Planification de l'architecture Horizon

VMware Horizon 2111

vmware®

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

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

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

Table des matières

Planification de l'architecture Horizon

Planification de l'architecture Horizon présente VMware Horizon™. Il décrit ses principales fonctionnalités et options de déploiement et présente le mode de configuration générale des composants dans un environnement de production.

Ce guide répond à la question suivante :

- Le produit résout-il les problèmes pour lesquels vous avez besoin d'une solution ?

Toutes les fonctionnalités et capacités de VMware Horizon sont disponibles dans toutes les éditions de licence. Pour comparer les fonctionnalités de chaque édition, consultez la page https://www.vmware.com/products/horizon.html.

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 VMware Horizon répond aux exigences de leur entreprise pour fournir de façon efficace et sécurisée des applications et des postes de travail virtuels à leurs utilisateurs finaux.

Présentation de VMware Horizon 1

Avec VMware Horizon, 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. 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 VMware Horizon

Les avantages de VMware Horizon incluent la simplicité, la sécurité, la vitesse et la montée en charge pour fournir des applications et des postes de travail virtuels avec des économies et une souplesse comme dans le cloud.

Déploiements flexibles de VMware Horizon

VMware Horizon offre la possibilité de déployer des applications et des postes de travail virtuels sur site, dans un environnement hébergé dans le cloud ou un mélange hybride des deux. Divers environnements de déploiement peuvent nécessiter des licences différentes.

Vous pouvez déployer VMware Horizon dans les environnements suivants.

Déploiement sur site

Vous pouvez déployer VMware Horizon sur des infrastructures sur site ou dans un cloud privé. Vous pouvez utiliser une licence perpétuelle pour un déploiement sur site. Vous pouvez éventuellement acheter la licence d'abonnement Horizon qui permet d'accéder au Horizon Control Plane et aux services associés.

Déploiement hébergé dans le cloud

Vous pouvez déployer VMware Horizon dans un cloud public, tel que VMware Cloud on AWS ou les solutions Azure VMware. Vous devez utiliser une licence d'abonnement pour le

déploiement dans un cloud public. Avec la licence d'abonnement, vous disposez des options permettant d'accéder au Horizon Control Plane et aux services associés.

Déploiement hybride

Vous pouvez disposer de déploiements de VMware Horizon sur site, ainsi que dans des environnements hébergés dans le cloud. Vous pouvez lier ces déploiements dans une fédération. Dans ce scénario de déploiement hybride, vous pouvez disposer des déploiements suivants :

- Utilisez la licence perpétuelle pour vos déploiements sur site et utilisez une licence d'abonnement pour vos déploiements hébergés dans le cloud.
- Utilisez la licence d'abonnement pour vos déploiements sur site ainsi que vos déploiements hébergés dans le cloud.

Connexion de vos déploiements Horizon au Horizon Control Plane

Pour utiliser la licence d'abonnement et accéder au Horizon Control Plane, vous devez utiliser le dispositif virtuel Horizon Cloud Connector pour connecter votre déploiement d'Horizon au plan de contrôle Horizon.

Horizon Control Plane (activé par la licence d'abonnement) offre les avantages suivants lorsqu'il est connecté à vos déploiements d'Horizon :

- Horizon Universal Console fournit une console unifiée unique dans les déploiements sur site et multicloud pour l'utilisation de la flotte d'espaces connectés au cloud de votre locataire.
- L'orchestration hybride multicloud fournit un workflow unique pour activer les technologies JMP (Just-in-Time Management Platform) de VMware.
- Horizon Universal Broker est la technologie d'intermédiation basée sur le cloud qui permet de gérer les ressources virtuelles de vos attributions multicloud et de les allouer à vos utilisateurs finaux.
- Cloud Monitoring Service (CMS) est l'un des services centraux fournis dans le plan de contrôle Horizon. Il vous offre la possibilité de surveiller la capacité, l'utilisation et la santé des composants de l'ensemble de vos espaces connectés au cloud, quels que soient les environnements de déploiement dans lesquels ces espaces individuels résident.
- Le service de gestion des images Horizon est un service basé sur le cloud qui simplifie et automatise la gestion des images système utilisées par les attributions de poste de travail, telles que les pools de postes de travail et les batteries de serveurs, dans vos espaces Horizon connectés au cloud.
- Le document *Planification de l'architecture Horizon* fournit une présentation et la configuration requise de déploiement de VMware Horizon. Pour plus d'informations sur la Horizon Control Plane, consultez la documentation d'VMware Horizon Cloud Service.

Just-in-Time Management Platform (JMP)

JMP représente les capacités de VMware Horizon permettant de fournir des applications et des postes de travail virtuels juste-à-temps qui sont flexibles, rapides et personnalisés. JMP inclut les technologies VMware suivantes.

