flottants sans état](#). Les pools d'Instant Clone ne sont pas pris en charge sur les banques de données locales.

Note Pour obtenir des informations sur les autres types d'options de stockage, reportez-vous à [Réduction et gestion des exigences de stockage](#).

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

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

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

Pour tous les pools de postes de travail, utilisez les paramètres de pool généraux suivants :

- Créez un pool automatisé pour que les postes de travail puissent être créés lors de la création du pool ou générés à la demande en fonction de l'utilisation du pool.
- Utilisez une affectation flottante pour que les utilisateurs ouvrent une session sur n'importe quel poste de travail disponible. Ce paramètre réduit le nombre de postes de travail requis s'il n'est pas nécessaire que tout le monde ouvre une session simultanément.
- Créez des postes de travail d'Instant Clone ou de clone lié View Composer pour que les postes de travail partagent la même image de base et utilisent moins d'espace de stockage dans le centre de données que des machines virtuelles complètes.

Pools pour travailleurs du savoir et utilisateurs expérimentés

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

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

Pour les pools de postes de travail d'Instant Clone, utilisez les paramètres de pool suivants :

- Si vous utilisez des postes de travail d'Instant Clone, implémentez un partage de fichiers, un profil itinérant ou une autre solution de gestion des profils.

Pour les pools de postes de travail de clone lié de View Composer, utilisez les paramètres de pool suivants :

- Si vous utilisez View Composer avec des postes de travail virtuels vSphere, activez la fonctionnalité de récupération d'espace pour vCenter Server et pour le pool de postes de travail. Avec la fonction de récupération d'espace, les données périmées ou supprimées dans un système d'exploitation client sont automatiquement récupérées avec un processus d'effacement et de réduction.
- Si vous utilisez des postes de travail de clone lié de View Composer, implémentez Persona Management, des profils itinérants ou une autre solution de gestion des profils. Vous pouvez également configurer des disques persistants pour pouvoir actualiser et recomposer les disques du système d'exploitation de clone lié tout en conservant une copie du profil d'utilisateur sur les disques persistants.
- Utilisez la fonction Gestion de persona pour que les utilisateurs disposent toujours de leur apparence de poste de travail et de leurs paramètres d'application préférés, comme avec les profils d'utilisateur Windows.

Pour tous les pools de postes de travail, utilisez les paramètres de pool généraux suivants :

- Certains travailleurs expérimentés et travailleurs du savoir, tels que les comptables, les directeurs commerciaux, les analystes en recherche marketing, peuvent avoir besoin de se connecter au même poste de travail à chaque fois. Créez des pools d'affectation dédiée pour eux.
- Utilisez vStorage Thin Provisioning pour que chaque poste de travail n'utilise que l'espace de stockage dont le disque a besoin pour son fonctionnement initial.
- Pour les utilisateurs expérimentés et les travailleurs du savoir qui doivent installer leurs propres applications, ce qui ajoute des données au disque du système d'exploitation, il existe deux options. Une option consiste à créer des postes de travail de machine virtuelle complète.

La seconde option consiste à créer un pool de clones liés ou d'Instant Clones et à utiliser App Volumes pour conserver les applications installées par l'utilisateur et les données utilisateur à travers les connexions.

- Si des travailleurs du savoir n'ont pas besoin d'applications installées par l'utilisateur sauf pour une utilisation temporaire, vous pouvez créer des postes de travail de clone lié ou des postes de travail d'Instant Clone View Composer. Les images de poste de travail partagent la même image de base et utilisent moins d'espace de stockage que des machines virtuelles complètes.

Pools pour utilisateurs de kiosque

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

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

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

Pour configurer le mode kiosque, vous devez utiliser l'interface de ligne de commande `vdmadmin` et effectuer plusieurs procédures décrites dans les rubriques sur le mode kiosque du document *Administration d'Horizon 7*.

Dans le cadre de cette configuration, vous pouvez utiliser les paramètres de pool de postes de travail d'Instant Clone suivants.

- Si vous utilisez des pools de postes de travail d'Instant Clone, Horizon 7 supprime automatiquement l'Instant Clone dès qu'un utilisateur se déconnecte. Un Instant Clone est créé et prêt pour la connexion du prochain utilisateur, ce qui actualise effectivement le poste de travail à chaque déconnexion.

Dans le cadre de cette configuration, vous pouvez utiliser les paramètres de pool de postes de travail de clone lié de View Composer suivants.

- Si vous utilisez des postes de travail de clone lié View Composer, créez une stratégie d'actualisation pour que le poste de travail soit actualisé régulièrement, comme à chaque déconnexion de l'utilisateur.

- Le cas échéant, envisagez de stocker des postes de travail sur des magasins de données ESXi locaux. Cette stratégie peut offrir des avantages tels que du matériel peu coûteux, un approvisionnement de machine virtuelle rapide, des opérations d'alimentation haute performance et une gestion simple. Pour voir une liste des limites, consultez [Magasins de données locaux pour postes de travail flottants sans état](#). Les pools d'Instant Clone ne sont pas pris en charge sur les banques de données locales.

Note Pour obtenir des informations sur les autres types d'options de stockage, reportez-vous à [Réduction et gestion des exigences de stockage](#).

Dans le cadre de cette configuration, vous pouvez utiliser les paramètres généraux suivants pour tous les pools de postes de travail.

- Créez un pool automatisé pour que les postes de travail puissent être créés lors de la création du pool ou générés à la demande en fonction de l'utilisation du pool.
- Utilisez l'affectation flottante pour que les utilisateurs puissent accéder à n'importe quel poste de travail disponible dans le pool.
- Créez des postes de travail d'Instant Clone ou de clone lié View Composer pour que les postes de travail partagent la même image de base et utilisent moins d'espace de stockage dans le centre de données que des machines virtuelles complètes.
- Utilisez un GPO Active Directory pour configurer l'impression basée sur l'emplacement afin que le poste de travail utilise l'imprimante la plus proche. Pour obtenir la liste complète et la description des paramètres disponibles dans les modèles d'administration (ADMX) de stratégie de groupe, reportez-vous à *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
- Utilisez un GPO ou la fonctionnalité Stratégies de carte à puce pour contrôler si des périphériques USB locaux sont connectés au poste de travail lorsque ce dernier est lancé ou lorsque des périphériques USB sont branchés sur l'ordinateur client.

Configuration de machine virtuelle de poste de travail

Les exemples des divers paramètres, tels que la capacité de mémoire, le nombre de processeurs virtuels et l'espace disque, sont spécifiques à Horizon 7.

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

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

Les recommandations présentées dans le tableau suivant concernent un poste de travail de machine virtuelle Windows 7 ou version ultérieure standard.

Tableau 4-2. Exemple de machine virtuelle de poste de travail pour Windows 7 ou Windows 8

Élément	Exemple
Système d'exploitation	Windows 7 32 bits ou 64 bits ou version ultérieure (avec le dernier Service Pack)
RAM	1 Go (4 Go si les utilisateurs doivent disposer de fonctionnalités graphiques à accélération matérielle pour le rendu 3D)
CPU virtuelle	1 (2 pour les systèmes 64 bits ou si les utilisateurs doivent lire de la vidéo haute définition ou plein écran)
Capacité de disque système	24 Go (un peu moins que la norme)
Capacité des données utilisateur (sous forme de disque persistant)	5 Go (point de départ)
Type d'adaptateur SCSI virtuel	LSI Logic SAS (par défaut)
Adaptateur de réseau virtuel	VMXNET 3

Configuration d'une machine virtuelle hôte RDS

Utilisez les hôtes des services Bureau à distance (RDS) pour fournir des applications publiées et des postes de travail distants basés sur une session aux utilisateurs finaux.

Un hôte RDS peut être une machine physique ou une machine virtuelle. Cet exemple utilise une machine virtuelle avec les spécifications répertoriées dans le tableau suivant. L'hôte ESXi pour cette machine virtuelle peut faire partie d'un cluster VMware HA pour se protéger des pannes de serveur physique.

Tableau 4-3. Exemple de machine virtuelle d'hôte RDS

Élément	Exemple
Système d'exploitation	Windows Server 2008 R2 ou Windows Server 2012 R2 64 bits
RAM	24 Go
CPU virtuelle	4
Capacité de disque système	40 Go
Type d'adaptateur SCSI virtuel	LSI Logic SAS (par défaut pour Windows Server 2008)
Adaptateur de réseau virtuel	VMXNET 3
1 carte réseau	1 Gigabit
Nombre maximal de connexions clientes au total (notamment les connexions d'applications publiées et de postes de travail distants basées sur une session)	50

Note Si vous configurez des hôtes RDS proches de la limite inférieure des spécifications de ressources, vous pouvez rencontrer des contraintes de ressources lors de l'utilisation de toutes les fonctionnalités au lieu de l'installation par défaut.

Pour plus d'informations sur la configuration d'un hôte RDS et les charges de travail testées, reportez-vous au livre blanc *VMware Horizon 6 Reference Architecture (Architecture de référence de VMware Horizon 6)* à l'adresse

<http://www.vmware.com/files/pdf/techpaper/VMware-Reference-Architecture-Horizon-6-View-Mirage-Workspace.pdf>.

Configuration d'une machine virtuelle vCenter Server et View Composer

Vous pouvez installer vCenter Server et View Composer sur la même machine virtuelle ou sur des serveurs distincts. Ces serveurs requièrent beaucoup plus de mémoire et de puissance de traitement qu'une machine virtuelle de poste de travail.

VMware a testé la création et l'approvisionnement par View Composer de 2 000 postes de travail par pool à l'aide de vSphere 5.1 ou version ultérieure. VMware a également effectué des tests avec View Composer qui exécute une opération de recomposition sur 2 000 postes de travail à la fois. Pour ces tests, vCenter Server et View Composer ont été installés sur des machines virtuelles distinctes.

La taille du pool de postes de travail est limitée par les facteurs suivants :

- Chaque pool de postes de travail ne peut contenir qu'un seul cluster vSphere.
- Avec certaines configurations, les clusters peuvent contenir jusqu'à 32 hôtes. Avec d'autres configurations, les clusters sont limités à 8 hôtes. Pour plus d'informations, reportez-vous à la section [Clusters vSphere](#).
- Chaque cœur de CPU dispose de capacité de calcul pour 8 à 10 postes de travail virtuels.
- Le nombre d'adresses IP disponibles pour le sous-réseau limite le nombre de postes de travail dans le pool. Par exemple, si votre réseau est configuré pour que le sous-réseau du pool contienne uniquement 256 adresses IP utilisables, la taille du pool est limitée à 256 postes de travail. Vous pouvez toutefois configurer plusieurs étiquettes réseau afin d'augmenter considérablement le nombre d'adresses IP attribuées aux machines virtuelles d'un pool.

Bien qu'il soit possible d'installer vCenter Server et View Composer sur une machine physique, cet exemple utilise des machines virtuelles distinctes avec les spécifications répertoriées dans les tableaux suivants. L'hôte ESXi de ces machines virtuelles peut faire partie d'un cluster VMware HA pour se protéger contre les pannes de serveur physique.

Cet exemple suppose que vous utilisez Horizon 7 avec vSphere 5.1 ou version ultérieure et vCenter Server 5.1 ou version ultérieure.

Important Cet exemple part également du principe que View Composer et vCenter Server sont installés sur des machines virtuelles distinctes.

Tableau 4-4. Exemple de machine virtuelle vCenter Server

Élément	Exemple pour un système vCenter Server qui gère 10 000 postes de travail	Exemple pour un système vCenter Server qui gère 2 000 postes de travail
Système d'exploitation	Windows Server 2008 R2 Enterprise 64 bits	Windows Server 2008 R2 Enterprise 64 bits
RAM	48 Go	10 à 24 Go, en fonction de la version de vSphere
CPU virtuelle	16	2 à 8, en fonction de la version de vSphere
Capacité de disque système	180 Go	40 Go
Type d'adaptateur SCSI virtuel	LSI Logic SAS (par défaut pour Windows Server 2008)	LSI Logic SAS (par défaut pour Windows Server 2008)
Adaptateur de réseau virtuel	E1000 (par défaut)	VMXNET 3 (E1000, celui par défaut, convient également)
Opérations d'approvisionnement de vCenter simultanées maximum	20	20
Opérations d'alimentation simultanées maximum	50	50

Tableau 4-5. Exemple de machine virtuelle View Composer

Élément	Exemple pour View Composer qui gère 10,000 postes de travail	Exemple pour View Composer qui gère 2 000 postes de travail
Système d'exploitation	Windows Server 2008 R2 Enterprise 64 bits	Windows Server 2008 R2 Enterprise 64 bits
RAM	10 Go ou plus, en fonction de la version de vSphere	4 à 10 Go, en fonction de la version de vSphere
CPU virtuelle	4 ou plus, en fonction de la version de vSphere	2 à 4, en fonction de la version de vSphere
Capacité de disque système	50 Go	40 Go
Type d'adaptateur SCSI virtuel	LSI Logic SAS (par défaut pour Windows Server 2008)	LSI Logic SAS (par défaut pour Windows Server 2008)
Adaptateur de réseau virtuel	VMXNET 3	VMXNET 3
Taille de pool maximale de View Composer	2,000 postes de travail	1,000 postes de travail
Nombre maximum d'opérations de maintenance View Composer simultanées	12	12
Nombre maximum d'opérations d'approvisionnement View Composer simultanées	8	8

Important VMware vous recommande de placer la base de données à laquelle vCenter Server et View Composer se connectent sur une machine virtuelle séparée.

Configuration maximale du Serveur de connexion Horizon et configuration de machine virtuelle

Lorsque vous installez le Serveur de connexion Horizon, l'interface utilisateur d'Horizon Administrator est également installée.

Configuration du Serveur de connexion

Bien qu'il soit possible d'installer le Serveur de connexion sur une machine physique, cet exemple utilise une machine virtuelle avec les spécifications répertoriées dans Exemple de machine virtuelle de serveur de connexion. L'hôte ESXi pour cette machine virtuelle peut faire partie d'un cluster VMware HA pour se protéger des pannes de serveur physique.

Tableau 4-6. Exemple de machine virtuelle de serveur de connexion

Élément	Exemple
Système d'exploitation	Prenez connaissance des systèmes d'exploitation pris en charge dans le document <i>Installation d'Horizon 7</i> .
RAM	10 Go
CPU virtuel	4
Capacité de disque système	70 Go
Type d'adaptateur SCSI virtuel	LSI Logic SAS (par défaut pour Windows Server 2008)
Adaptateur de réseau virtuel	VMXNET 3
Adaptateur réseau	Carte réseau 1 Gbit/s

Considérations sur la conception de cluster du Serveur de connexion

Vous pouvez déployer plusieurs instances du Serveur de connexion répliquées dans un groupe pour prendre en charge l'équilibrage de charge et la haute disponibilité. Des groupes d'instances répliquées sont conçus pour prendre en charge le clustering dans un environnement de centre de données unique connecté à un réseau LAN.

Important Pour utiliser un groupe d'instances du Serveur de connexion répliquées dans un réseau étendu, un réseau métropolitain ou autre réseau non local dans des scénarios dans lesquels un déploiement d'Horizon doit s'étendre sur des centres de données, vous devez utiliser la fonctionnalité Architecture Cloud Pod. Pour plus d'informations, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Nombre maximal de connexions pour le Serveur de connexion

Connexions Bureau à distance fournit des informations sur les limites testées concernant le nombre de connexions simultanées auquel un déploiement d'Horizon 7 peut s'adapter.

Tableau 4-7. Connexions Bureau à distance

Serveurs de connexion par déploiement	Type de connexion	Connexions simultanées maximum
1 serveur de connexion	Connexion directe, RDP, Blast Extreme ou PCoIP	4 000 (configuration testée)
1 serveur de connexion	Connexion par tunnel, RDP	2 000 (configuration par défaut) 4 000 (configuration testée)
1 serveur de connexion	connexion à PCoIP Secure Gateway	2 000 (configuration par défaut) 4 000 (configuration testée)
1 serveur de connexion	Connexion à Blast Secure Gateway	2 000 (configuration par défaut) 4 000 (configuration testée)
1 serveur de connexion	Accès unifié à des PC physiques	2 000 (configuration testée)
1 serveur de connexion	Accès unifié à des hôtes RDS	2 000 (configuration testée)
7 serveurs de connexion	Connexion directe, RDP, Blast Extreme ou PCoIP	20 000 (configuration testée)

Note Les configurations testées sont entièrement prises en charge. Pour atteindre la configuration testée de 4 000 connexions simultanées au maximum sur un seul Serveur de connexion pour la connexion par tunnel, PCoIP Secure Gateway et Blast Secure Gateway, créez le fichier `locked.properties` sur la machine virtuelle sur laquelle le Serveur de connexion est installé : `C:\Program Files\VMware\VMware View\Server\sslgateway\conf`. Ensuite, définissez `maxConnections=4000` dans le fichier `locked.properties` et redémarrez le Serveur de connexion. Unified Access Gateway prend actuellement en charge 2 000 sessions et, par conséquent, 14 dispositifs Unified Access Gateway ont été utilisés lors du test de 20 000 sessions.

Des connexions PCoIP Secure Gateway sont requises si vous utilisez des serveurs de sécurité ou des dispositifs Unified Access Gateway pour les connexions PCoIP en dehors du réseau d'entreprise. Des connexions Blast Secure Gateway sont requises si vous utilisez des serveurs de sécurité ou des dispositifs Unified Access Gateway pour les connexions Blast Extreme ou HTML Access en dehors du réseau d'entreprise. Des connexions par tunnel sont requises si vous utilisez des serveurs de sécurité ou des dispositifs Unified Access Gateway pour les connexions RDP en dehors du réseau d'entreprise et pour la redirection USB et l'accélération MMR (redirection multimédia) avec une connexion PCoIP ou Blast Secure Gateway. Vous pouvez coupler plusieurs serveurs de sécurité sur une instance du Serveur de connexion.

Même si un seul serveur de sécurité ou dispositif Unified Access Gateway peut prendre en charge un maximum de 2 000 connexions simultanées, au lieu d'utiliser un seul serveur de sécurité par instance du Serveur de connexion (avec 2 000 sessions), vous pouvez choisir d'en utiliser 2 ou 4. La surveillance du serveur de sécurité peut indiquer que l'activité pour 2 000 utilisateurs est trop intense. La quantité requise de mémoire et d'utilisation du CPU peut indiquer la nécessité d'ajouter des serveurs de sécurité.

supplémentaires par instance du Serveur de connexion pour répartir la charge. Par exemple, vous pouvez utiliser 2 serveurs de sécurité traitant chacun 1 000 connexions ou utiliser 4 serveurs de sécurité traitant chacun 500 connexions. Le taux de serveurs de sécurité par rapport aux instances du Serveur de connexion dépend des conditions requises de l'environnement particulier.

Le nombre de connexions par dispositif Unified Access Gateway est semblable à celui des serveurs de sécurité. Pour plus d'informations sur les dispositifs Unified Access Gateway, consultez *Déploiement et configuration d'Unified Access Gateway*.

Note Dans cet exemple, bien que cinq instances du Serveur de connexion (configurées correctement) seraient en mesure de gérer 20 000 connexions, le chiffre 7 est affiché dans le tableau à des fins de planification de la disponibilité, et pour s'adapter aux connexions provenant de l'intérieur et de l'extérieur du réseau d'entreprise.

Par exemple, si vous aviez 20 000 utilisateurs, parmi lesquels 16 000 situés à l'intérieur du réseau d'entreprise, vous auriez besoin de cinq instances du Serveur de connexion à l'intérieur du réseau d'entreprise. Ainsi, si l'une des instances devient indisponible, les quatre instances restantes pourraient gérer la charge. De même, concernant les 4 000 connexions provenant de l'extérieur du réseau d'entreprise, vous utiliseriez deux instances du Serveur de connexion de sorte que si l'une devenait indisponible, il vous resterait encore l'autre pour gérer la charge.

Ces nombres supposent que des connexions externes sont présentées via une passerelle. Dans cet exemple, chacune des instances du Serveur de connexion gérant des connexions externes est couplée avec trois serveurs de sécurité, afin que, en cas d'indisponibilité de l'un d'eux, les deux restants puissent gérer la charge. Si vous utilisez des dispositifs Unified Access Gateway plutôt que des serveurs de sécurité, il vous en faudrait trois au total, à équilibrage de charge sur les deux instances du Serveur de connexion, afin que, en cas d'indisponibilité de l'un d'eux, les deux restants puissent gérer la charge.

Dans tous les cas, les utilisateurs doivent se reconnecter s'ils utilisaient un Serveur de connexion ou une passerelle qui est devenu indisponible.

Configuration matérielle requise pour Unified Access Gateway avec Horizon 7

VMware vous recommande d'utiliser 4 vCPU et 10 Go de RAM pour que les dispositifs Unified Access Gateway prennent en charge le nombre maximal de connexions lorsqu'ils sont utilisés avec Horizon 7.

Tableau 4-8. Configuration matérielle requise pour Unified Access Gateway

Élément	Exemple
Système d'exploitation	OVA (SUSE Linux Enterprise 12 (64 bits))
RAM	4 Go
CPU virtuel	4
Capacité de disque système	20 Go (modifier le niveau de journal par défaut requiert de l'espace supplémentaire)
Type d'adaptateur SCSI virtuel	LSI Logic Parallel (valeur par défaut pour OVA)

Tableau 4-8. Configuration matérielle requise pour Unified Access Gateway (Suite)

Élément	Exemple
Adaptateur de réseau virtuel	VMXNET 3
Adaptateur réseau	Carte réseau 1 Gbit/s
Mappage de réseau	Option à une seule carte réseau

Clusters vSphere

Les déploiements d'Horizon 7 peuvent utiliser des clusters VMware HA pour se protéger contre les pannes du serveur physique. Selon votre configuration, les clusters peuvent contenir jusqu'à 32 nœuds.

vSphere et vCenter Server fournissent un ensemble étendu de fonctionnalités pour la gestion de clusters de serveurs qui hébergent des postes de travail de machine virtuelle. La configuration du cluster est également importante, car chaque pool de postes de travail de machine virtuelle doit être associé à un pool de ressources vCenter Server. 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 d'Horizon 7 très volumineux, les performances et la réactivité de vCenter Server peuvent être améliorées en ne plaçant qu'un seul objet de cluster par objet de centre de données, ce qui n'est pas le comportement par défaut. Par défaut, vCenter Server crée des clusters dans le même objet de centre de données.

Note Pour découvrir les dernières mises à jour sur les limites de dimensionnement et les recommandations d'Horizon 7, consultez l'article de la base de connaissances de VMware <https://kb.vmware.com/s/article/2150348>.

Dans les conditions suivantes, vSphere les clusters peuvent contenir jusqu'à 32 hôtes ESXi ou nœuds :

- vSphere 5.1 et versions ultérieures, avec des pools de clone lié View Composer, et stocker des disques de réplica sur des banques de données NFS ou VMFS5 ou des banques de données ultérieures
- vSphere 6.0 et versions ultérieures, et stocker des pools sur des banques de données Virtual Volumes

Si vous disposez de vSphere 5.5 Update 1 et versions antérieures et que vous stockez des pools dans des banques de données vSAN, les clusters vSphere peuvent contenir jusqu'à 20 hôtes ESXi.

Si vous stockez les réplicas View Composer sur une version VMFS antérieure à VMFS5, un cluster peut contenir 8 hôtes au maximum. Les disques du système d'exploitation et les disques persistants peuvent être stockés sur des magasins de données NFS ou VMFS.

Pour plus d'informations, consultez le chapitre sur la création de pools de postes de travail dans le document *Configuration des postes de travail virtuels dans Horizon 7*. Les exigences de réseau dépendent du type de serveur, du nombre d'adaptateurs réseau et de la façon dont VMotion est configuré.

Déterminer des exigences de haute disponibilité

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

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

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

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

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

Exemple : Exemples de configuration de cluster

Les paramètres répertoriés dans les tableaux suivants sont propres à Horizon 7. Pour plus d'informations sur les limites des clusters HA dans vSphere, reportez-vous au document *Configurations maximales pour VMware vSphere*.

Note L'exemple d'infrastructure suivant a été testé avec View 5.2 et vSphere 5.1. L'exemple utilise des clones liés View Composer, plutôt que des Instant Clones, car le test a été exécuté avec View 5.2. La fonctionnalité d'Instant Clone est introduite avec Horizon 7. D'autres fonctionnalités qui n'étaient pas disponibles avec View 5.2 incluent vSAN et Virtual Volumes.

Tableau 4-9. Exemple d'infrastructure de cluster Horizon 7

Élément	Exemple
Machines virtuelles	Instances de vCenter Server, Active Directory, serveur de base de données SQL, View Composer, instances du Serveur de connexion, serveurs de sécurité, machines virtuelles parentes à utiliser en tant que sources de pools de postes de travail
Nœuds (hôtes ESXi)	6 serveurs Dell PowerEdge R720 (16 cœurs * 2 GHz ; et 192 Go de RAM sur chaque hôte)
Stockage SSD	Machines virtuelles pour vCenter Server, View Composer, serveur de base de données SQL et machines virtuelles parentes
Stockage non SSD	Machines virtuelles pour Active Directory, Serveur de connexion et serveur de sécurité
Type de cluster	DRS (Distributed Resource Scheduler)/HA

Tableau 4-10. Exemple de cluster de postes de travail de machine virtuelle

Élément	Exemple
Nombre de clusters	5
Nombre de postes de travail et de pools par cluster	1 pool de 2 000 postes de travail (machines virtuelles) par cluster
Nœuds (hôtes ESXi)	Voici des exemples de divers serveurs qui pourraient être utilisés pour chaque cluster : <ul style="list-style-type: none"> ■ 12 Dell PowerEdge R720 (16 cœurs * 2 GHz ; et 192 Go de RAM sur chaque hôte) ■ 16 Dell PowerEdge R710 (12 cœurs * 2 526 GHz ; et 144 Go de RAM sur chaque hôte) ■ 8 Dell PowerEdge R810 (24 cœurs * 2 GHz ; et 256 Go de RAM sur chaque hôte) ■ 6 Dell PowerEdge R810 + 3 PowerEdge R720
Stockage SSD	Machines virtuelles répliquées
Stockage non SSD	32 magasins de données non SSD pour les clones (450 Go par magasin de données)
Type de cluster	DRS (Distributed Resource Scheduler)/HA

Exigences de stockage et de bande passante

Plusieurs points doivent être pris en compte pour la planification du stockage partagé de postes de travail de machine virtuelle, la planification des exigences de bande passante de stockage concernant les tempêtes d'E/S et la planification des besoins de bande passante réseau.

Des détails sur les composants de stockage et de réseau utilisés dans une installation test chez VMware sont fournis dans ces rubriques connexes.

■ Exemple de stockage partagé

Pour un environnement de test View 5.2, des machines virtuelles répliquées View Composer ont été placées sur des disques SSD à performances de lecture élevées, qui prennent en charge des dizaines de milliers d'E/S par seconde (IOPS). Des clones liés ont été placés sur des magasins de données sur des supports de rotation traditionnels à faibles performances, qui sont moins chers et fournissent une plus grande capacité de stockage. L'exemple utilise des clones liés View Composer, plutôt que des Instant Clones, car le test a été exécuté avec View 5.2. La fonctionnalité d'Instant Clone est introduite avec Horizon 7.

- **Considérations de bande passante de stockage**

Dans un environnement Horizon 7, les tempêtes d'ouvertures de session constituent le principal élément à prendre en compte pour déterminer les exigences de bande passante.

- **Considérations de bande passante réseau**

Certains composants de réseau virtuels et physiques sont requis pour s'adapter à une charge de travail classique.

- **Résultats des tests de performances de View Composer**

Ces résultats de test décrivent une installation de View 5.2 comportant 10 000 postes de travail, dans laquelle une instance de vCenter Server 5.1 gère 5 pools comportant chacun 2 000 postes de travail de machine virtuelle. Une seule période de maintenance était requise pour l'approvisionnement d'un nouveau pool ou pour la recomposition, l'actualisation ou le rééquilibrage d'un pool existant de 2 000 machines virtuelles. Une tempête d'ouverture de session de 10 000 utilisateurs a également été testée.

- **Prise en charge de WAN**

Pour les réseaux WAN (Wide-Area Network), vous devez prendre en compte les contraintes de bande passante et les problèmes de latence. Les protocoles d'affichage PCoIP et Blast Extreme fournis par VMware s'adaptent aux conditions variables de latence et de bande passante.

Exemple de stockage partagé

Pour un environnement de test View 5.2, des machines virtuelles répliquées View Composer ont été placées sur des disques SSD à performances de lecture élevées, qui prennent en charge des dizaines de milliers d'E/S par seconde (IOPS). Des clones liés ont été placés sur des magasins de données sur des supports de rotation traditionnels à faibles performances, qui sont moins chers et fournissent une plus grande capacité de stockage. L'exemple utilise des clones liés View Composer, plutôt que des Instant Clones, car le test a été exécuté avec View 5.2. La fonctionnalité d'Instant Clone est introduite avec Horizon 7.

Les critères de conception du stockage sont un des éléments les plus importants pour la réussite d'une architecture Horizon 7. 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. Les fichiers binaires ESXi, les fichiers d'échange de machine virtuelle et les répliquées View Composer de machines virtuelles parentes sont stockés sur le système de stockage partagé.

Le système de stockage externe utilisé par vSphere peut être un réseau SAN (Storage Area Network) Fibre Channel ou iSCSI ou un réseau NAS (Network-Attached Storage) NFS (Network File System). Avec la fonctionnalité vSAN, disponible avec vSphere 5.5 Update 1 ou version ultérieure, le système de stockage peut également être un stockage SAS (Server-Attached Storage) local agrégé.

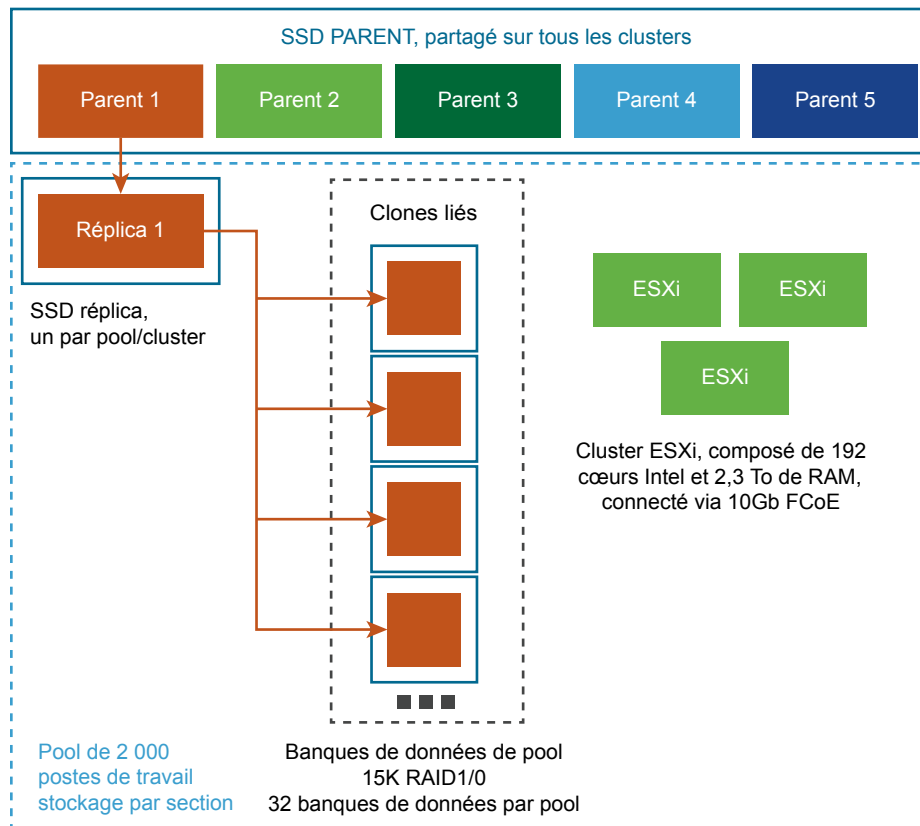
L'exemple suivant décrit la stratégie de stockage hiérarchisé utilisée dans une installation test de View 5.2 dans laquelle un seul système vCenter Server gère 10 000 postes de travail.

Note Cet exemple était utilisé dans une configuration de View 5.2, qui était effectuée avant la commercialisation de VMware vSAN. Pour obtenir des instructions sur le dimensionnement et la conception des composants clés des infrastructures de postes de travail virtuels View pour VMware vSAN, consultez le livre blanc à l'adresse <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

La fonctionnalité vSAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport à la fonctionnalité disponible avec vSphere 5.5 Update 1. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie. Pour plus d'informations sur vSAN dans vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware vSAN*.

Stockage physique	<ul style="list-style-type: none"> ■ Bloc EMC VNX7500 uniquement ■ 1,8 To de cache rapide (SSD) ■ 8 connexions principales 10 Gbits FCoE (4 par contrôleur).
Couche de stockage SSD	<p>Un pool de stockage RAID5 :</p> <ul style="list-style-type: none"> ■ 12 EFD * 200 Go ■ 250 Go de LUN pour les images parentes ■ 500 Go de LUN pour l'infrastructure ■ 75 Go de LUN pour les magasins de réplicas (1 par cluster de pools de postes de travail)
Couche de stockage de poste de travail de machine virtuelle	<p>2 pools de stockage RAID 1/0 :</p> <p>Pour le pool 1 :</p> <ul style="list-style-type: none"> ■ 360 15K 300 Go HDD (47 To utilisables) ■ 97 LUN de 450 Go pour les postes de travail <p>Pour le pool 2 :</p> <ul style="list-style-type: none"> ■ 296 15K 300 Go HDD (39 To utilisables) ■ 7 LUN de 450 Go pour l'infrastructure ■ 85 LUN de 450 Go pour les postes de travail

Cette stratégie de stockage est illustrée dans la figure suivante.