Instant Clones

Instant Clone est une technologie de clonage basée sur vSphere utilisée pour provisionner des milliers de postes de travail virtuels non persistants à partir d'une image standard unique. Les postes de travail Instant Clone offrent les avantages suivants :

- Vitesse d'approvisionnement rapide qui dure 1 à 2 secondes en moyenne pour créer un poste de travail.
- Fournit un poste de travail vierge haute performance chaque fois qu'un utilisateur se connecte.
- Améliore la sécurité en détruisant le poste de travail chaque fois qu'un utilisateur se déconnecte.
- Élimine le besoin de disposer d'un poste de travail dédié pour chaque utilisateur individuel.
- Aucune interruption de service pour l'application de correctifs à un pool de postes de travail.
- Vous pouvez coupler des Instant Clones avec VMware App Volumes et VMware Dynamic Environment Manager pour fournir des postes de travail entièrement personnalisés.

VMware App Volumes

VMware App Volumes est un système unifié et intégré de gestion d'utilisateurs et de distribution d'applications pour VMware Horizon et d'autres environnements virtuels. VMware App Volumes offre les avantages suivants :

- Approvisionnement rapide des applications à grande échelle.
- Attachement dynamique des applications à des utilisateurs, des groupes ou des périphériques, même lorsque les utilisateurs sont déjà connectés à leur poste de travail.
- Approvisionnement, fourniture, mise à jour et retrait d'applications en temps réel.
- Fourniture d'un volume accessible en écriture par l'utilisateur. Cela permet aux utilisateurs d'installer des applications qui suivent sur les postes de travail.

VMware Dynamic Environment Manager

VMware Dynamic Environment Manager offre une personnalisation et une configuration de stratégie dynamique dans tout environnement virtuel, physique et basé sur le cloud. VMware Dynamic Environment Manager offre les avantages suivants :

- Accès rapide des utilisateurs finaux à un espace de travail Windows et aux applications, avec une expérience personnalisée et cohérente pour les périphériques et les emplacements.
- Simplification de la gestion des profils d'utilisateurs finaux en fournissant aux organisations une solution unique et évolutive qui tire parti de l'infrastructure existante.
- Accélération du processus de connexion en appliquant les paramètres de configuration et d'environnement dans un processus asynchrone plutôt que la totalité lors de la connexion.
- Configuration d'un environnement dynamique, par exemple les mappages de lecteur ou d'imprimante, lorsqu'un utilisateur lance une application.

Outre l'utilisation des trois technologies JMP sous-jacentes, vous pouvez également orchestrer leur utilisation dans un workflow unique à partir de l'assistant Attribution dans le plan de contrôle Horizon.

Fiabilité et sécurité

Vous pouvez centraliser les postes de travail et applications en intégrant VMware vSphere® et en virtualisant les 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 SecurelD, VASCO DIGIPASS, SMS Passcode et SafeNet, entre autres.
- L'intégration à VMware Workspace ONE Access signifie que les utilisateurs finaux disposent d'un 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 une application. 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.
- 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.

- 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.

Intégration étroite à l'écosystème de VMware

Vous pouvez utiliser VMware Horizon avec VMware vSphere, vSAN, NSX pour étendre la puissance de la virtualisation avec le calcul virtuel, le stockage virtuel, la mise en réseau virtuelle et la sécurité pour réduire les coûts, améliorer l'expérience utilisateur et offrir une plus grande réactivité. Vous pouvez effectuer votre déploiement sur un cloud public tel que VMware Cloud on AWS ou les solutions Azure VMware.

Vous pouvez également exploiter des logiciels de gestion supplémentaires, tels que vRealize, Avi Networks et Carbon Black.

Expérience utilisateur riche

VMware Horizon fournit l'environnement de poste de travail connu et personnalisé que les utilisateurs finaux attendent, y compris les expériences utilisateur suivantes :

- Sélection riche de protocoles d'affichage.
- Possibilité d'accéder à des périphériques USB et autres connectés à leur ordinateur local.
- Envoi de documents vers n'importe quelle imprimante détectable par leur ordinateur local.
- Fonctionnalités audio/vidéo en temps réel.
- Authentification par carte à puce.
- Utilisation de plusieurs moniteurs d'affichage.
- Prise en charge des graphiques 3D.

RESTful API

Les RESTful API VMware Horizon automatisent le déploiement, le fonctionnement, la gestion, la surveillance, les rapports et les analyses de l'infrastructure, des charges de travail et de l'intégration de VMware Horizon à des produits tiers. Vous pouvez utiliser ces API pour effectuer les fonctions suivantes :

- Gestion du pool de postes de travail
- Gestion des machines virtuelles et des batteries de serveurs
- Publication d'applications
- Autorisation d'accès à des applications publiées
- Détection de l'infrastructure
- Surveillance et dépannage