Chiffre 4-1. Exemple de stockage étagé pour un pool de postes de travail volumineux

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

Si vous utilisez View Composer avec des postes de travail de machine virtuelle vSphere 5.1 ou version ultérieure, vous pouvez utiliser la fonctionnalité de récupération d'espace. Avec cette fonction, les données périmées ou supprimées dans un système d'exploitation client sont automatiquement récupérées avec un processus d'effacement et de réduction lorsque la quantité d'espace disque inutilisé atteint un certain seuil. Notez que la fonctionnalité de récupération d'espace n'est pas prise en charge si vous utilisez une banque de données vSAN.

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

Note Les meilleures décisions concernant les composants de stockage dédié peuvent être prises lors d'une phase pilote. La considération principale est les E/S par seconde (IOPS). Vous pouvez mettre en place une stratégie de stockage multicouche ou un stockage vSAN pour optimiser les performances et réduire les coûts.

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

Considérations de bande passante de stockage

Dans un environnement Horizon 7, les tempêtes d'ouvertures de session constituent le principal élément à prendre en compte pour déterminer les exigences de bande passante.

Bien que de nombreux éléments soient importants pour concevoir un système de stockage prenant en charge un environnement Horizon 7, du point de vue de la configuration du serveur, il est essentiel de prévoir une bande passante de stockage adaptée. Vous devez également prendre en compte les effets du matériel de consolidation de port.

Occasionnellement, les environnements Horizon 7 peuvent subir des charges de tempêtes 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. VMware a testé un scénario de tempête d'ouverture de session pour 10 000 postes de travail. Pour plus d'informations, reportez-vous à la section [Résultats des tests de performances de View Composer](#).

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

- Configurez manuellement les paramètres du pool de façon que les réplicas soient stockés sur des banques de données distinctes, hautes performances.
- Utilisez vSAN, disponible avec vSphere 5.5 Update 1 ou version ultérieure, qui utilise la gestion basée sur la stratégie du logiciel pour déterminer quel type de disque il convient d'utiliser pour les réplicas.

- Utilisez Virtual Volumes, disponible avec vSphere 6.0 ou version ultérieure, qui utilise la gestion basée sur la stratégie du logiciel pour déterminer quel type de disque il convient d'utiliser pour les répliques.

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

Considérations de bande passante réseau

Certains composants de réseau virtuels et physiques sont requis pour s'adapter à une charge de travail classique.

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

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

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

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

Pour plus d'informations, consultez le guide d'informations intitulé *Protocole d'affichage PCoIP : guide d'informations et de dimensionnement d'un réseau basé sur un scénario*.

Contrôles d'optimisation disponibles avec PCoIP et Blast Extreme

Si vous utilisez le protocole d'affichage PCoIP ou Blast Extreme de VMware, vous pouvez régler plusieurs éléments qui affectent l'utilisation de bande passante.

- Vous pouvez configurer le niveau de qualité d'image et la fréquence d'image utilisés lors de périodes de surcharge du réseau. Le paramètre de niveau de qualité vous permet de limiter la qualité initiale des régions modifiées de l'image affichée. Vous pouvez également ajuster la fréquence d'image.

Ce contrôle fonctionne bien pour le contenu d'écran statique qui n'a pas à être mis à jour ou lorsque seulement une partie doit être actualisée.

- En ce qui concerne la bande passante de la session, vous pouvez configurer la bande passante maximale, en kilobits par seconde, afin qu'elle corresponde au type de connexion réseau, tel qu'une connexion Internet de 4 Mbit/s. La bande passante inclut la création d'images, le son, le canal virtuel, USB et le trafic de contrôle PCoIP ou Blast.

Vous pouvez également configurer une limite inférieure, en kilobits par seconde, pour la bande passante réservée pour la session. Ainsi l'utilisateur n'a pas à attendre que la bande passante devienne disponible. Vous pouvez spécifier la taille de l'unité de transmission maximale (MTU) pour les paquets UDP d'une session, de 500 à 1 500 octets.

Pour plus d'informations, consultez les sections « Paramètres généraux de PCoIP » et « Paramètres de stratégie de VMware Blast » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Exemple de configuration réseau

Dans un groupe test View 5.2 dans lequel une instance de vCenter Server 5.1 gère 5 pools comportant chacun 2 000 machines virtuelles, chaque hôte ESXi disposait des matériels et logiciels suivants pour les exigences de mise en réseau.

Note Cet exemple était utilisé dans une configuration de View 5.2, qui était effectuée avant la commercialisation de VMware vSAN. Pour obtenir des instructions sur le dimensionnement et la conception des composants clés des infrastructures de postes de travail virtuels View pour VMware vSAN, consultez le livre blanc à l'adresse <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>. De plus, l'exemple utilise des clones liés View Composer, plutôt que des Instant Clones, car le test a été exécuté avec View 5.2. La fonctionnalité d'Instant Clone est introduite avec Horizon 7.

Composants physiques pour chaque hôte

- Adaptateur Brocade 1860 Fabric utilisant 10Gig Ethernet et FCoE pour le trafic réseau et de stockage, respectivement.
- Connexion à un adaptateur Brocade VCS Ethernet Fabric comportant 6 commutateurs VDX6720-60. Les commutateurs avaient une liaison montante avec le reste du réseau avec deux connexions de 1 Go à un routeur Juniper J6350.

Résumé vLAN

- Un vLAN 10 Gbits par pool de postes de travail (5 pools)
- Un vLAN 1 Gbit pour le réseau de gestion
- Un vLAN 1 Gbit pour le réseau VMotion
- Un vLAN 10 Gbits pour le réseau d'infrastructure

Virtual VMotion-dvswitch (1 liaison montante par hôte)

Ce commutateur était utilisé par les hôtes ESXi de machines virtuelles d'infrastructure, parentes et de poste de travail.

- Trame Jumbo (9000 MTU)
- 1 groupe de ports distribués éphémères

	<ul style="list-style-type: none"> ■ VLAN privé et adressage 192.168.x.x
Infra-dvswitch (2 liaisons montantes par hôte)	<p>Ce commutateur était utilisé par les hôtes ESXi de machines virtuelles d'infrastructure.</p> <ul style="list-style-type: none"> ■ Trame Jumbo (9 000 MTU) ■ 1 groupe de ports distribués éphémères ■ VLAN d'infrastructure /24 (256 adresses)
Desktop-dvswitch (2 liaisons montantes par hôte)	<p>Ce commutateur était utilisé par les hôtes ESXi de machines virtuelles parentes et de poste de travail.</p> <ul style="list-style-type: none"> ■ Trame Jumbo (9000 MTU) ■ 6 groupes de ports distribués éphémères ■ 5 groupes de ports de postes de travail (1 par pool) ■ Chaque réseau était /21, 2 048 adresses

Résultats des tests de performances de View Composer

Ces résultats de test décrivent une installation de View 5.2 comportant 10 000 postes de travail, dans laquelle une instance de vCenter Server 5.1 gérait 5 pools comportant chacun 2 000 postes de travail de machine virtuelle. Une seule période de maintenance était requise pour l'approvisionnement d'un nouveau pool ou pour la recomposition, l'actualisation ou le rééquilibrage d'un pool existant de 2 000 machines virtuelles. Une tempête d'ouverture de session de 10 000 utilisateurs a également été testée.

Les résultats de test fournis ici ont été réalisés avec les paramètres logiciels, matériels et de configuration décrits dans les rubriques suivantes :

- Configurations de postes de travail et de pools décrites dans la section [Configuration maximale du Serveur de connexion Horizon et configuration de machine virtuelle](#)
- Composants de stockage étagé décrits dans la section [Exemple de stockage partagé](#)
- Composants de réseau décrits dans la section [Considérations de bande passante réseau](#)

Capacité d'une tempête d'ouverture de session de 10 000 utilisateurs d'une heure

Note Cet exemple était utilisé dans une configuration de View 5.2, qui était effectuée avant la commercialisation de VMware vSAN. Pour obtenir des instructions sur le dimensionnement et la conception des composants clés des infrastructures de postes de travail virtuels View pour VMware vSAN, consultez le livre blanc à l'adresse <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>. Pour afficher des résultats de tests avec diverses charges de travail et opérations View lors de l'utilisation de vSAN, reportez-vous au livre blanc sur l'architecture de référence à l'adresse <http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf>.

La fonctionnalité vSAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport à la fonctionnalité disponible avec vSphere 5.5 Update 1. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie. Pour plus d'informations sur vSAN dans vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware vSAN*.

Dans une installation test, les configurations de poste de travail et de pool suivantes étaient utilisées pour un scénario de tempête d'ouverture de session pour 10 000 postes de travail. La règle d'alimentation pour les postes de travail était définie sur Toujours active.

Pour 10 000 postes de travail, la tempête d'ouverture de session se produisait sur une période de 60 minutes, en utilisant une distribution normale d'heures d'ouverture de session. Les machines virtuelles étaient activées et disponibles avant le début de la tempête d'ouverture de session. Après l'ouverture de session, une charge de travail démarrait, qui incluait les applications suivantes : Adobe Reader, Microsoft Outlook, Internet Explorer, Microsoft Word et Bloc-notes.

Voici des détails supplémentaires de la tempête d'ouverture de session qui était supportée lors des tests :

- 95 % des ouvertures de session se produisaient dans une fenêtre d'écart-type +/- 2 (40 minutes).
- 68 % des ouvertures de session se produisaient dans une fenêtre d'écart-type +/- 1 (20 minutes).
- Le taux maximal d'ouverture de session était 400/min, ou 6,67/seconde.

Durée requise pour l'approvisionnement d'un pool

Les pools sont approvisionnés à l'avance, lorsque vous créez le pool, ou à la demande, à mesure que des utilisateurs y sont affectés. L'approvisionnement signifie qu'il faut créer la machine virtuelle et la configurer pour qu'elle utilise les paramètres d'image du système d'exploitation et réseau corrects.

Dans une installation test contenant déjà 4 pools de 2 000 machines virtuelles chacun, l'approvisionnement d'un cinquième pool qui contenait 2 000 machines virtuelles a pris 4 heures. Toutes les machines virtuelles ont été approvisionnées à l'avance.

Durée requise pour la recomposition d'un pool

Vous pouvez utiliser une opération de recomposition pour fournir des correctifs de système d'exploitation, installer ou mettre à jour des applications ou modifier les paramètres matériels du poste de travail de machines virtuelles dans un pool. Avant de recomposer un pool, vous prenez un snapshot d'une machine virtuelle avec une nouvelle configuration. L'opération de recomposition utilise ce snapshot pour mettre à jour toutes les machines virtuelles dans le pool.

Dans une installation test de 5 pools de 2 000 machines virtuelles chacun, la recomposition d'un pool de 2 000 machines virtuelles a pris 6 heures et 40 minutes. Toutes les machines virtuelles étaient activées et disponibles avant le début de l'opération de recomposition.

Durée requise pour l'actualisation d'un pool

Comme les disques croissent avec le temps, vous pouvez conserver l'espace disque en actualisant un poste de travail à son état d'origine lorsque des utilisateurs ferment leur session, ou vous pouvez définir un planning pour l'actualisation périodique des postes de travail. Par exemple, vous pouvez programmer l'actualisation quotidienne, hebdomadaire ou mensuelle des postes de travail.

Dans une installation test de 5 pools de 2 000 machines virtuelles chacun, l'actualisation d'un pool de 2 000 machines virtuelles a pris 2 heures et 40 minutes. Toutes les machines virtuelles étaient activées et disponibles avant le début de l'opération d'actualisation.

Durée requise pour le rééquilibrage d'un pool

Une opération de rééquilibrage de poste de travail redistribue de façon égale des postes de travail de clone lié sur des lecteurs logiques disponibles. Une opération de rééquilibrage économise de l'espace de stockage sur des lecteurs surchargés et garantit qu'aucun lecteur n'est sous-utilisé. Vous pouvez également utiliser une opération de rééquilibrage pour migrer toutes les machines virtuelles d'un pool de postes de travail vers une banque de données vSAN ou à partir de celle-ci.

Dans un groupe test qui contenait 5 pools de 2 000 machines virtuelles chacun, 2 magasins de données ont été ajoutés au groupe pour un test. Pour un autre test, 2 magasins de données ont été supprimés du groupe. Après l'ajout ou la suppression des magasins de données, une opération de rééquilibrage a été effectuée sur l'un des pools. Le rééquilibrage d'un pool de 2 000 machines virtuelles a pris 9 heures. Toutes les machines virtuelles étaient activées et disponibles avant le début de l'opération de rééquilibrage.

Prise en charge de WAN

Pour les réseaux WAN (Wide-Area Network), vous devez prendre en compte les contraintes de bande passante et les problèmes de latence. Les protocoles d'affichage PCoIP et Blast Extreme fournis par VMware s'adaptent aux conditions variables de latence et de bande passante.

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

- L'optimisation WAN est intéressante pour les protocoles TCP, tels que RDP, car ces protocoles requièrent plusieurs connexions entre client et serveur. La latence de ces connexions peut être assez élevée. L'usurpation des accélérateurs WAN répond aux connexions pour que la latence du réseau soit masquée pour le protocole. Comme PCoIP et Blast Extreme sont basés sur UDP, cette forme d'accélération WAN est inutile.
- Les accélérateurs WAN compriment également le trafic réseau entre client et serveur, mais cette compression est généralement limitée à des taux de compression de 2:1. PCoIP et Blast Extreme disposent de taux de compression beaucoup plus élevés.

Pour plus d'informations sur les contrôles que vous pouvez utiliser pour ajuster la façon dont PCoIP et Blast Extreme consomment la bande passante, reportez-vous à la section [Contrôles d'optimisation disponibles avec PCoIP et Blast Extreme](#).

Exigences de bande passante pour différents types d'utilisateurs

Lorsque vous déterminez les exigences de bande passante minimum pour PCoIP, utilisez les estimations suivantes :

- Bande passante moyenne comprise entre 100 et 150 Kbit/s pour un poste de travail avec une productivité de bureau basique : applications de bureau classiques sans vidéo ni graphique 3D, et paramètres Windows et Horizon 7 par défaut.
- Bande passante moyenne comprise entre 50 et 100 Kbit/s pour un poste de travail avec une productivité de bureau optimisée : applications de bureau classiques sans vidéo ni graphique 3D, et paramètres de poste de travail Windows et Horizon 7 optimisés.
- Bande passante moyenne comprise entre 400 et 600 Kbit/s pour postes de travail virtuels utilisant plusieurs écrans, 3D, Aero et Microsoft Office.
- Bande passante maximum comprise entre 500 Kbit/s et 1 Mbit/s pour fournir de la marge pour les rafales de changements d'écrans. En général, dimensionnez votre réseau à l'aide de la bande passante moyenne, mais tenez compte de la bande passante maximum pour gérer les rafales de trafic d'images liées aux changements d'écrans importants.

- 2 Mbit/s par utilisateur simultanément exécutant une vidéo 480p, en fonction de la limite de fréquence d'images configurée et du type de vidéo.

Note L'estimation de 50 à 150 Kbit/s par utilisateur classique se base sur l'hypothèse que tous les utilisateurs opèrent sans interruption et exécutent des tâches similaires sur une journée de 8 à 10 heures. Le chiffre d'utilisation de la bande passante de 50 Kbit/s provient de tests de View Planner sur un réseau LAN avec la fonction de développement sans perte désactivée. Les situations peuvent varier car certains utilisateurs peuvent être assez inactifs et ne presque pas consommer de bande passante, ce qui permet plus d'utilisateurs par lien. Par conséquent, le but de ces conseils est de fournir un point de départ pour planifier et tester la bande passante de façon plus détaillée.

L'exemple suivant montre comment calculer le nombre d'utilisateurs simultanés dans une succursale ou un bureau à distance avec une ligne T1 de 1,5 Mbit/s.

Scénario dans une succursale ou un bureau à distance

- Les utilisateurs possèdent des applications Microsoft Office de productivité basique, pas vidéo, pas de graphique 3D, des claviers et des souris USB.
- La bande passante requise par utilisateur de bureau classique sur Horizon 7 est comprise entre 50 et 150 Kbit/s.
- La capacité du réseau T1 est de 1,5 Mbit/s.
- L'utilisation de la bande passante est de 80 % (facteur d'utilisation 0,8).

Formule pour déterminer le nombre d'utilisateurs pris en charge

- Dans le pire des cas, les utilisateurs requièrent 150 Kbit/s : $(1,5 \text{ Mbit/s} * 0,8) / 150 \text{ Kbit/s} = (1\,500 * 0,8) / 150 = 8$ utilisateurs
- Dans le meilleur des cas, les utilisateurs requièrent 50 Kbit/s : $(1,5 \text{ Mbit/s} * 0,8) / 50 \text{ Kbit/s} = (1\,500 * 0,8) / 50 = 24$ utilisateurs

Résultat

Ce bureau à distance peut prendre en charge entre 8 et 24 utilisateurs simultanés par ligne T1 avec une capacité de 1,5 Mbit/s.

Important Une optimisation des paramètres de poste de travail Horizon 7 et Windows peut être nécessaire pour atteindre cette densité d'utilisateurs.

Blocs constitutifs Horizon 7

Un bloc constitutif est composé de serveurs physiques, d'une infrastructure vSphere, de serveurs Horizon 7, d'un stockage partagé et de postes de travail de machine virtuelle pour les utilisateurs finaux. Un bloc constitutif est une construction logique qui ne doit pas être dimensionnée pour plus de 2 000 postes de travail Horizon. En général, les clients incluent jusqu'à cinq blocs constitutifs dans un espace Horizon 7, même s'il est possible en théorie d'utiliser plus de blocs que cela, tant que l'espace ne dépasse pas 10 000 sessions et 7 instances du Serveur de connexion Horizon.

Tableau 4-11. Exemple de bloc constitutif Horizon sur un réseau local pour 2 000 postes de travail de machine virtuelle

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

Chaque vCenter Server peut prendre en charge jusqu'à 10 000 machines virtuelles. Cette prise en charge vous permet d'avoir des blocs constitutifs qui contiennent plus de 2 000 postes de travail de machine virtuelle. Toutefois, la taille de bloc réelle est également soumise à d'autres limites propres à Horizon 7.

Si vous ne possédez qu'un bloc constitutif dans un espace, utilisez deux instances du Serveur de connexion pour la redondance.

Espaces Horizon 7

Un espace est une unité d'organisation déterminée par les limites d'extensibilité d'Horizon 7.

Exemple de groupe utilisant cinq blocs constitutifs

Un espace Horizon 7 traditionnel intègre cinq blocs constitutifs de 2 000 utilisateurs que vous pouvez gérer comme une seule entité.

Tableau 4-12. Exemple d'un espace Horizon 7 basé sur un réseau local composé de 5 blocs constitutifs

Élément	Nombre
Blocs constitutifs d'un espace Horizon 7	5
vCenter Server et View Composer	5 (1 machine virtuelle qui héberge les deux dans chaque bloc constitutif)

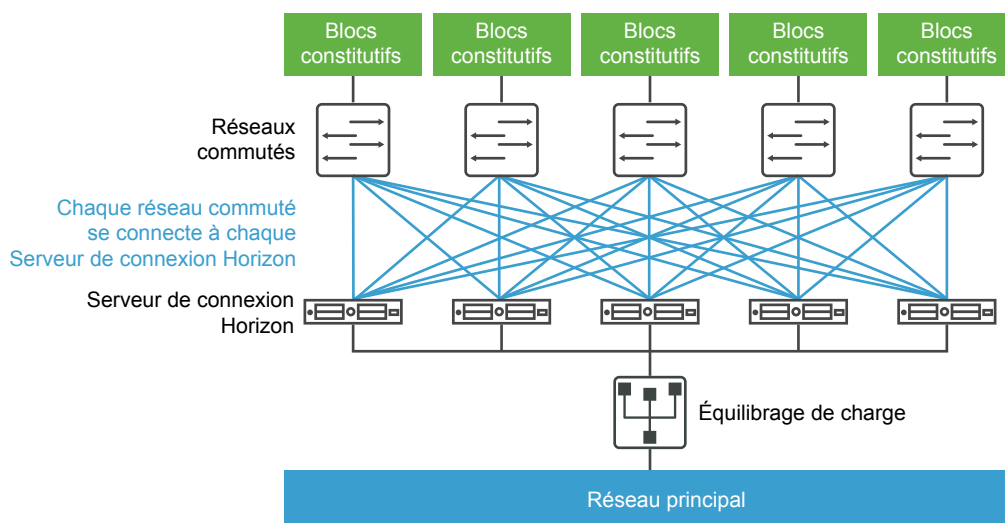
Tableau 4-12. Exemple d'un espace Horizon 7 basé sur un réseau local composé de 5 blocs constitutifs (Suite)

Élément	Nombre
Serveur de base de données	5 serveurs de base de données MS SQL Server ou Oracle (1 serveur de base de données autonome dans chaque bloc constitutif)
Serveurs de connexion	7 (5 pour les connexions de l'intérieur du réseau d'entreprise et 2 pour les connexions de l'extérieur)
vLAN	Reportez-vous à la section Tableau 4-11 .
Module Ethernet 10 Gbits	1
Commutateur de réseau modulaire	1

Chaque instance de vCenter Server peut prendre en charge jusqu'à 35 000 machines virtuelles enregistrées. Cette prise en charge vous permet d'avoir des blocs constitutifs qui contiennent plus de 2 000 postes de travail de machine virtuelle. Toutefois, la taille de bloc réelle est également soumise à d'autres limites propres à Horizon 7.

Pour les deux exemples décrits ici, un cœur de réseau peut équilibrer les charges des demandes entrantes dans les instances du Serveur de connexion. La prise en charge d'un mécanisme de redondance et de basculement, habituellement au niveau du réseau, peut éviter que l'équilibreur de charge ne devienne un point de défaillance. Par exemple, le protocole VRRP (Virtual Router Redundancy Protocol) peut communiquer avec un équilibreur de charge pour ajouter des capacités de redondance et de basculement.

Si une instance du Serveur de connexion 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 conservés dans le poste de travail de machine virtuelle pour que les utilisateurs puissent se connecter à une instance du Serveur de connexion différente et leur session de poste de travail reprend à l'endroit où elle était lors de l'échec.

Chiffre 4-2. Schéma d'un espace comportant 10 000 postes de travail de machine virtuelle

Exemple d'un espace utilisant une seule instance de vCenter Server

Dans la section précédente, l'espace Horizon 7 était composé de plusieurs blocs constitutifs. Chaque bloc constitutif prenait en charge 2 000 machines virtuelles avec une seule instance de vCenter Server. VMware a reçu de nombreux messages de clients et de partenaires demandant à utiliser une seule instance de vCenter Server pour gérer un espace Horizon 7. Cette demande provient du fait qu'une seule instance de vCenter Server peut prendre en charge 10 000 machines virtuelles. Les clients ont la possibilité d'utiliser une seule instance de vCenter Server pour gérer un environnement de 10 000 postes de travail. Cette rubrique illustre une architecture basée sur l'utilisation d'une seule instance de vCenter Server pour gérer 10 000 postes de travail.

Même si l'utilisation d'une seule instance de vCenter Server et de View Composer pour 10 000 postes de travail est possible, cela crée une situation impliquant un seul point de défaillance. La perte de cette instance unique de vCenter Server rend l'intégralité du déploiement de poste de travail indisponible pour les opérations d'alimentation, d'approvisionnement et d'adaptation. Pour cette raison, choisissez une architecture de déploiement qui satisfait vos exigences pour une résilience globale des composants.

Dans cet exemple, un espace de 10 000 utilisateurs comprend des serveurs physiques, une infrastructure vSphere, des serveurs Horizon 7, un stockage partagé et 5 clusters de 2 000 postes de travail virtuels chacun.

Tableau 4-13. Exemple d'un espace Horizon 7 basé sur un réseau local avec une seule instance de vCenter Server

Élément	Exemple
Clusters vSphere	6 (5 clusters avec un pool de clone lié par cluster et 1 cluster d'infrastructure)
vCenter Server	1
View Composer	1 (autonome)
Serveur de base de données	1 serveur de base de données MS SQL Server ou Oracle (autonome)
Serveur Active Directory	1 ou 2
Instances du Serveur de connexion	5
Serveurs de sécurité	5
vLAN	8 (5 pour les clusters de pools de postes de travail et 1 chacun pour la gestion, VMotion et le cluster d'infrastructure)

Présentation de Architecture Cloud Pod

Pour utiliser un groupe d'instances du Serveur de connexion répliquées dans un réseau étendu, un réseau métropolitain ou autre réseau non local dans des scénarios dans lesquels un déploiement d'Horizon doit s'étendre sur des centres de données, vous devez utiliser la fonctionnalité Architecture Cloud Pod.

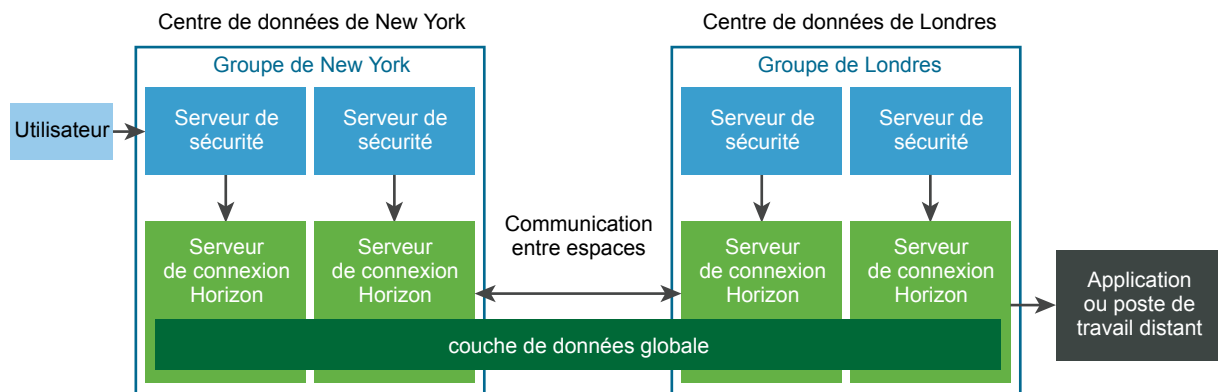
Cette fonctionnalité utilise les composants standard d'Horizon pour fournir l'administration de plusieurs centres de données, une correspondance globale et flexible des utilisateurs avec les postes de travail à haute disponibilité et des fonctionnalités de récupération d'urgence.

Une topologie Architecture Cloud Pod standard se compose d'au moins deux espaces qui sont reliés entre eux dans une fédération d'espaces. Les fédérations d'espaces sont soumises à certaines limites.

Tableau 4-14. Limites des fédérations d'espaces

Objet	Limite
Nombre total de sessions	250 000
Groupes	50
Sessions par espace	10 000
Sites	15
Instances du Serveur de connexion par espace	7
Nombre total d'instances du Serveur de connexion	350

Le graphique suivant présente un exemple d'une topologie Architecture Cloud Pod de base.



Dans l'exemple de topologie, deux espaces précédemment autonomes dans différents centres de données sont joints pour former une fédération d'espaces unique. Un utilisateur final de cet environnement peut se connecter à une instance du Serveur de connexion dans le centre de données de New York et recevoir un poste de travail ou une application dans le centre de données de Londres.

La fonction Architecture Cloud Pod n'est pas prise en charge dans un environnement IPv6.

Pour plus d'informations, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Avantages à utiliser plusieurs vCenter Server dans un groupe

Lorsque vous créez une conception pour un environnement de production Horizon 7 qui comporte plus de 500 postes de travail, plusieurs considérations affectent la décision d'utiliser une seule instance de vCenter Server plutôt que plusieurs instances.

À partir de View 5.2, VMware prend en charge la gestion de 10 000 machines virtuelles de poste de travail maximum dans un seul espace Horizon 7 avec un seul serveur vCenter 5.1 ou version ultérieure. Avant d'essayer de gérer 10 000 machines virtuelles avec une seule instance de vCenter Server, prenez en compte les considérations suivantes :

- Durée des fenêtres de maintenance de votre entreprise
- Capacité de tolérance aux pannes des composants d'Horizon 7
- Fréquence des opérations d'alimentation, d'approvisionnement et d'adaptation
- Simplicité de l'infrastructure

Durée des fenêtres de maintenance

Les paramètres de simultanéité des opérations d'alimentation, d'approvisionnement et de maintenance des machines virtuelles sont déterminés par instance de vCenter Server.

Conceptions d'espaces avec une seule instance de vCenter Server	<p>Les paramètres de simultanéité déterminent le nombre d'opérations pouvant être mises en file d'attente à la fois pour l'intégralité d'un espace Horizon 7.</p> <p>Par exemple, si vous définissez le nombre d'opérations d'approvisionnement simultanées sur 20 et que vous ne disposez que d'une seule instance de vCenter Server dans un espace, un pool de plus de 20 postes de travail entraînera la sérialisation des opérations d'approvisionnement. Après la mise en file d'attente de 20 opérations simultanées simultanément, une opération doit se terminer pour que la suivante commence. Dans les déploiements Horizon 7 à grande échelle, cette opération d'approvisionnement peut prendre beaucoup de temps.</p>
Conceptions d'espaces avec plusieurs instances de vCenter Server	Chaque instance peut approvisionner 20 machines virtuelles simultanément.

Pour garantir la simultanéité d'un plus grand nombre d'opérations dans une fenêtre de maintenance unique, vous pouvez ajouter plusieurs instances de vCenter Server (5 maximum) à votre espace et déployer plusieurs pools de postes de travail dans des clusters vSphere gérés par des instances de vCenter Server distinctes. Un cluster vSphere peut être géré par une seule instance de vCenter Server à la fois. Pour garantir la simultanéité sur plusieurs instances de vCenter Server, vous devez déployer vos pools de postes de travail en conséquence.

Capacité de tolérance aux échecs des composants

Le rôle de vCenter Server dans des espaces Horizon 7 consiste à fournir des opérations d'alimentation, d'approvisionnement et d'adaptation (actualisation, recomposition et rééquilibrage). Une fois qu'un poste de travail de machine virtuelle est déployé et activé, Horizon 7 ne repose pas sur vCenter Server pour le cours normal des opérations.

Comme chaque cluster vSphere doit être géré par une seule instance de vCenter Server, ce serveur représente un point de défaillance unique dans toutes les conceptions d'Horizon 7. Ce risque est également vrai pour chaque instance de View Composer. (Il existe un mappage un-à-un entre chaque instance de View Composer et de vCenter Server.) L'utilisation de l'un des produits suivants peut réduire l'impact d'une panne de vCenter Server ou de View Composer :

- VMware vSphere High Availability (HA)
- Produits de basculement tiers compatibles

Important Pour utiliser l'une de ces stratégies de basculement, l'instance de vCenter Server ne doit pas être installée dans une machine virtuelle faisant partie du cluster que l'instance gérée par vCenter Server.

En plus de ces options automatisées pour le basculement de vCenter Server, vous pouvez choisir de recréer le serveur en échec sur une nouvelle machine virtuelle ou sur un nouveau serveur physique. La plupart des informations clés sont stockées dans la base de données vCenter Server.

La tolérance aux risques est un facteur important dans le choix d'utiliser une ou plusieurs instances de vCenter Server dans votre conception d'espace. Si vos opérations requièrent la possibilité d'exécuter des tâches de gestion des postes de travail, telles que l'alimentation et l'adaptation de tous les postes de travail simultanément, vous devez diffuser l'impact d'une panne sur le moins de postes de travail possible à la fois en déployant plusieurs instances de vCenter Server. Si vous pouvez tolérer que votre environnement de poste de travail soit indisponible pour des opérations de gestion ou d'approvisionnement pendant un long moment, ou si vous choisissez d'utiliser un processus de recréation manuel, vous pouvez déployer une seule instance de vCenter Server pour votre espace.

Fréquence des opérations d'alimentation, d'approvisionnement et d'adaptation

Certaines opérations d'alimentation, d'approvisionnement et d'adaptation de postes de travail de machine virtuelle sont initiées uniquement par des actions d'administrateur, sont généralement prévisibles et contrôlables et peuvent être limitées à des fenêtres de maintenance établies. D'autres opérations d'alimentation et d'adaptation de postes de travail de machine virtuelle sont déclenchées par le comportement de l'utilisateur, tel que l'utilisation des paramètres Actualisation à la fermeture de session ou Interruption à la fermeture de session, ou par une action scriptée, telle que l'utilisation de DPM (Distributed Power Management) lors des fenêtres d'inactivité de l'utilisateur pour désactiver les hôtes ESXi inactifs.

Si votre conception d'Horizon 7 ne requiert pas d'opérations d'alimentation et d'adaptation déclenchées par l'utilisateur, une seule instance de vCenter Server peut probablement répondre à vos besoins. Sans une fréquence élevée d'opérations d'alimentation et d'adaptation déclenchées par l'utilisateur, aucune longue file d'attente d'opérations ne peut se former, ce qui peut entraîner sur le Serveur de connexion Horizon l'expiration du délai d'attente d'exécution par vCenter Server des opérations demandées dans les limites de simultanéité définies.

De nombreux clients choisissent de déployer des pools flottants et d'utiliser le paramètre Actualisation à la fermeture de session pour fournir de façon cohérente des postes de travail sans données périmées provenant de sessions précédentes. Les données périmées sont par exemple des pages de mémoire non réclamées dans les fichiers `pagefile.sys` ou `temp` de Windows. Les pools flottants peuvent également réduire l'impact des programmes malveillants en réinitialisant fréquemment les postes de travail à un état propre connu.

Certains clients réduisent la consommation électrique en configurant Horizon 7 de manière à désactiver les postes de travail inutilisés afin que vSphere DRS (Distributed Resources Scheduler) puisse consolider sur un nombre minimal d'hôtes ESXi les machines virtuelles en cours d'exécution. VMware Distributed Power Management désactive ensuite les hôtes inactifs. Dans ce type de scénario, plusieurs instances de vCenter Server peuvent mieux s'adapter à une fréquence élevée d'opérations d'alimentation et d'adaptation, et ainsi éviter l'expiration du délai d'attente des opérations.