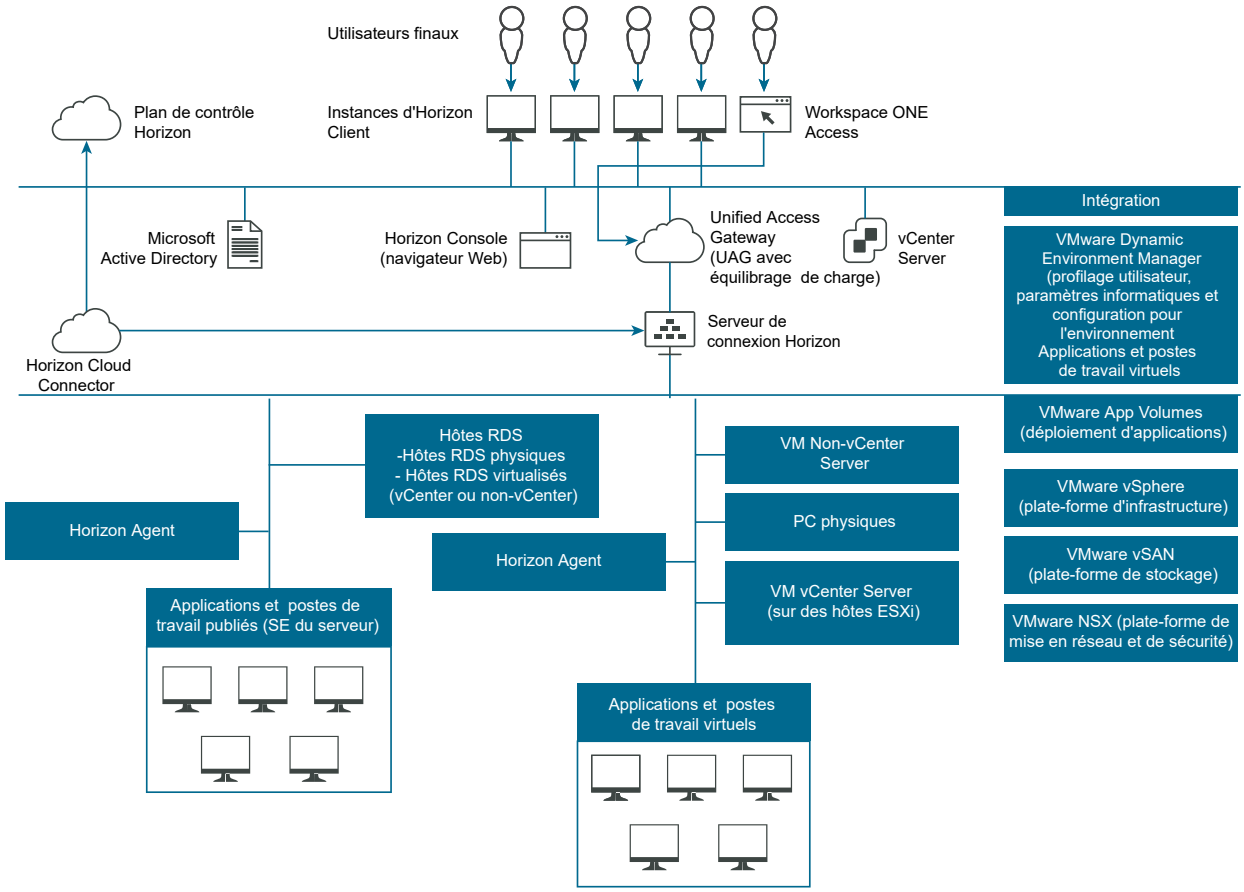
Pour plus d'informations sur les RESTful API VMware Horizon, consultez les RESTful API disponibles sur https://code.vmware.com/apis/1122/view-rest-api. Pour obtenir une liste des API RESTful d'Horizon pour chaque version, reportez-vous à l'article 84155 de la base de connaissances.

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.

L'exemple général d'un environnement VMware Horizon montre les relations entre les principaux composants d'un déploiement de VMware Horizon.

Figure 1-1. Exemple général d'un environnement VMware Horizon



Périphériques clients

Le principal avantage de l'utilisation d'VMware Horizon 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 VMware Horizon Thin Client et peuvent être configurés pour que la seule application pouvant être lancée par les utilisateurs directement sur le périphérique soit VMware Horizon Thin Client. Requalifier un PC hérité en poste de travail de client léger peut allonger la durée de vie du matériel de trois à cinq ans. Par exemple, en utilisant VMware Horizon sur un poste de travail léger, vous pouvez utiliser un système d'exploitation plus récent, comme Windows 10, 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 ;
- 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 un dispositif Unified Access Gateway. Les dispositifs Unified Access Gateway de la zone DMZ communiquent avec les Serveurs de connexion dans le pare-feu d'entreprise. 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 d'entreprise est celui pour le compte d'un utilisateur dont l'authentification est renforcée. Les utilisateurs ne peuvent accéder qu'aux ressources dont l'accès leur est autorisé.

Pour plus d'informations sur les dispositifs Unified Access Gateway, reportez-vous à la documentation d'Unified Access Gateway à l'adresse https://docs.vmware.com/fr/Unified-Access-Gateway/index.html.

Important Il est possible de créer une installation d'VMware Horizon sans utiliser le Serveur de connexion. Si vous installez le plug-in View Agent Direct Connect sur un poste de travail de machine virtuelle distante, 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, reportez-vous au document *Administration du plug-in View Agent Direct-Connection* .

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.

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 telles que le contrôle des connexions, l'impression intégrée et l'accès à des périphériques USB connectés localement.

Si la source de poste de travail est une machine virtuelle, vous devez d'abord installer le service Horizon Agent sur cette machine virtuelle, puis utiliser celle-ci comme modèle ou image standard des 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 Console

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, vous obtenez également l'URL de l'interface Web d'Horizon Console. Cette interface Web 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.

vCenter Server

Si vous déployez Horizon sur vSphere, vCenter Server fait office d'administrateur central des serveurs VMware ESXi 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'VMware Horizon, notamment des instances du Horizon Connection Server, des serveurs Active Directory, des hôtes RDS Microsoft et des instances de vCenter Server.