Simplicité de l'infrastructure

Une seule instance de vCenter Server dans une conception d'Horizon 7 à grande échelle offre certains avantages irréfutables, tels qu'un emplacement unique permettant de gérer des images maître et des machines virtuelles parentes, un affichage unique de vCenter Server permettant de correspondre à l'affichage de la console Horizon Administrator et moins de bases de données principales de production et de serveurs de base de données. La planification de récupération d'urgence est plus simple pour une seule instance de vCenter Server que pour plusieurs instances. Comparez les avantages offerts par l'utilisation de plusieurs instances de vCenter Server, tels que la durée des fenêtres de maintenance et la fréquence des opérations d'alimentation et d'adaptation, par rapports aux inconvénients, tels que la lourdeur des tâches administratives pour gérer des images de machine virtuelle parente et l'accroissement du nombre de composants d'infrastructure requis.

Votre conception peut bénéficier d'une approche hybride. Vous pouvez choisir d'utiliser de très grands pools relativement statiques gérés par une seule instance de vCenter Server ou des pools de postes de travail plus petits, plus dynamiques gérés par plusieurs instances de vCenter Server. La meilleure stratégie pour la mise à niveau de groupes à grande échelle existants consiste à d'abord mettre à niveau les composants logiciels VMware de votre groupe existant. Avant de modifier votre conception d'espace, mesurez l'impact des améliorations des opérations d'alimentation, d'approvisionnement et d'adaptation de la dernière version, et testez ensuite l'augmentation de la taille de vos pools de postes de travail pour trouver le bon équilibre entre un plus grand nombre de grands pools de postes de travail et un plus faible nombre d'instances de vCenter Server.

Planification des fonctions de sécurité

5

Horizon 7 offre une sécurité réseau renforcée pour protéger les données d'entreprise sensibles. Pour plus de sécurité, vous pouvez intégrer Horizon 7 avec certaines solutions d'authentification utilisateur tierces, utiliser un serveur de sécurité et mettre en place la fonction d'autorisations limitées.

Important Horizon 6 version 6.2 et ultérieures peut exécuter des opérations cryptographiques à l'aide d'algorithmes conformes à FIPS (Federal Information Processing Standard) 140-2. Il est possible d'activer l'utilisation de ces algorithmes en installant Horizon 7 en mode FIPS. Le mode FIPS ne prend pas en charge toutes les fonctionnalités. Pour plus d'informations, reportez-vous au document *Installation d'Horizon 7*.

Ce chapitre contient les rubriques suivantes :

- [Comprendre les connexions client](#)
- [Choisir une méthode d'authentification utilisateur](#)
- [Restriction de l'accès aux postes de travail distants](#)
- [Utilisation de paramètres de stratégie de groupe pour sécuriser des applications et postes de travail distants](#)
- [Utilisation de Stratégies de carte à puce](#)
- [Implémentation de meilleures pratiques pour sécuriser des systèmes client](#)
- [Affectation de rôles d'administrateur](#)
- [Préparation pour l'utilisation d'un serveur de sécurité](#)
- [Comprendre les protocoles de communication](#)

Comprendre les connexions client

Horizon Client et Horizon Administrator communiquent avec un hôte du Serveur de connexion Horizon sur des connexions sécurisées HTTPS. Les informations sur le certificat du serveur sur le Serveur de connexion sont communiquées au client au titre de la négociation TLS entre le client et le serveur.

La connexion Horizon Client initiale, utilisée pour l'authentification utilisateur et la sélection d'applications et de postes de travail distants, est créée lorsqu'un utilisateur ouvre Horizon Client et fournit un nom de domaine complet pour l'hôte du Serveur de connexion, du serveur de sécurité ou Unified Access Gateway. La connexion Horizon Administrator est créée lorsqu'un administrateur saisit l'URL d'Horizon Administrator dans un navigateur Web.

Un certificat de serveur TLS par défaut est généré au cours de l'installation du Serveur de connexion. Par défaut, ce certificat est présenté aux clients TLS lorsqu'ils visitent une page sécurisée telle qu'Horizon Administrator.

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

- **Connexions clientes utilisant PCoIP Secure Gateway et Blast Secure Gateway**

Lorsque des clients se connectent à une application ou un poste de travail distant avec le protocole d'affichage PCoIP ou Blast Extreme à partir de VMware, Horizon Client peut réaliser une deuxième connexion au composant Secure Gateway applicable sur une instance du Serveur de connexion Horizon, un serveur de sécurité ou un dispositif Unified Access Gateway. Cette connexion fournit le niveau requis de sécurité et de connectivité lors de l'accès à des applications et postes de travail distants depuis Internet.

- **Connexions client par tunnel avec Microsoft RDP**

Lorsque des utilisateurs se connectent à un poste de travail distant avec le protocole d'affichage Microsoft RDP, Horizon Client peut établir une deuxième connexion HTTPS à l'hôte du Serveur de connexion Horizon. Cette connexion est appelée connexion par tunnel car elle fournit un tunnel pour le transport des données RDP.

- **Connexions client directes**

Les administrateurs peuvent configurer des paramètres du Serveur de connexion Horizon pour que les sessions d'applications publiées et de postes de travail distants soient établies directement entre le système client et la machine virtuelle d'application ou de poste de travail publié, en contournant l'hôte du Serveur de connexion. Ce type de connexion est appelé connexion client directe.

Connexions clientes utilisant PCoIP Secure Gateway et Blast Secure Gateway

Lorsque des clients se connectent à une application ou un poste de travail distant avec le protocole d'affichage PCoIP ou Blast Extreme à partir de VMware, Horizon Client peut réaliser une deuxième connexion au composant Secure Gateway applicable sur une instance du Serveur de connexion Horizon, un serveur de sécurité ou un dispositif Unified Access Gateway. Cette connexion fournit le niveau requis de sécurité et de connectivité lors de l'accès à des applications et postes de travail distants depuis Internet.

Les serveurs de sécurité et les dispositifs Unified Access Gateway comportent un composant PCoIP Secure Gateway et un composant Blast Secure Gateway, ce qui offre les avantages suivants :

- Le seul trafic d'application et de poste de travail à distance qui peut entrer dans le centre de données de l'entreprise est le trafic au nom d'un utilisateur dont l'authentification est renforcée.
- Les utilisateurs ne peuvent accéder qu'aux ressources dont l'accès leur est autorisé.
- La connexion PCoIP Secure Gateway prend en charge PCoIP et la connexion Blast Secure Gateway prend en charge Blast Extreme. Il s'agit de protocoles d'affichage à distance avancés qui utilisent le réseau plus efficacement en encapsulant des paquets d'affichage vidéo dans UDP plutôt que TCP.
- PCoIP et Blast Extreme sont sécurisés par le chiffrement AES-128 par défaut. Vous pouvez toutefois modifier le chiffrement à AES-256.
- Aucun VPN n'est requis, tant que le protocole d'affichage n'est pas bloqué par un composant de réseau. Par exemple, une personne tentant d'accéder à son application ou poste de travail distant depuis une chambre d'hôtel peut constater que le proxy utilisé par l'hôtel n'est pas configuré pour transmettre des paquets UDP.

Pour plus d'informations, reportez-vous à la section [Règles de pare-feu pour serveurs de sécurité basés sur une zone DMZ](#).

Les serveurs de sécurité s'exécutent sur les systèmes d'exploitation Windows Server 2008 R2 et Windows Server 2012 R2, et tirent pleinement parti de l'architecture 64 bits. Ce serveur de sécurité peut également bénéficier de processeurs Intel qui prennent en charge AESNI (AES New Instructions) pour des performances de chiffrement et de déchiffrement hautement optimisées.

Pour plus d'informations sur les dispositifs virtuels Unified Access Gateway, consultez le document *Déploiement et configuration d'Unified Access Gateway*.

Connexions client par tunnel avec Microsoft RDP

Lorsque des utilisateurs se connectent à un poste de travail distant avec le protocole d'affichage Microsoft RDP, Horizon Client peut établir une deuxième connexion HTTPS à l'hôte du Serveur de connexion Horizon. 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 Horizon 7 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 du Serveur de connexion, la connexion sécurisée HTTPS se termine sur le Serveur de connexion. Dans le déploiement d'une zone DMZ, la connexion sécurisée HTTPS se termine sur un serveur de sécurité ou un dispositif Unified Access Gateway. Reportez-vous à [Préparation pour l'utilisation d'un serveur de sécurité](#) pour plus d'informations sur les déploiements de zone DMZ et les serveurs de sécurité.

Les clients utilisant le protocole d'affichage PCoIP ou Blast Extreme peuvent utiliser la connexion par tunnel pour la redirection USB et l'accélération MMR (redirection multimédia), mais pour toutes les autres données, PCoIP utilise le composant PCoIP Secure Gateway et Blast Extreme utilise le composant Blast Secure Gateway sur un serveur de sécurité ou un dispositif Unified Access Gateway. Pour plus d'informations, reportez-vous à la section [Connexions clientes utilisant PCoIP Secure Gateway et Blast Secure Gateway](#).

Pour plus d'informations sur les dispositifs virtuels Unified Access Gateway, consultez le document *Déploiement et configuration d'Unified Access Gateway*.

Connexions client directes

Les administrateurs peuvent configurer des paramètres du Serveur de connexion Horizon pour que les sessions d'applications publiées et de postes de travail distants soient établies directement entre le système client et la machine virtuelle d'application ou de poste de travail publié, en contournant l'hôte du Serveur de connexion. Ce type de connexion est appelé connexion client directe.

Avec des connexions clientes directes, une connexion HTTPS peut toujours être établie entre le client et l'hôte du Serveur de connexion pour que les utilisateurs s'authentifient et sélectionnent des applications publiées et des postes de travail distants, mais la deuxième connexion HTTPS (la connexion par tunnel) n'est pas utilisée.

Les connexions PCoIP et Blast Extreme directes comportent les fonctions de sécurité intégrées suivantes :

- Prise en charge du chiffrement AES (Advanced Encryption Standard), qui est activé par défaut, et d'IP Security (IPsec).
- Prise en charge des clients VPN tiers

Pour les clients qui utilisent le protocole d'affichage Microsoft RDP, les connexions clientes directes aux postes de travail distants conviennent uniquement si votre déploiement se trouve sur un réseau d'entreprise. Avec des connexions clientes directes, le trafic RDP est envoyé non chiffré sur la connexion entre le client et la machine virtuelle de poste de travail.

Choisir une méthode d'authentification utilisateur

Horizon 7 utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs. Pour une sécurité améliorée, vous pouvez intégrer Horizon 7 avec des solutions d'authentification à deux facteurs, telles que RSA SecurID et RADIUS, et des solutions d'authentification par carte à puce.

- **Authentification Active Directory**

Chaque instance du Serveur de connexion Horizon 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.

- **Utilisation de l'authentification à deux facteurs**

Vous pouvez configurer une instance du Serveur de connexion Horizon pour forcer les utilisateurs à utiliser l'authentification RSA SecurID ou RADIUS (Remote Authentication Dial-In User Service).

- **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. Un type de carte à puce utilisé par le Département de la Défense des États-Unis se nomme carte CAC (Common Access Card).

- **Utilisation de la fonctionnalité Se connecter en tant qu'utilisateur actuel, disponible avec Horizon Client pour Windows**

Avec Horizon Client pour Windows, lorsque des utilisateurs sélectionnent **Se connecter en tant qu'utilisateur actuel** dans le menu **Options**, les informations d'identification qu'ils fournissent lors de l'ouverture de session sur le système client sont utilisées pour les authentifier sur l'instance du Serveur de connexion Horizon et sur le poste de travail distant. Aucune autre authentification d'utilisateur n'est requise.

Authentification Active Directory

Chaque instance du Serveur de connexion Horizon 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 du Serveur de connexion 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 du Serveur de connexion avec Horizon Client.

De même, 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 du Serveur de connexion avec Horizon Client.

Vous pouvez placer des utilisateurs et des groupes dans les domaines Active Directory suivants :

- Le domaine du Serveur de connexion
- Un domaine différent ayant une relation de confiance bidirectionnelle avec le domaine du Serveur de connexion
- Un domaine dans une forêt différente de celle du domaine du Serveur de connexion qui est approuvée par le domaine du Serveur de connexion dans une relation de confiance unidirectionnelle externe ou de domaine

- Un domaine dans une forêt différente de celle du domaine du Serveur de connexion qui est approuvée par le domaine du Serveur de connexion dans une relation de confiance de forêt transitive unidirectionnelle ou bidirectionnelle

Le Serveur de connexion 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, le Serveur de connexion peut déterminer rapidement une liste complète de domaines, mais le temps que cela prend augmente, car le nombre de domaines s'accroît ou la connectivité entre les domaines diminue. La liste peut également inclure des domaines que vous ne souhaitez pas proposer aux utilisateurs lorsqu'ils se connectent à leurs applications et leurs postes de travail distants.

Les administrateurs peuvent utiliser l'interface de ligne de commande `vdadmin` pour configurer le filtrage de domaines, qui limite les domaines qu'une instance du Serveur de connexion recherche et qu'elle affiche aux utilisateurs. Consultez le document *Administration de Horizon 7* pour plus d'informations.

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.

Utilisation de l'authentification à deux facteurs

Vous pouvez configurer une instance du Serveur de connexion Horizon pour forcer les utilisateurs à utiliser l'authentification RSA SecurID ou RADIUS (Remote Authentication Dial-In User Service).

- La prise en charge de RADIUS offre une large gamme d'autres options d'authentification à deux facteurs basée sur des jetons.
- Horizon 7 fournit également une interface d'extension standard ouverte pour permettre aux fournisseurs de solutions tiers d'intégrer des extensions d'authentification avancées dans Horizon 7.

Comme les solutions d'authentification à deux facteurs, telles que RSA SecurID et RADIUS, fonctionnent avec les gestionnaires d'authentification installés sur des serveurs séparés, vous devez configurer ces serveurs et les rendre accessibles à l'hôte du Serveur de connexion. Par exemple, si vous utilisez RSA SecurID, le gestionnaire d'authentification utilise RSA Authentication Manager. Si vous disposez de RADIUS, le gestionnaire d'authentification sera un serveur RADIUS.

Pour utiliser l'authentification à deux facteurs, chaque utilisateur doit posséder un jeton, tel qu'un jeton RSA SecurID, qui est enregistré avec son gestionnaire d'authentification. Un jeton d'authentification à deux facteurs est un élément matériel ou logiciel qui génère un code d'authentification à intervalles fixes. Souvent, l'authentification requiert de connaître un code PIN et un code d'authentification.

Si vous disposez de plusieurs instances du Serveur de connexion, vous pouvez configurer l'authentification à deux facteurs sur certaines instances, et configurer une méthode d'authentification utilisateur différente sur d'autres. Par exemple, vous pouvez configurer l'authentification à deux facteurs uniquement pour les utilisateurs qui accèdent à des applications et à des postes de travail à distance depuis l'extérieur du réseau d'entreprise, sur Internet.

Horizon 7 est certifié par le programme RSA SecurID Ready et prend en charge l'ensemble des fonctionnalités SecurID, notamment 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. Un type de carte à puce utilisé par le Département de la Défense des États-Unis se nomme carte CAC (Common Access Card).

Les administrateurs peuvent activer des instances du Serveur de connexion individuelles pour l'authentification par carte à puce. L'activation d'une instance du Serveur de connexion 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 du Serveur de connexion.

Toutes les connexions client, y compris les connexions client qui utilisent l'authentification par carte à puce, sont activées pour TLS/SSL.

Pour utiliser des cartes à puce, des machines client doivent comporter un intergiciel de carte à puce et un lecteur de carte à puce. Pour installer des certificats sur des cartes à puce, vous devez configurer un ordinateur afin qu'il agisse comme station d'inscription. Pour savoir si un type particulier d'Horizon Client prend en charge les cartes à puce, reportez-vous à la documentation d'Horizon Client à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Utilisation de la fonctionnalité **Se connecter en tant qu'utilisateur actuel**, disponible avec Horizon Client pour Windows

Avec Horizon Client pour Windows, lorsque des utilisateurs sélectionnent **Se connecter en tant qu'utilisateur actuel** dans le menu **Options**, les informations d'identification qu'ils fournissent lors de l'ouverture de session sur le système client sont utilisées pour les authentifier sur l'instance du Serveur de connexion Horizon et sur le poste de travail distant. Aucune autre authentification d'utilisateur n'est requise.

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

- Sur l'instance du Serveur de connexion, les informations d'identification utilisateur sont chiffrées et stockées dans la session utilisateur avec le nom d'utilisateur, le domaine et le nom d'utilisateur principal (UPN) facultatif. Les informations d'identification sont ajoutées lors de l'authentification et sont supprimées lors de la destruction de l'objet de session. 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 une mémoire volatile et n'est pas stocké dans Horizon LDAP ou dans un fichier de disque.

- Sur l'instance du Serveur de connexion, activez le paramètre **Autoriser l'ouverture de session en tant qu'utilisateur actuel** pour permettre à l'instance du Serveur de connexion d'accepter l'identité et les informations d'identification utilisateur qui sont transmises lorsque les utilisateurs sélectionnent **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** dans Horizon Client.

Important Vous devez comprendre les risques de sécurité avant d'activer ce paramètre. Consultez la section « Paramètres de serveur liés à la sécurité pour l'authentification utilisateur » dans le document *Sécurité d'Horizon 7*.

- Sur le système client, les informations d'identification d'utilisateur sont chiffrées et stockées dans un tableau dans Authentication Package, qui est un composant d'Horizon Client. Les informations d'identification sont ajoutées au tableau quand l'utilisateur ouvre une session et sont supprimées du tableau quand l'utilisateur ferme sa session. Le tableau réside dans la mémoire volatile.

Les administrateurs peuvent utiliser des paramètres de stratégie de groupe Horizon Client pour contrôler la disponibilité du paramètre **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** et pour spécifier sa valeur par défaut. Les administrateurs peuvent également utiliser une stratégie de groupe pour spécifier les instances du Serveur de connexion qui acceptent l'identité et les informations d'identification de l'utilisateur qui sont transmises lorsque celui-ci sélectionne **Se connecter en tant qu'utilisateur actuel** dans Horizon Client.

La fonction de déverrouillage récursif est activée lorsqu'un utilisateur se connecte au Serveur de connexion avec la fonction **Se connecter en tant qu'utilisateur actuel**. Cette fonctionnalité déverrouille toutes les sessions distantes après que la machine cliente a été déverrouillée. Les administrateurs peuvent contrôler la fonction de déverrouillage récursif avec le paramètre de stratégie globale **Déverrouiller les sessions distantes lorsque la machine cliente est déverrouillée** dans Horizon Client. Pour plus d'informations sur les paramètres de stratégie globale pour Horizon Client, consultez la documentation Horizon Client dans la page Web de la [documentation des clients VMware Horizon Client](#).

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

- Lorsque l'authentification par carte à puce est requise sur une instance du Serveur de connexion, l'authentification échoue pour les utilisateurs qui sélectionnent **Se connecter en tant qu'utilisateur actuel** lorsqu'ils se connectent à cette instance. Ces utilisateurs doivent s'authentifier à nouveau avec leur carte à puce et leur code PIN lorsqu'ils se connectent au Serveur de connexion.
- L'heure du système sur lequel le client se connecte et l'heure de l'hôte du Serveur de connexion doivent être synchronisées.
- Si les affectations de droits d'usage par défaut **Accéder à cet ordinateur à partir du réseau** sont modifiées sur le système client, elles doivent être modifiées comme indiqué dans l'article 1025691 de la base de connaissances de VMware.

- La machine client doit pouvoir communiquer avec le serveur Active Directory de l'entreprise et ne pas utiliser les informations d'identification mises en cache pour l'authentification. Par exemple, si des utilisateurs ouvrent une session sur leurs machines client depuis l'extérieur du réseau d'entreprise, les informations d'identification mises en cache sont utilisées pour l'authentification. Si l'utilisateur tente de se connecter à un serveur de sécurité ou à une instance du Serveur de connexion sans établir au préalable une connexion VPN, il est invité à fournir des informations d'identification, et la fonctionnalité Se connecter en tant qu'utilisateur actuel ne fonctionne pas.

Restriction de l'accès aux postes de travail distants

Vous pouvez utiliser la fonctionnalité de droits d'accès limités pour restreindre l'accès aux postes de travail distants en fonction de l'instance du Serveur de connexion Horizon à laquelle un utilisateur se connecte.

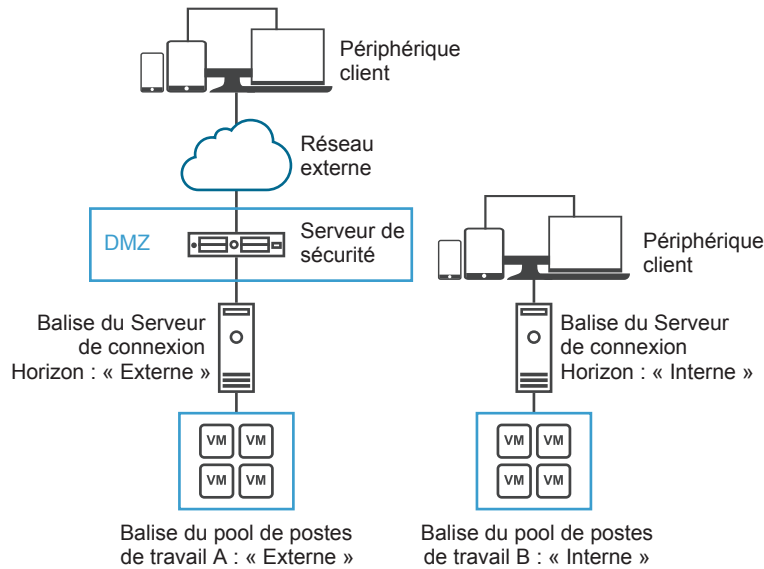
Avec des autorisations limitées, vous attribuez une ou plusieurs balises à une instance du Serveur de connexion. Ensuite, lorsque vous configurez un pool de postes de travail, vous sélectionnez les balises des instances du Serveur de connexion que vous voulez rendre capables d'accéder au pool de postes de travail. Lorsque les utilisateurs ouvrent une session via une instance marquée du Serveur de connexion, ils ne peuvent accéder qu'aux pools de postes de travail qui ont au moins une balise correspondante ou qui n'ont aucune balise.

Par exemple, votre déploiement d'Horizon 7 peut comporter deux instances du Serveur de connexion. 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 du Serveur de connexion qui prend en charge les utilisateurs internes.
- Attribuez la balise « External » à l'instance du Serveur de connexion qui est couplée avec le serveur de sécurité et qui prend en charge les utilisateurs externes.
- Affectez la balise « Internal » aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs internes.
- Affectez la balise « External » aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs externes.

Les utilisateurs externes ne peuvent pas voir les pools de postes de travail marqués comme « Internal », car ils ouvrent une session via le Serveur de connexion marqué comme « External ». Les utilisateurs internes ne peuvent pas voir les pools de postes de travail marqués comme « External », car ils ouvrent une session via le Serveur de connexion marqué comme « Internal ». [Chiffre 5-1](#) illustre cette configuration.

Chiffre 5-1. Exemple d'autorisations limitées



Vous pouvez également utiliser des autorisations limitées pour contrôler l'accès à des postes de travail en fonction de la méthode d'authentification utilisateur que vous configurez pour une instance du Serveur de connexion particulière. Par exemple, vous pouvez rendre certains pools de postes de travail disponibles pour des utilisateurs qui se sont authentifiés avec une carte à puce.

La fonction d'autorisations limitées ne fait qu'appliquer la correspondance de balise. Vous devez concevoir votre topologie de réseau pour forcer certains clients à se connecter via une instance du Serveur de connexion particulière.

Utilisation de paramètres de stratégie de groupe pour sécuriser des applications et postes de travail distants

Horizon 7 comporte des modèles d'administration ADMX de stratégie de groupe qui contiennent des paramètres de stratégie de groupe liés à la sécurité que vous pouvez utiliser pour sécuriser vos applications et postes de travail distants.

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

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

- Empêcher les systèmes client non-Horizon Client d'utiliser RDP pour se connecter à des postes de travail distants. Vous pouvez définir cette stratégie pour que les connexions soient obligatoirement gérées par Horizon Client, ce qui signifie que les utilisateurs doivent utiliser Horizon 7 pour se connecter à des postes de travail distants.

Consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7* pour plus d'informations sur l'utilisation des postes de travail distants et des paramètres de stratégie de groupe Horizon Client.

Utilisation de Stratégies de carte à puce

Vous pouvez utiliser Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des fonctionnalités de redirection USB, d'impression virtuelle, de redirection du Presse-papiers, de redirection du lecteur client et de protocole d'affichage PCoIP sur des postes de travail distants spécifiques. Vous pouvez également utiliser Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des applications publiées.

Avec Stratégies de carte à puce, vous pouvez créer des stratégies qui ne prennent effet que si certaines conditions sont respectées. Par exemple, vous pouvez configurer une stratégie qui désactive la fonctionnalité de redirection du lecteur client si un utilisateur se connecte à un poste de travail distant depuis l'extérieur du réseau d'entreprise.

La fonctionnalité Stratégies de carte à puce requiert User Environment Manager. Pour plus d'informations, consultez les rubriques sur Stratégies de carte à puce dans *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Implémentation de meilleures pratiques pour sécuriser des systèmes client

Implémentez les meilleures pratiques pour sécuriser des systèmes client.

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

Pour une référence succincte sur toutes les fonctions de sécurité fournies par Horizon 7, consultez le document *Sécurité de Horizon 7*.

Affectation de rôles d'administrateur

Une tâche de gestion clé dans un environnement Horizon 7 consiste à déterminer qui peut utiliser Horizon Administrator et les tâches que ces utilisateurs sont autorisés à effectuer.

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

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

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

Préparation pour l'utilisation d'un serveur de sécurité

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

Important Avec Horizon 6 version 6.2 et ultérieures, il est possible d'utiliser les dispositifs Unified Access Gateway au lieu de serveurs de sécurité. Les dispositifs Unified Access Gateway sont déployés en tant que dispositifs virtuels renforcés, qui sont basés sur un dispositif Linux qui a été personnalisé pour fournir un accès sécurisé. Pour plus d'informations sur les dispositifs virtuels Unified Access Gateway, consultez le document *Déploiement et configuration d'Unified Access Gateway*.

Un serveur de sécurité réside dans une zone DMZ et agit comme un hôte proxy pour les connexions dans votre réseau approuvé. Chaque serveur de sécurité est couplé avec une instance du Serveur de connexion et transmet tout le trafic à cette instance. Vous pouvez coupler plusieurs serveurs de sécurité sur un seul serveur de connexion. Cette conception fournit une couche supplémentaire de sécurité en protégeant l'instance du Serveur de connexion contre l'Internet public et en forçant toutes les demandes de session non protégées via le serveur de sécurité.

Un déploiement de serveur de sécurité basé sur une zone DMZ requiert l'ouverture de quelques ports sur le pare-feu afin d'autoriser des clients à se connecter à des serveurs de sécurité dans la zone DMZ. Vous devez également configurer des ports pour la communication entre des serveurs de sécurité et les instances du Serveur de connexion sur le réseau interne. Consultez [Règles de pare-feu pour serveurs de sécurité basés sur une zone DMZ](#) pour en savoir plus sur des ports spécifiques.

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

Note Les serveurs de sécurité incluent un composant PCoIP Secure Gateway et un composant Blast Secure Gateway afin que les clients qui utilisent le protocole d'affichage PCoIP ou Blast Extreme puissent utiliser un serveur de sécurité plutôt qu'un VPN.

Pour plus d'informations sur la configuration de réseaux privés virtuels avec PCoIP, consultez les présentations de solutions VPN, disponibles dans la section Technology Partner Resource du centre de ressources techniques sur <http://www.vmware.com/products/view/resources.html>.

Meilleures pratiques pour des déploiements de serveur de sécurité

Suivez ces règles de sécurité et des procédures de meilleure pratique lorsque vous utilisez un serveur de sécurité dans une zone DMZ.

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

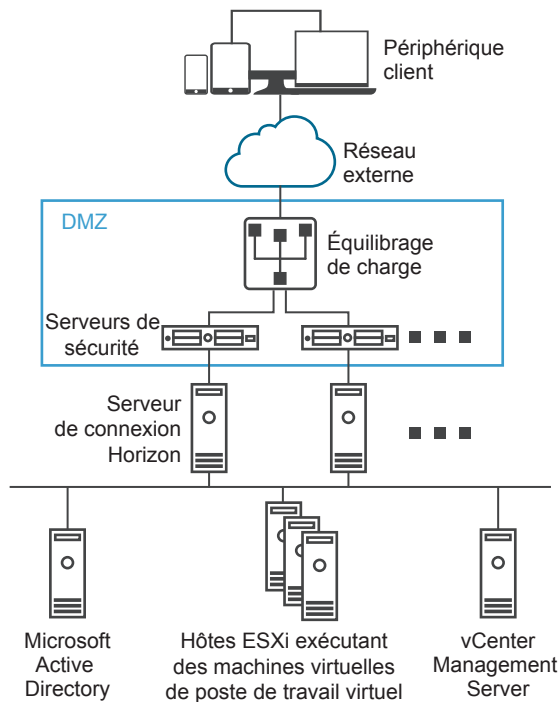
Pour limiter la portée des diffusions d'image, les instances du Serveur de connexion Horizon couplées avec des serveurs de sécurité doivent être déployées sur un réseau isolé. Cette topologie peut permettre d'empêcher un utilisateur malveillant sur le réseau interne de surveiller les communications entre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

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

Topologies de serveur de sécurité

Vous pouvez implémenter plusieurs topologies de serveur de sécurité différentes.

La topologie illustrée dans [Chiffre 5-2](#) montre un environnement hautement disponible qui comprend deux serveurs de sécurité avec équilibrage de charge dans une zone DMZ. Les serveurs de sécurité communiquent avec deux instances du Serveur de connexion Horizon dans le réseau interne.

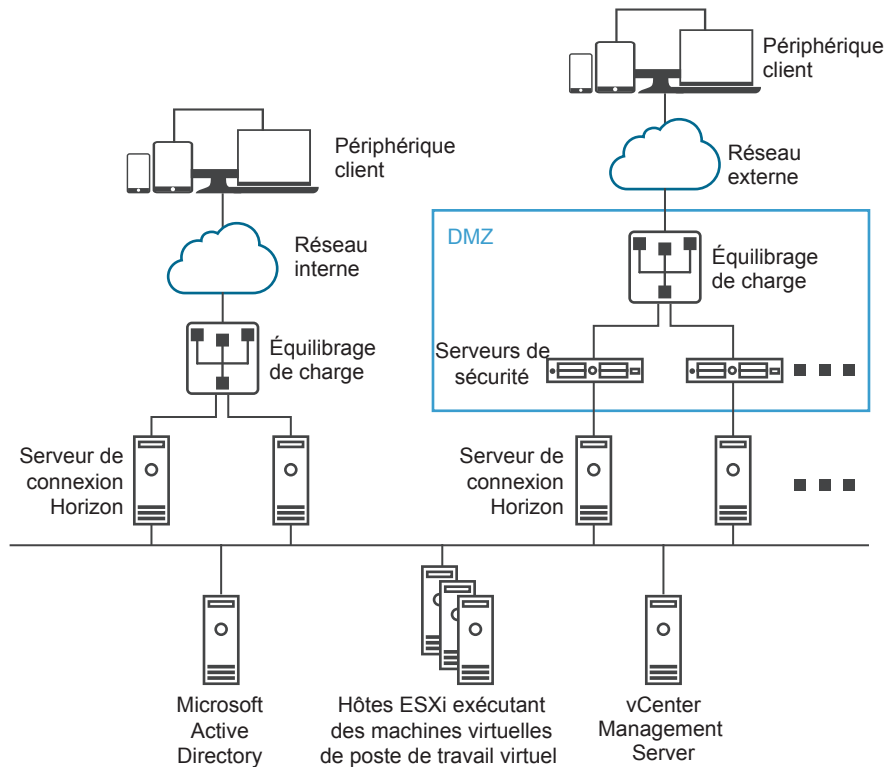
Chiffre 5-2. Serveurs de sécurité avec équilibrage de charge dans une zone DMZ

Lorsque des utilisateurs extérieurs au réseau d'entreprise se connectent à un serveur de sécurité, ils doivent s'authentifier avec succès avant de pouvoir accéder à des applications et à des postes de travail distants. Avec des règles de pare-feu adéquates des deux côtés de la zone DMZ, cette topologie est appropriée pour accéder à des applications et à des postes de travail distants à partir de périphériques clients situés sur Internet.

Vous pouvez connecter plusieurs serveurs de sécurité à chaque instance du Serveur de connexion. 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 [Chiffre 5-3](#) montre un environnement où quatre instances du Serveur de connexion 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 du Serveur de connexion 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.

Chiffre 5-3. Plusieurs serveurs de sécurité



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

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

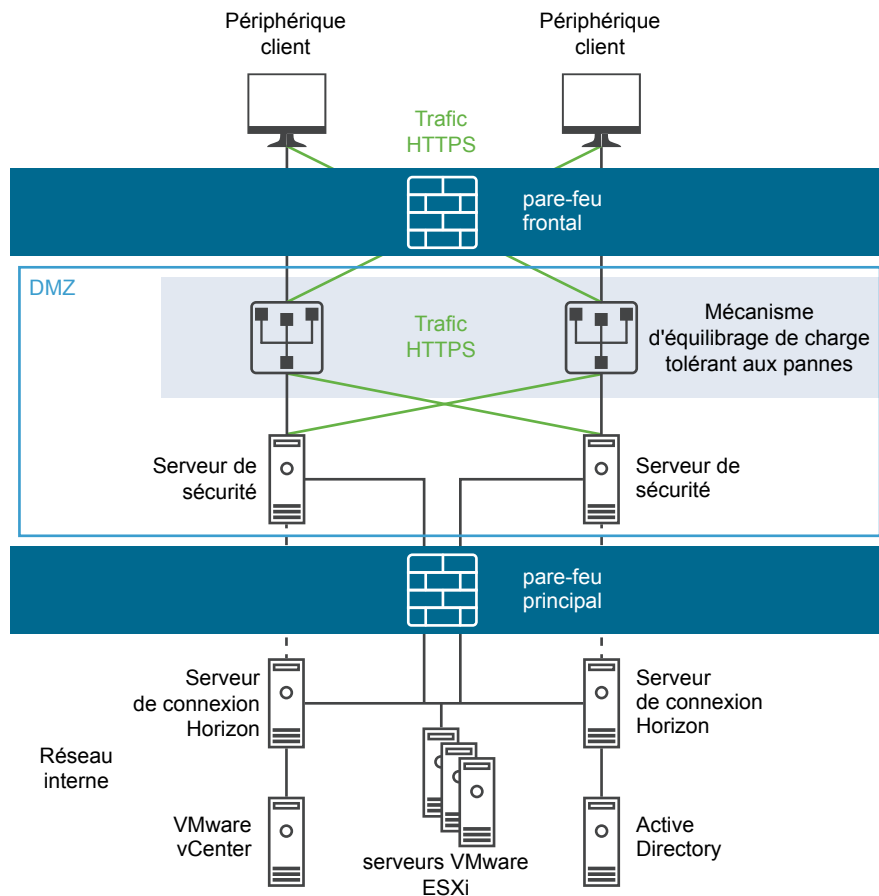
Un déploiement de serveur de sécurité basé sur une zone DMZ doit comporter deux pare-feu.