Intégration de VMware Horizon

Pour améliorer l'efficacité d'VMware Horizon dans votre entreprise, vous pouvez utiliser plusieurs interfaces pour intégrer VMware Horizon 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 d'VMware Horizon avec un logiciel de Business Intelligence

Vous pouvez configurer Horizon Connection Server pour enregistrer des événements dans une base de données Microsoft SQL Server, Oracle ou PostgreSQL.

- 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 *Administration d'Horizon*.

Vous pouvez également générer des événements VMware Horizon 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*.

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 applets de commande Horizon PowerCLI, consultez la *Référence des applets de commande VMware PowerCLI* disponible sur https://code.vmware.com/docs/6978/cmdlet-reference.

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 Horizon 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 VMware Horizon.

- 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.
- 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 VMware Horizon

Lorsque vous utilisez Horizon Console pour modifier la configuration de VMware Horizon, les données LDAP appropriées dans le référentiel sont mises à jour. L'Horizon Connection Server 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 VMware Horizon. Ces commandes sont destinées aux administrateurs avancés qui souhaitent utiliser des scripts pour mettre à jour des données de configuration sans utiliser Horizon Console 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 VMware Horizon, tels que des pools de postes de travail, et ajouter ces objets à vos instances du Serveur de connexion sans utiliser Horizon Console 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 *Administration d'Horizon*.

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 Console ou qui doivent être exécutées automatiquement depuis des scripts.

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

Planification d'une expérience d'utilisateur riche

2

VMware Horizon fournit l'environnement de poste de travail familier 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.

VMware Horizon 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

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 invités pris en charge dépendent de la version de Windows.

Pour obtenir une liste des systèmes d'exploitation invités Windows 10, consultez l'article https://kb.vmware.com/s/article/78714 de la base de connaissances VMware.

Pour connaître les systèmes d'exploitation Windows autres que Windows 10, consultez l'article https://kb.vmware.com/s/article/78715 de la base de connaissances 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'VMware Horizon. 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 qui sont compatibles avec H.264, HEVC, JPEG, PNG et le codec Blast propriétaire. De tous les protocoles d'affichage, VMware Blast Extreme est celui qui offre la consommation du 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.

Vous pouvez utiliser le protocole d'affichage VMware Blast Extreme 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 des connexions chiffrées et sécurisées à un dispositif Unified Access Gateway dans la zone DMZ de l'entreprise.

  Note Il n'est pas recommandé d'utiliser le VPN, car les connexions Blast sont déjà chiffrées. Pour une meilleure expérience utilisateur, utilisez plutôt le dispositif Unified Access Gateway.

- 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, vous pouvez 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 Windows. 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.

- Le codec Blast s'améliore sur les encodeurs adaptatifs et H.264 lors de l'utilisation de postes de travail en offrant des images et des polices plus nettes. Il fonctionne comme un codec vidéo avec détection de mouvement, vecteurs de mouvement et macroblocs inter-prédits. Il est pris en charge dans les environnements suivants et désactivé par défaut :
  - Agents Windows et Linux. Pour activer le codec :
    - Sur un agent Windows, définissez la clé de registre : `HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderBlastCodecEnabled = 1`
    - Sur un agent Linux : `\etc\vmware\config`, définissez `RemoteDisplay.allowBlastCodec=TRUE`
  - Désactivez H.264 et HEVC sur les paramètres du client Windows, Linux et MacOS. Cette fonctionnalité n'est pas prise en charge sur les clients mobiles et le client Web.
- Un commutateur d'encodeur dynamique vous permet de basculer entre un encodeur vidéo optimisé (H.264 4:2:0 ou H.264 4:4:4) et un encodeur de texte optimisé (codec Blast ou adaptatif). Ce commutateur permet de garantir la netteté du texte et des images vidéo tout en réduisant l'utilisation de la bande passante. Pour utiliser cette fonctionnalité, activez le commutateur de codage :
  - Sur un agent Windows, définissez la clé de registre `HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1`
  - Sur un agent Linux : `\etc\vmware\config`, définissez `RemoteDisplay.allowSwitchEncoder=TRUE`
  - Activez le codec Blast, qui est désactivé par défaut. Si le codec Blast n'est pas activé, l'encodeur de commutation utilise l'encodage Adaptatif pour le texte optimisé.
  - Activez H.264 sur les paramètres du client Windows, Linux et MacOS. Cette fonctionnalité n'est pas prise en charge sur les clients mobiles et le client Web.

  Note Le commutateur d'encodeur utilise uniquement le logiciel H.264 et ne prend pas en charge les graphiques à accélération matérielle.
- Blast Extreme implémente le codage HDR (High Dynamic Range), qui augmente la plage de luminosité d'une image numérique pour fournir une représentation plus réaliste d'une scène. HDR est activé par défaut sur l'agent. Vous pouvez ajouter ces clés de registre facultatives REG_SZ (valeur de chaîne) sur un agent Windows :
  - `PixelProviderHDRReferenceWhite` : un nombre entier supérieur à 0 qui contrôle la luminosité relative du niveau blanc du papier. La valeur par défaut est 80.
  - `TopologyHDREnabled = 1` pour activer HDR. La valeur par défaut est 1.
  - `TopologyHDREnabled = 0` pour désactiver HDR.