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

La règle de pare-feu contrôle exclusivement les communications entrantes provenant des services de la zone DMZ, ce qui réduit considérablement le risque que le réseau interne soit compromis. Pour plus d'informations sur les ports requis pour configurer des serveurs de sécurité, reportez-vous au document *Sécurité d'Horizon 7*.

La figure suivante montre un exemple de configuration qui comporte des pare-feu frontal et principal.

Chiffre 5-4. Topologie de double pare-feu



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

Les serveurs de sécurité basés sur une zone DMZ requièrent certaines règles de pare-feu sur les pare-feu frontaux et principaux. Lors de l'installation, les services Horizon 7 sont configurés pour écouter sur certains ports réseau par défaut. Si nécessaire, pour respecter les stratégies d'entreprise ou pour éviter la contention, vous pouvez modifier les numéros de port utilisés.

Important Pour plus d'informations et des recommandations de sécurité, reportez-vous au document *Sécurité de Horizon 7*.

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 sur certains ports TCP et UDP. [Tableau 5-1](#) résume les règles de pare-feu frontal.

Tableau 5-1. Règles de pare-feu frontal

Source	Port par défaut	Protocole	Destination	Port par défaut	Remarques
Horizon Client	Tout port TCP	HTTP	Serveur de sécurité	TCP 80	(Facultatif) Les périphériques client externes se connectent à un serveur de sécurité dans la zone DMZ sur le port TCP 80 et sont automatiquement dirigés vers HTTPS. Pour plus d'informations sur les aspects de la sécurité liés au fait de laisser les utilisateurs se connecter avec HTTP plutôt qu'avec HTTPS, reportez-vous au guide <i>Sécurité de Horizon 7</i> .
Horizon Client	Tout port TCP	HTTPS	Serveur de sécurité	TCP 443	Les périphériques clients externes se connectent à un serveur de sécurité dans la zone DMZ sur le port TCP 443 pour communiquer avec une instance du Serveur de connexion et avec des applications et des postes de travail distants.
Horizon Client	Tout port TCP Tout port UDP	PCoIP	Serveur de sécurité	TCP 4172 UDP 4172	Les périphériques client externes se connectent à un serveur de sécurité dans la zone DMZ sur le port TCP 4172 et sur le port UDP 4172 pour communiquer avec une application ou un poste de travail distant sur PCoIP.
Serveur de sécurité	UDP 4172	PCoIP	Horizon Client	Tout port UDP	Les serveurs de sécurité renvoient des données PCoIP à un périphérique client externe à partir du port UDP 4172. Le port UDP de destination est le port source des paquets UDP reçus. Comme ces paquets contiennent des données de réponse, il est normalement inutile d'ajouter une règle de pare-feu explicite pour ce trafic.
Horizon Client ou navigateur Web client	Tout port TCP	HTTPS	Serveur de sécurité	TCP 8443 UDP 8443	Les périphériques client externes et les clients Web externes (HTML Access) se connectent à un serveur de sécurité dans la zone DMZ sur le port HTTPS 8443 pour communiquer avec des postes de travail distants.

Règles de pare-feu principal

Pour autoriser un serveur de sécurité à communiquer avec chaque instance de Serveur de connexion View 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 applications et postes de travail distants et les instances du Serveur de connexion à communiquer entre eux. [Tableau 5-2](#) résume les règles de pare-feu principal.

Tableau 5-2. Règles de pare-feu principal

Source	Port par défaut	Protocole	Destination	Port par défaut	Remarques
Serveur de sécurité	UDP 500	IPSec	Serveur de connexion	UDP 500	Des serveurs de sécurité négocient IPSec avec des instances du Serveur de connexion sur le port UDP 500.
Serveur de connexion	UDP 500	IPSec	Serveur de sécurité	UDP 500	Des instances du Serveur de connexion répondent à des serveurs de sécurité sur le port UDP 500.

Tableau 5-2. Règles de pare-feu principal (Suite)

Source	Port par défaut	Protocole	Destination	Port par défaut	Remarques
Serveur de sécurité	UDP 4500	NAT-T ISAKMP	Serveur de connexion	UDP 4500	Requis si NAT est utilisé entre un serveur de sécurité et son instance du Serveur de connexion couplée. Les serveurs de sécurité utilisent le port UDP 4500 pour traverser les NAT et négocier la sécurité IPsec.
Serveur de connexion	UDP 4500	NAT-T ISAKMP	Serveur de sécurité	UDP 4500	Des instances du Serveur de connexion répondent à des serveurs de sécurité sur le port UDP 4500 si NAT est utilisé.
Serveur de sécurité	Tout port TCP	AJP13	Serveur de connexion	TCP 8009	Des serveurs de sécurité se connectent à des instances du Serveur de connexion sur le port TCP 8009 pour transférer le trafic Web à partir de périphériques clients externes. Si vous activez IPSec, le trafic AJP13 n'utilise pas le port TCP 8009 après le couplage. Il utilise plutôt NAT-T (port UDP 4500) ou ESP.
Serveur de sécurité	Tout port TCP	JMS	Serveur de connexion	TCP 4001	Des serveurs de sécurité se connectent à des instances du Serveur de connexion sur le port TCP 4001 pour échanger le trafic JMS (Java Message Service).
Serveur de sécurité	Tout port TCP	JMS	Serveur de connexion	TCP 4002	Des serveurs de sécurité se connectent à des instances du Serveur de connexion sur le port TCP 4002 pour échanger du trafic JMS (Java Message Service) sécurisé.
Serveur de sécurité	Tout port TCP	RDP	Poste de travail distant	TCP 3389	Les serveurs de sécurité se connectent à des postes de travail distants sur le port TCP 3389 pour échanger du trafic RDP.
Serveur de sécurité	Tout port TCP	MMR	Poste de travail distant	TCP 9427	Les serveurs de sécurité se connectent à des postes de travail distants sur le port TCP 9427 afin de recevoir le trafic lié à la redirection multimédia (MMR) et à la redirection de lecteur client.
Serveur de sécurité	Tout port TCP UDP 55000	PCoIP	Application ou poste de travail distant	TCP 4172 UDP 4172	Les serveurs de sécurité se connectent aux applications et postes de travail distants sur le port TCP 4172 et le port UDP 4172 pour échanger du trafic PCoIP.
Application ou poste de travail distant	UDP 4172	PCoIP	Serveur de sécurité	UDP 55000	Des applications et des postes de travail distants renvoient des données PCoIP à un serveur de sécurité à partir du port UDP 4172. Le port UDP de destination sera le port source des paquets UDP reçus. Comme ces paquets sont des données de réponse, il est normalement inutile d'ajouter une règle de pare-feu explicite pour cela.
Serveur de sécurité	Tout port TCP	USB-R	Poste de travail distant	TCP 32111	Des serveurs de sécurité se connectent à des postes de travail distants sur le port TCP 32111 pour échanger le trafic de redirection USB entre un périphérique client externe et le poste de travail distant.

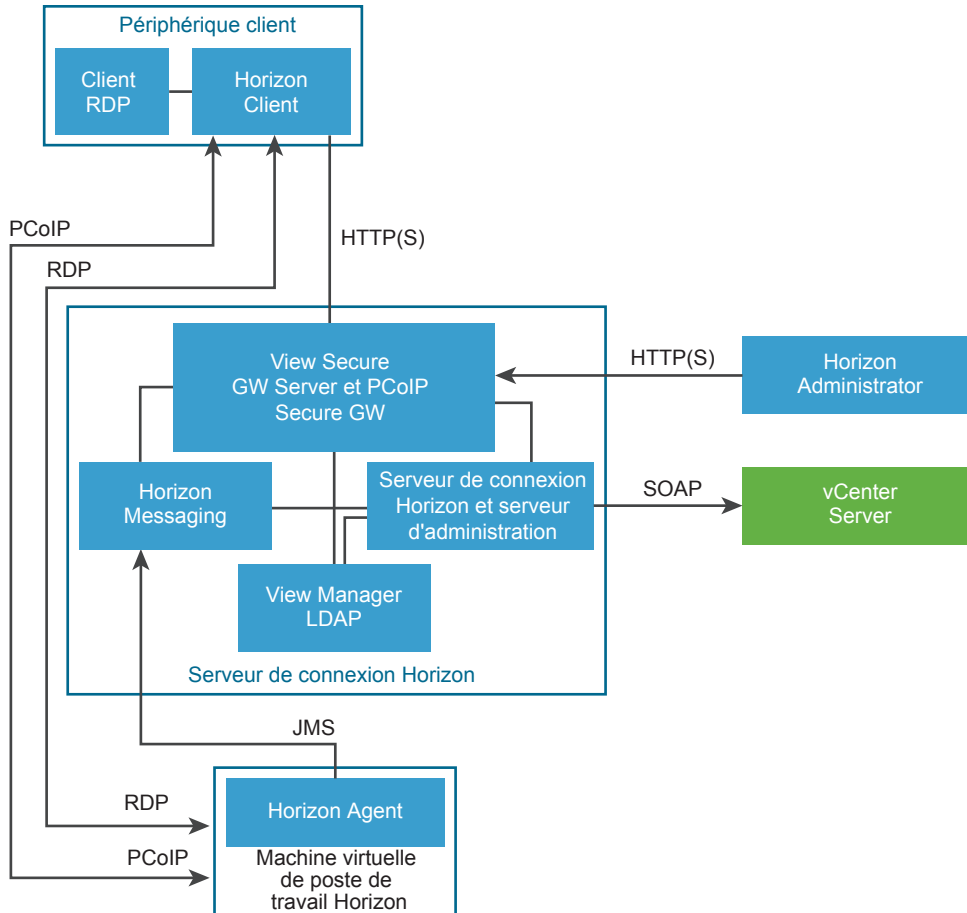
Tableau 5-2. Règles de pare-feu principal (Suite)

Source	Port par défaut	Protocole	Destination	Port par défaut	Remarques
Serveur de sécurité	Tout port TCP or UDP	Blast Extreme	Application ou poste de travail distant	TCP ou UDP 2244 3	Des serveurs de sécurité se connectent à des applications et des postes de travail distants sur le port TCP et UDP 22443 pour échanger du trafic Blast Extreme.
Serveur de sécurité	Tout port TCP	HTTPS	Poste de travail distant	TCP 22443	Si vous utilisez HTML Access, les serveurs de sécurité se connectent à des postes de travail distants sur le port HTTPS 22443 pour communiquer avec l'agent Blast Extreme.
Serveur de sécurité		ESP	Serveur de connexion		Trafic AJP13 encapsulé lorsque NAT Traversal n'est pas requis. ESP est le protocole IP 50. Les numéros de ports ne sont pas spécifiés.
Serveur de connexion		ESP	Serveur de sécurité		Trafic AJP13 encapsulé lorsque NAT Traversal n'est pas requis. ESP est le protocole IP 50. Les numéros de ports ne sont pas spécifiés.

Comprendre les protocoles de communication

Les composants d'Horizon 6 et Horizon 7 échangent des messages en utilisant plusieurs protocoles différents.

Chiffre 5-5 illustre les protocoles que chaque composant utilise pour communiquer lorsqu'un serveur de sécurité n'est pas configuré. Cela signifie que le tunnel sécurisé pour RDP, Blast Secure Gateway et PColP Secure Gateway ne sont pas activés. Cette configuration peut être utilisée dans un déploiement LAN classique.

Chiffre 5-5. Composants d'Horizon 6 et Horizon 7 et protocoles sans serveur de sécurité

Note Cette figure montre des connexions directes pour des clients utilisant le protocole PCoIP ou RDP. Toutefois, le paramètre par défaut consiste à avoir des connexions directes pour PCoIP et des connexions par tunnel pour RDP.

Consultez [Tableau 5-3](#) pour connaître les ports par défaut utilisés pour chaque protocole.

Chiffre 5-6 illustre les protocoles que chaque composant utilise pour communiquer lorsqu'un serveur de sécurité est configuré. Cette configuration peut être utilisée dans un déploiement WAN classique.

Chiffre 5-6. Composants d'Horizon 6 et Horizon 7 et protocoles avec un serveur de sécurité

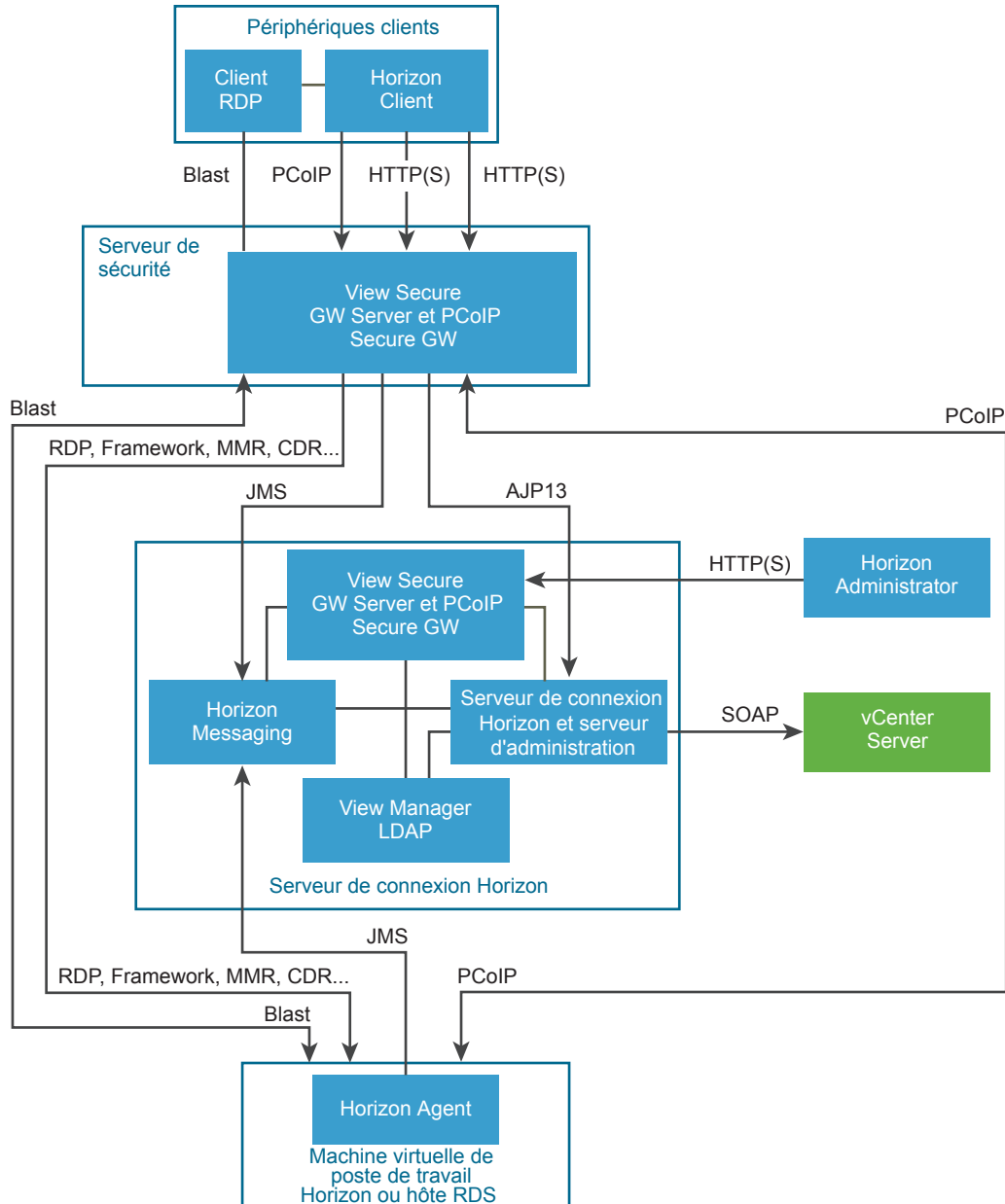


Tableau 5-3 répertorie les ports par défaut utilisés par chaque protocole. Si nécessaire, pour respecter les stratégies d'entreprise ou pour éviter la contention, vous pouvez modifier les numéros de port utilisés.

Tableau 5-3. Ports par défaut

Protocole	Port
JMS	Port TCP 4001
	Port TCP 4002
AJP13	Port TCP 8009
	Note AJP13 n'est utilisé que dans une configuration avec serveur de sécurité.
HTTP	Port TCP 80

Tableau 5-3. Ports par défaut (Suite)

Protocole	Port
HTTPS	Port TCP 443
MMR/CDR	Pour la redirection multimédia et la redirection de lecteur client, port TCP 9427
RDP	Port TCP 3389 Note Si l'instance du Serveur de connexion est configurée pour des connexions client directes, ces protocoles se connectent directement depuis le client au poste de travail distant et ne sont pas envoyés par tunnel via le composant View Secure GW Server.
SOAP	Port TCP 80 ou 443
PCoIP	Port TCP 4172 Ports UDP 4172, 50002, 55000
redirection USB	Port TCP 32111. Ce port est également utilisé pour la synchronisation de fuseau horaire.
VMware Blast Extreme	Ports TCP 8443, 22443 Ports UDP 443, 8443, 22443
HTML Access	Ports TCP 8443, 22443

Ports TCP pour l'intercommunication du Serveur de connexion

Les instances du Serveur de connexion dans un groupe utilisent des ports TCP supplémentaires pour communiquer entre eux. Par exemple, les instances du Serveur de connexion utilisent le port 4100 ou 4101 pour se transmettre le trafic interroutage JMS (JMSIR). Les pare-feu ne sont généralement pas utilisés entre les instances du Serveur de connexion d'un groupe.

View Secure Gateway Server

View Secure Gateway Server est le composant côté serveur pour la connexion sécurisée HTTPS entre des systèmes clients et un serveur de sécurité, un dispositif Unified Access Gateway ou une instance du Serveur de connexion.

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

Note Les clients utilisant le protocole d'affichage PCoIP ou Blast Extreme peuvent utiliser la connexion par tunnel pour la redirection USB et l'accélération MMR (redirection multimédia), mais pour toutes les autres données, PCoIP utilise le composant PCoIP Secure Gateway et Blast Extreme utilise le composant Blast Secure Gateway sur un serveur de sécurité ou un dispositif Unified Access Gateway.

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

Blast Secure Gateway

Les serveurs de sécurité et les dispositifs Unified Access Gateway comprennent un composant Blast Secure Gateway. Lorsque Blast Secure Gateway est activé, après l'authentification, les clients qui utilisent Blast Extreme ou HTML Access peuvent établir une autre connexion sécurisée à un serveur de sécurité ou à un dispositif Unified Access Gateway. Cette connexion permet aux clients d'accéder à des applications et à des postes de travail distants depuis Internet.

Lorsque vous activez le composant Blast Secure Gateway, le trafic Blast Extreme est transmis par un serveur de sécurité ou un dispositif Unified Access Gateway aux applications et aux postes de travail distants. Si des clients utilisant Blast Extreme utilisent également la fonctionnalité de redirection USB ou l'accélération MMR (redirection multimédia), vous pouvez activer le composant View Secure Gateway afin de transmettre ces données.

Lorsque vous configurez des connexions client directes, le trafic Blast Extreme et les autres trafics vont directement d'un client vers une application ou un poste de travail distant.

Lorsque les utilisateurs finaux tels que des travailleurs à domicile ou mobiles accèdent à des postes de travail depuis Internet, des serveurs de sécurité ou des dispositifs Unified Access Gateway fournissent le niveau requis de sécurité et de connectivité donc une connexion VPN n'est pas nécessaire. Le composant Blast Secure Gateway garantit que le seul trafic à distance pouvant entrer dans le centre de données de l'entreprise est le trafic pour le compte d'un utilisateur dont l'authentification est renforcée. Les utilisateurs finaux ne peuvent accéder qu'aux ressources dont l'accès leur est autorisé.

Un client natif Blast qui fonctionne via une passerelle Blast Secure Gateway s'attend à ce que sa connexion TLS de session Blast soit authentifiée par le certificat TLS qui est configuré sur Blast Secure Gateway. Si la connexion Blast du client voit d'autres certificats TLS, la connexion est ignorée et le client signale une incompatibilité d'empreinte de certificat.

Si vous optez pour que le client établisse sa connexion à un proxy de terminaison TLS placé entre le client et la passerelle Blast Secure Gateway, vous pouvez répondre aux exigences de certificat du client et éviter une erreur d'incompatibilité d'empreinte en réglant le proxy pour qu'il présente une copie du certificat (et de la clé privée) de Blast Secure Gateway, ce qui permet la réussite de la connexion Blast à partir du client.

Une alternative à la copie de certificat de la passerelle Blast Secure Gateway sur le proxy consiste à fournir le proxy avec son propre certificat TLS, puis de configurer la passerelle Blast Secure Gateway pour qu'elle conseille au client d'attendre et d'accepter le certificat du proxy plutôt que celui de la passerelle Blast Secure Gateway.

Vous pouvez configurer Blast Secure Gateway dans une passerelle Unified Access Gateway en téléchargeant le certificat du proxy dans **Certificat du proxy Blast** dans les paramètres d'Horizon Unified Access Gateway. Consultez le document *Déploiement et configuration de VMware Unified Access Gateway* à l'adresse <https://docs.vmware.com/fr/Unified-Access-Gateway/index.html>.

Note Seul le certificat du proxy est téléchargé. La clé privée correspondante n'est pas communiquée à la passerelle Unified Access Gateway.

PCoIP Secure Gateway

Les serveurs de sécurité et les dispositifs Unified Access Gateway comprennent un composant PCoIP Secure Gateway. Lorsque PCoIP Secure Gateway est activé, après l'authentification, les clients qui utilisent PCoIP peuvent établir une autre connexion sécurisée à un serveur de sécurité ou un dispositif Unified Access Gateway. Cette connexion permet aux clients d'accéder à des applications et à des postes de travail distants depuis Internet.

Lorsque vous activez le composant PCoIP Secure Gateway, le trafic PCoIP est transmis par un serveur de sécurité ou un dispositif Unified Access Gateway aux applications et aux postes de travail distants. Si des clients utilisant PCoIP utilisent également la fonction de redirection USB ou l'accélération MMR (redirection multimédia), vous pouvez activer le composant View Secure Gateway afin de transmettre ces données.

Lorsque vous configurez des connexions client directes, le trafic PCoIP et les autres trafics vont directement d'un client vers une application ou un poste de travail distant.

Lorsque les utilisateurs finaux tels que des travailleurs à domicile ou mobiles accèdent à des postes de travail depuis Internet, des serveurs de sécurité ou des dispositifs Unified Access Gateway fournissent le niveau requis de sécurité et de connectivité, de sorte qu'une connexion VPN n'est pas nécessaire. Le composant PCoIP Secure Gateway garantit que le seul trafic à distance pouvant entrer dans le centre de données de l'entreprise est le trafic au nom d'un utilisateur dont l'authentification est renforcée. Les utilisateurs finaux ne peuvent accéder qu'aux ressources dont l'accès leur est autorisé.

View LDAP

View LDAP est un répertoire LDAP incorporé dans Serveur de connexion View. Il s'agit également du référentiel de configuration de toutes les données de configuration d'Horizon 7.

View LDAP contient des entrées qui représentent chaque application et poste de travail distant, chaque poste de travail distant accessible, plusieurs postes de travail distants gérés ensemble et des paramètres de configuration de composant Horizon 7.

View LDAP comporte également un ensemble de DLL de plug-in d'Horizon 7 qui fournissent des services d'automatisation et de notification pour d'autres composants d'Horizon 7.

Horizon Messaging

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

Ce composant prend en charge l'API JMS (Java Message Service) qui est utilisée pour la messagerie dans Horizon 7.

La validation du message inter-composant utilise des clés DSA. La taille de la clé est de 512 bits par défaut, sauf en mode FIPS, où la taille de la clé est de 2 048 bits.

Note Lorsque le mode de sécurité des messages est défini sur **Amélioré**, SSL/TLS est utilisé pour sécuriser les connexions JMS plutôt que d'utiliser un chiffrement par message. En mode de sécurité des messages amélioré, la validation s'applique à un seul type de message. Pour le mode des messages amélioré, VMware recommande d'augmenter la taille de la clé à 2 048 bits. Si vous n'utilisez pas le mode de sécurité des messages amélioré, VMware recommande de ne pas modifier la valeur par défaut de 512 bits, car l'augmentation de la taille de la clé affecte les performances et l'évolutivité.

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

Règles de pare-feu pour le Serveur de connexion Horizon

Certains ports doivent être ouverts sur le pare-feu pour les instances du Serveur de connexion et les serveurs de sécurité.

Lorsque vous installez le Serveur de connexion, le programme d'installation peut éventuellement configurer les règles de Pare-feu Windows requises à votre place. Ces règles ouvrent les ports utilisés par défaut. Si vous modifiez les ports par défaut après l'installation, vous devez configurer manuellement le Pare-feu Windows pour permettre à des périphériques Horizon Client de se connecter à Horizon 7 via les ports mis à jour.

Le tableau suivant répertorie les ports par défaut pouvant être ouverts automatiquement lors de l'installation. Les ports sont entrants sauf indication contraire.

Tableau 5-4. Ports ouverts lors de l'installation du Serveur de connexion Horizon

Protocole	Ports	Type d'instance du Serveur de connexion Horizon
JMS	TCP 4001	Standard et réplica
JMS	TCP 4002	Standard et réplica
JMSIR	TCP 4100	Standard et réplica
JMSIR	TCP 4101	Standard et réplica
AJP13	TCP 8009	Standard et réplica
HTTP	TCP 80	Standard, réplica et serveur de sécurité
HTTPS	TCP 443	Standard, réplica et serveur de sécurité
PCoIP	TCP 4172 entrant ; UDP 4172 dans les 2 sens	Standard, réplica et serveur de sécurité

Tableau 5-4. Ports ouverts lors de l'installation du Serveur de connexion Horizon (Suite)

Protocole	Ports	Type d'instance du Serveur de connexion Horizon
HTTPS	TCP 8443	Standard, réplica et serveur de sécurité.
	UDP 8443	Une fois la première connexion à Horizon 7 établie, le navigateur Web ou le périphérique client se connecte à Blast Secure Gateway sur le port TCP 8443. Blast Secure Gateway doit être activé sur un serveur de sécurité ou une instance du Serveur de connexion View pour autoriser cette seconde connexion.
HTTPS	TCP 8472	Standard et réplica Pour la fonctionnalité Architecture Cloud Pod : utilisée pour la communication entre les espaces.
HTTP	TCP 22389	Standard et réplica Pour la fonctionnalité Architecture Cloud Pod : utilisée pour la réplication LDAP globale.
HTTPS	TCP 22636	Standard et réplica Pour la fonctionnalité Architecture Cloud Pod : utilisée pour la réplication LDAP globale sécurisée.

Règles de pare-feu pour View Agent ou Horizon Agent

Les programmes d'installation de View Agent et d'Horizon Agent peuvent éventuellement configurer des règles de pare-feu Windows sur des postes de travail distants et des hôtes RDS pour ouvrir les ports réseau par défaut. Les ports sont entrants sauf indication contraire.

Les programmes d'installation de View Agent et d'Horizon Agent configurent la règle de pare-feu locale pour les connexions RDP entrantes pour qu'elle corresponde au port RDP actuel du système d'exploitation hôte, qui est en général le port 3389.

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

Si vous modifiez le numéro du port RDP après l'installation, vous devez modifier les règles de pare-feu associées. Si vous modifiez un port par défaut après l'installation, vous devez reconfigurer manuellement les règles de pare-feu Windows pour autoriser l'accès sur le port mis à jour. Reportez-vous à la section « Remplacement des ports par défaut pour les services View » dans le document *Installation d'Horizon 7*.

Les règles de pare-feu Windows de View Agent ou d'Horizon Agent sur des hôtes RDS indiquent un bloc de 256 ports UDP contigus ouverts pour le trafic entrant. Ce bloc de ports est destiné à une utilisation interne de VMware Blast dans View Agent ou Horizon Agent. Un pilote spécial signé par Microsoft sur les hôtes RDS bloque le trafic entrant de sources externes vers ces ports. À cause de ce pilote, le pare-feu Windows traite les ports comme étant fermés.

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

Tableau 5-5. Ports TCP et UDP ouverts pendant l'installation de View Agent ou d'Horizon Agent

Protocole	Ports
RDP	Port TCP 3389
Redirection USB et synchronisation de fuseau horaire	Port TCP 32111
MMR (redirection multimédia) et CDR (redirection de lecteur client)	Port TCP 9427
PCoIP	<p>Pour les hôtes RDS, PCoIP utilise les numéros de port suivants : port TCP 4172 et port UDP 4172 (bidirectionnel).</p> <p>Pour les postes de travail, PCoIP utilise les numéros de port choisis dans une plage configurable. Par défaut, les ports TCP 4172 à 4173 et les ports UDP 4172 à 4182. Les règles de pare-feu de ces ports ne spécifient pas les numéros de port, mais suivent dynamiquement les ports ouverts par chaque serveur PCoIP Server. Les numéros de port choisis sont communiqués au client via le Serveur de connexion.</p>
VMware Blast	<p>Port TCP 22443</p> <p>Port UDP 22443 (bidirectionnel)</p> <p>Note UDP n'est pas utilisé sur les postes de travail Linux.</p>
HTML Access	Port TCP 22443
XDMCP	<p>UDP 177</p> <p>Note Ce port est ouvert pour l'accès XDMCP uniquement sur les postes de travail Linux exécutant Ubuntu 18.04. Les règles de pare-feu bloquent tous les accès de l'hôte externe à ce port.</p>
X11	<p>TCP 6100</p> <p>Note Ce port est ouvert pour l'accès XServer uniquement sur les postes de travail Linux exécutant Ubuntu 18.04. Les règles de pare-feu bloquent tous les accès de l'hôte externe à ce port.</p>

Règles de pare-feu pour Active Directory

Si un pare-feu se trouve entre votre environnement Horizon 7 et votre serveur Active Directory, vous devez vous assurer que tous les ports nécessaires sont ouverts.

Par exemple, Serveur de connexion View 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.

Présentation des étapes de configuration d'un environnement Horizon 7

6

Effectuez ces tâches de haut niveau pour installer Horizon 7 et configurer un déploiement initial.

Tableau 6-1. Liste de vérification d'installation et de configuration de Horizon 7

Étape	Tâche
1	Configurez les utilisateurs et les groupes d'administrateurs requis dans Active Directory. Instructions : <i>Installation de Horizon 7</i> et documentation de vSphere.
2	Si ce n'est pas encore fait, installez et configurez les hôtes ESXi et vCenter Server. Instructions : documentation de VMware vSphere.
3	(Facultatif) Si vous êtes sur le point de déployer des postes de travail de clone lié, installez View Composer sur le système vCenter Server ou sur un serveur séparé. Aussi, installez la base de données View Composer. Instructions : document <i>Installation de Horizon 7</i> .
4	Installez et configurez le Serveur de connexion Horizon. Aussi, installez la base de données des événements. Instructions : document <i>Installation de Horizon 7</i> .
5	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 ou des pools de postes de travail d'Instant Clone. Instructions : <i>Configuration des postes de travail virtuels dans Horizon 7</i> .
6	(Facultatif) Configurez un hôte RDS et installez les applications devant être utilisées à distance par des utilisateurs finaux. Instructions : <i>Configuration d'applications et de postes de travail publiés dans Horizon 7</i> .
7	Créez des pools de poste de travail, des pools d'applications ou les deux. Instructions : <i>Configuration des postes de travail virtuels dans Horizon 7</i> et <i>Configuration d'applications et de postes de travail publiés dans Horizon 7</i> .
8	Contrôlez l'accès des utilisateurs aux postes de travail. Instructions : <i>Configuration des fonctionnalités de poste de travail distant dans Horizon 7</i> .
9	Installez Horizon Client sur des machines d'utilisateurs finaux et demandez aux utilisateurs d'accéder à leurs applications et à leurs postes de travail distants. Instructions : documentation d'Horizon Client à l'adresse https://docs.vmware.com/fr/VMware-Horizon-Client/index.html .
10	(Facultatif) Créez et configurez des administrateurs supplémentaires pour autoriser différents niveaux d'accès à des objets d'inventaire et des paramètres spécifiques. Instructions : document <i>Administration de Horizon 7</i> .

Tableau 6-1. Liste de vérification d'installation et de configuration de Horizon 7 (Suite)

Étape	Tâche
11	(Facultatif) Configurez des stratégies pour contrôler le comportement de composants de Horizon 7, de pools d'applications et de postes de travail, et d'utilisateurs finaux. Instructions : <i>Configuration des fonctionnalités de poste de travail distant dans Horizon 7.</i>
12	(Facultatif) Configurez Horizon Persona Management, ce qui permet aux utilisateurs d'accéder à des données et à des paramètres personnalisés lorsqu'ils ouvrent une session sur un poste de travail. Instructions : <i>Configuration des postes de travail virtuels dans Horizon 7.</i>
13	(Facultatif) Pour une sécurité améliorée, intégrez une solution d'authentification par carte à puce ou d'authentification à deux facteurs RADIUS. Instructions : document <i>Administration de Horizon 7.</i>