  Sur le client, définissez la clé de registre facultative REG_SZ (valeur de chaîne) `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Client\AllowClientHDR` sur True ou False pour les demandes de topologie HDR. La valeur par défaut est True.

Dans les paramètres du client VMware Blast, **Autoriser le format HEVC (High Efficiency Video Coding)** et **Autoriser le décodage de plage dynamique élevée (HDR)**.

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 de l'écran maximale est 1 920 x 1 200.

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 société ou établir une connexion chiffrée et sécurisée avec un dispositif Unified Access Gateway dans la zone DMZ d'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 avec une résolution de 4K (3 840 x 2 160). 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 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.

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 de connexion Horizon, 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 VMware Horizon fonctionnent de la même façon que les autres solutions d'accès à distance aux applications. Les applications publiées par VMware Horizon sont fournies à l'aide du protocole d'affichage Blast Extreme ou PCoIP, pour une expérience utilisateur optimisée.

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 255 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*.

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 webcams et de 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 avec vSphere, cette fonctionnalité permet de partager un GPU (Graphical Processing Unit) physique sur un hôte ESXi entre des machines virtuelles. Utilisez cette fonctionnalité si vous avez besoin de graphiques de workstation haut de gamme accélérés par le matériel.

AMD MxGPU

Disponible avec vSphere, cette fonctionnalité permet à plusieurs machines virtuelles de partager un GPU AMD en faisant apparaître le GPU sous la forme de plusieurs périphériques 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 avec vSphere, 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 Consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php. 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 avec vSphere, 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 avec vSphere, permettent d'exécuter des applications DirectX 9 et OpenGL 2.1 sans nécessiter aucun GPU physique. Utilisez cette fonctionnalité pour les applications 3D moins exigeantes, comme les thèmes Windows Aero, Microsoft Office 2010 et Google Earth.

Important Consultez le Livre blanc de VMware concernant l'accélération graphique sur vSphere. Les options de rendu varient selon l'environnement (vSphere, non vSphere et PC physique) et des cas d'utilisation (postes de travail virtuels et postes de travail publiés). Pour connaître les options 3D disponibles spécifiques à votre environnement et cas d'utilisation, consultez les documents *Configuration des postes de travail virtuels dans Horizon* et *Configuration d'applications et de postes de travail publiés dans Horizon*. Pour plus d'informations sur les différents choix de rendu 3D, consultez le Guide de déploiement de NVIDIA GRID vGPU pour VMware Horizon 6.1 et le Guide d'utilisateur de NVIDIA GRID Virtual GPU.

Diffusion multimédia sur un poste de travail distant

La fonctionnalité Windows Media MMR (redirection multimédia), pour postes de travail et clients, 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. 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 de MMR est 9427 pour une connexion PCoIP.

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*.

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 au 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.
- - Les postes de travail virtuels Windows Server 2019 requièrent Horizon Agent 7.7 ou version ultérieure.
  - Les postes de travail virtuels Windows 7 et Windows 8.x ne sont pas pris en charge avec Horizon Agent 2006 et versions ultérieures.
- Avec le protocole d'affichage VMware Blast, une résolution d'écran de poste de travail distant de 8 000 pixels (7680 x 4320) est prise en charge. Deux affichages de 8 000 pixels sont pris en charge. La version matérielle de la machine virtuelle de poste de travail doit être 14 (ESXi 6.7 ou version ultérieure). Vous devez allouer suffisamment de ressources système sur la machine virtuelle pour prendre en charge un affichage de 8 000 pixels. Pour plus d'informations sur les configurations de moniteur prises en charge pour les postes de travail basés sur GRID et pour les profils de vGPU NVIDIA, reportez-vous au *Guide de l'utilisateur du logiciel des GPU virtuels* sur le site Web de NVIDIA. Cette fonctionnalité n'est prise en charge qu'avec le client Windows.
- Avec le protocole d'affichage VMware Blast ou PCoIP, la résolution de l'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 10.

Version du matériel	Nombre d'écrans 4K pris en charge
10 (compatible avec ESXi 5.5.x)	1
11 (compatible avec ESXi 6.0)	3
11	1
13, 14 ou version ultérieure	1 (fonctionnalité de rendu 3D activée) 4 (fonctionnalité de rendu 3D désactivée)

Pour optimiser les performances, la machine virtuelle doit disposer d'au moins 2 Go de RAM et de 2 vCPU. Cette fonction peut nécessiter de bonnes conditions de réseau, telles qu'une bande passante de 1 000 Mbit/s avec une faible latence du réseau et un taux de perte de paquets réduit.

Note Lorsque la résolution de l'écran de poste de travail distant est définie sur 3 840 x 2 160 (4K), les éléments sur l'écran peuvent sembler plus petits, et il peut vous être impossible d'utiliser la boîte de dialogue Résolution de l'écran sur le poste de travail distant pour agrandir le texte et les autres éléments. Sur un client Windows, vous pouvez définir le DPI de la machine cliente sur le paramètre approprié et activer la fonctionnalité de synchronisation DPI afin de rediriger le paramètre DPI de la machine cliente vers le poste de travail distant.

- 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-vsphere/index.html

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

3

Vous pouvez créer des pools qui incluent un ou plusieurs 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 VMware Horizon 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 :

Pools de postes de travail

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

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

- Une machine virtuelle hébergée sur un hôte ESXi et gérée par vCenter Server.
- 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* dans Horizon.
- Une machine non-vSphere telle qu'un PC de poste de travail physique.
- Une machine virtuelle s'exécutant sur une plate-forme de virtualisation autre que vCenter Server qui prend en charge Horizon Agent.

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

L'utilisation de pools pour gérer des postes de travail vous permet d'appliquer des paramètres ou de déployer des applications sur tous les postes de travail distants dans un pool. Pour plus d'informations sur les pools de postes de travail de machines virtuelles ou de machines non gérées, consultez le document *Configuration des postes de travail virtuels dans Horizon*. Pour plus d'informations sur les pools de postes de travail basés sur des sessions sur des hôtes RDS, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon*.

Pools d'applications

Avec les pools d'applications qui s'exécutent sur une batterie de serveurs d'hôtes RDS, vous autorisez les utilisateurs à accéder à des applications publiées qui s'exécutent sur des serveurs dans un centre de données plutôt que sur leurs ordinateurs ou périphériques personnels.

Les pools d'applications offrent plusieurs avantages importants :

- Accessibilité

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

- Indépendance des périphériques

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

- Contrôle d'accès

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

- Déploiement accéléré

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

- Facilité de gestion

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

- Sécurité et conformité réglementaire

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

- Réduction du coût

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

Approvisionnement d'applications

Avec VMware Horizon, vous disposez de plusieurs options concernant l'approvisionnement d'applications.

- Déployez des applications publiées à l'aide d'hôtes RDS. Reportez-vous à la section Déploiement d'applications publiées à l'aide d'un hôte RDS.
- Déployez des applications publiées qui s'exécutent sur des pools de postes de travail avec des applications hébergées de machine virtuelle. Reportez-vous à la section Déploiement d'applications publiées qui s'exécutent sur des pools de postes de travail avec des applications hébergées de machine virtuelle.
- Déployez des applications dans des postes de travail virtuels. Reportez-vous à la section Déploiement d'applications dans des postes de travail virtuels.
- Déployez des applications à l'aide de VMware App Volumes. Vous pouvez regrouper des applications et les envoyer à vos utilisateurs à l'aide de VMware App Volumes. Lorsque vos utilisateurs se connectent à leurs postes de travail distants, leurs applications sont attachées à leurs postes de travail. Pour plus d'informations, consultez la documentation de VMware App Volumes sur https://docs.vmware.com/fr/VMware-App-Volumes/index.html.

- Distribuez les modules d'application créés avec VMware ThinApp. Pour plus d'informations sur la distribution de modules d'application créés avec VMware ThinApp, reportez-vous à la documentation de VMware ThinApp sur https://docs.vmware.com/fr/VMware-ThinApp/index.html.
- Déploiement d'applications publiées 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 publiées qui s'exécutent sur des pools de postes de travail avec des applications hébergées de machine virtuelle

  Vous pouvez fournir une ou plusieurs applications publiées aux utilisateurs finaux sans créer de batterie de serveurs d'hôtes RDS. Vous pouvez créer un pool de postes de travail de machine virtuelle pour héberger les applications, puis exposer les utilisateurs finaux aux applications publiées uniquement.
- Déploiement d'applications dans des postes de travail virtuels

  Vous pouvez déployer des applications sur l'image standard et créer un pool de postes de travail tous identiques avec exactement la même copie d'applications.

Déploiement d'applications publiées 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 publiées qui s'exécutent sur des pools de postes de travail avec des applications hébergées de machine virtuelle

Vous pouvez fournir une ou plusieurs applications publiées aux utilisateurs finaux sans créer de batterie de serveurs d'hôtes RDS. Vous pouvez créer un pool de postes de travail de machine virtuelle pour héberger les applications, puis exposer les utilisateurs finaux aux applications publiées uniquement.

Cette approche avantage les types d'applications suivants.

Cette stratégie simplifie l'utilisation des types d'application suivants.

- Applications qui nécessitent la compatibilité de la version de .NET Framework.
- Applications qui nécessitent une prise en charge spéciale des périphériques, où les pilotes peuvent ne pas s'exécuter ou être pris en charge sur les hôtes RDS.
- Applications testées et certifiées uniquement sous Windows 10.
- Applications qui nécessitent une licence d'installation et des rapports d'utilisation par des fournisseurs de logiciels indépendants.

Pour plus d'informations, reportez-vous au document « Meilleures pratiques pour les applications et postes de travail publiés dans VMware Horizon et VMware Horizon Apps » disponible sur https://techzone.vmware.com.

Déploiement d'applications dans des postes de travail virtuels

Vous pouvez déployer des applications sur l'image standard et créer un pool de postes de travail tous identiques avec exactement la même copie d'applications.

Si vous déployez un pool de postes de travail d'Instant Clone, lorsque qu'il s'agit d'appliquer des correctifs aux applications sur tous les postes de travail, il suffit de mettre à jour l'image standard et d'utiliser la fonctionnalité d'image de transfert pour propager rapidement les modifications sur tous les postes de travail du pool de manière progressive. Lorsqu'un utilisateur se déconnecte d'un poste de travail virtuel d'Instant Clone, VMware Horizon supprime l'Instant Clone et crée un Instant Clone à partir de la dernière version de l'image standard. Ce nouveau clone est prêt pour la connexion de l'utilisateur suivant. Avec les mises à jour propagées, le temps d'arrêt lié à la maintenance de pool peut être réduit.

Vous pouvez utiliser cette fonctionnalité 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

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

VMware Horizon comporte de nombreux modèles d'administration ADMX de stratégie de groupe pour centraliser la gestion et la configuration de composants VMware Horizon 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 dans l'interface utilisateur d'Horizon Console. 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 au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Utilisation de stratégies de carte à puce avec Dynamic Environment Manager

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 nécessite Dynamic 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 Dynamic 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

Ce chapitre traite des directives de planification et des éléments de conception de l'architecture qui incluent 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 d'avoir une connaissance pratique de tous les éléments impliqués dans le déploiement d'une solution VMware Horizon.

Pour plus d'informations sur la définition de l'architecture d'un déploiement de VMware Horizon, consultez le document « Architecture de référence de VMware Workspace ONE et de VMware Horizon » disponible à l'adresse https://techzone.vmware.com.

Important Ce chapitre n'aborde pas les rubriques suivantes :

Conception de l'architecture pour les applications hébergées	Un espace VMware Horizon 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, reportez-vous au document *Configuration d'applications et de postes de travail publiés dans Horizon*. Si vous prévoyez d'utiliser des machines virtuelles pour les hôtes RDS, voir aussi Configuration d'une machine virtuelle hôte RDS.
Conception de l'architecture pour le plug-in View Agent Direct-Connection	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, reportez-vous au document *Administration du plug-in View Agent Direct-Connection* .

Ce chapitre contient les rubriques suivantes :

- Blocs constitutifs VMware Horizon
- Espaces Horizon
- Avantages à utiliser plusieurs vCenter Server dans un groupe
- Présentation de Architecture Cloud Pod

Configuration requise du système d'exploitation invité 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 du personnel

  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 personnel qui utilise le poste de travail virtuel et des applications qui doivent être installées.

- Types de postes de travail

  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. L'utilisation de postes de travail persistants ou non dépend du type de travailleur spécifique.

- 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.

- 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 VMware Horizon.

- 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.

Planification en fonction du personnel

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 personnel 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.

Personnel d'exécution

Le personnel d'exécution et le personnel administratif 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. L'ensemble du personnel d'exécution ayant des horaires spécifiques peut ouvrir simultanément une session sur les postes de travail virtuels. Le personnel d'exécution comprend 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'applications et les personnes qui utilisent des applications gourmandes en fonction graphique. Ces utilisateurs et applications ont tendance à consommer beaucoup de CPU et de mémoire. Ces considérations doivent donc être prises en compte dans le processus d'architecture.

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 nécessitent une ouverture de session automatique. L'authentification peut être effectuée via certaines applications si nécessaire.

Types de postes de travail

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. L'utilisation de postes de travail persistants ou non dépend du type de travailleur spécifique.

Poste de travail persistant

Les postes de travail persistants contiennent des données dans l'image du système d'exploitation elle-même qui doivent être préservées, conservées et sauvegardées. Par

exemple, ces utilisateurs qui doivent installer certaines de leurs propres applications ou qui possèdent des données qui ne peuvent pas être enregistrées en dehors de la machine virtuelle elle-même (comme sur un serveur de fichiers ou dans une base de données d'applications) ont besoin d'un poste de travail persistant.

Il existe plusieurs façons de créer des postes de travail persistants dans VMware Horizon :

Vous pouvez créer des pools automatisés de machines virtuelles de clone complet.

Si vous avez déjà créé des postes de travail virtuels ou des postes de travail physiques (machines virtuelles vCenter, machines virtuelles non-vCenter ou PC physiques), vous pouvez les importer dans VMware Horizon en tant que postes de travail persistants à l'aide du pool de postes de travail manuel avec une attribution dédiée.

Les postes de travail persistants offrent aux utilisateurs le plus haut niveau de flexibilité et de contrôle sur leurs propres postes de travail. Cependant, ils consomment plus de ressources de calcul et leur gestion est plus difficile par l'informatique. Ces postes de travail peuvent nécessiter des techniques de gestion d'image traditionnelles. Les postes de travail persistants peuvent avoir de faibles coûts de stockage avec certaines technologies de système de stockage. Étant donné que chaque poste de travail persistant est unique et doit être conservé, les technologies de sauvegarde et de récupération sont importantes lors de l'examen des stratégies de continuité d'activité.

Poste de travail non persistant

Les postes de travail non persistants sont des images sans état identiques les unes aux autres. Ils sont principalement utilisés par les utilisateurs qui n'ont pas besoin d'installer ou de conserver leurs propres applications. Les postes de travail non persistants ont plusieurs avantages. Ils 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 d'activité plus faciles et moins coûteuses. Les postes de travail virtuels ne doivent pas nécessairement être protégés, car il n'y a pas de données d'utilisateur uniques stockées. En cas de destruction des postes de travail virtuels, vous pouvez simplement les recréer à partir de l'image standard. La redirection de dossiers et diverses technologies de profil peuvent éventuellement être utilisées pour stocker des données de profil d'utilisateur et d'utilisateur.

Dans VMware Horizon, vous pouvez créer des postes de travail non persistants en exploitant les Instant Clones. Pour plus d'informations sur les Instant Clones, consultez le document *Configuration des postes de travail virtuels dans Horizon*.

Postes de travail pour le personnel d'exécution

Étant donné que le personnel d'exécution effectue des tâches répétitives dans un petit ensemble d'applications, vous pouvez utiliser des postes de travail non persistants, ce qui permet d'économiser sur les coûts de stockage et de calcul et de simplifier la gestion des postes de travail.

Postes de travail pour les travailleurs du savoir et les utilisateurs expérimentés

Les travailleurs du savoir doivent généralement créer des documents complexes et les conserver. Les utilisateurs expérimentés doivent souvent installer leurs propres applications et les conserver. En fonction de la nature et de la quantité de données personnelles qui doivent être conservées, elles nécessitent un poste de travail non persistant ou un poste de travail persistant.

Pour les travailleurs qui doivent installer leurs propres applications, ce qui ajoute des données au disque du système d'exploitation, la meilleure option consiste à créer un poste de travail persistant à l'aide de machines virtuelles de clone complet.

Postes de travail pour les 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 configurés pour s'exécuter en mode Kiosque utilisent des postes de travail non persistants, 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.

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*.

Pour plus d'informations sur la création de pools de postes de travail pour des types spécifiques de travailleurs, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon*.

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, cela peut affecter l'E/S de stockage en raison de la pagination Windows excessive. Si l'allocation de RAM est trop élevée, cela peut affecter la capacité de stockage, car le fichier de pagination dans le système d'exploitation invité 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 sélectionner un paramètre trop conservateur. Tenez compte des éléments suivants :

- 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.
- Étant donné que les performances des postes de travail virtuels sont sensibles aux temps de réponse, VMware recommande de réserver toute la mémoire.

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 l'accès à celui-ci est fréquent.

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 égaler 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. Capacité supplémentaire d'affichage du client PCoIP ou Blast Extreme 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.

Note Les résolutions UHD 5K et 8K ne sont disponibles que lors de l'utilisation du protocole Blast et uniquement pour les configurations à 1 ou 2 moniteurs. Si vous tentez de lancer une session PCoIP avec un moniteur 5K ou 8K configuré sur le client, la session échoue.

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

Standard de résolution d'affichage	Largeur (pixels)	Hauteur (pixels)	Capacité supplémentaire de 1 moniteur (Mo)	Capacité supplémentaire de 2 moniteurs (Mo)	Capacité supplémentaire de 3 moniteurs (Mo)	Capacité supplémentaire de 4 moniteurs (Mo)
VGA	640	480	1,20	3.20	4,80	5,60
WXGA	1 280	800	4,00	12,50	18,75	25,00
1 080 p	1 920	1 080	8,00	25,40	38,00	50,60
WQXGA	2 560	1 600	16,00	60,00	84,80	109,60
UHD (4K)	3 840	2 160	32,00	78,00	124,00	170,00

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

Standard de résolution d'affichage	Largeur (pixels)	Hauteur (pixels)	Capacité supplémentaire de 1 moniteur (Mo)	Capacité supplémentaire de 2 moniteurs (Mo)	Capacité supplémentaire de 3 moniteurs (Mo)	Capacité supplémentaire de 4 moniteurs (Mo)
5K Blast uniquement	5 120	2 880	64,00	128,00	NA	NA
UHD (8K) Blast uniquement	7 680	4 320	128,00	256,00	NA	NA

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

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 Console 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 capacité supplémentaire est précalculée pour plus de deux moniteurs afin de prendre en charge 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 Console, correspondent au système hôte, ou ajustez manuellement la quantité de mémoire en sélectionnant **Gérer à l'aide de vSphere Client** dans Horizon Console, 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.

L'allocation de 2 Go pour des postes de travail Windows 10 ou version ultérieure est un bon point de départ. Si vous souhaitez utiliser l'une des fonctionnalités de graphiques à accélération matérielle pour les charges de travail 3D, VMware vous recommande de prévoir deux 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 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 pools de postes de travail d'Instant Clone plutôt que des pools de postes de travail de machines virtuelles complètes pour vos postes de travail virtuels. Avec les Instant Clones, vous pouvez appliquer un correctif à l'image standard et utiliser l'image de transfert pour propager le correctif progressivement dans votre pool de postes de travail. Cela évite le goulot d'étranglement de mise à jour logicielle généralement associé au logiciel de gestion des correctifs traditionnel qui télécharge et met à jour le correctif directement sur chaque poste de travail virtuel individuel.
- Planifiez les mises à jour antivirus et logicielles pour qu'elles s'exécutent à des heures de faible activité, lorsque peu d'utilisateurs sont susceptibles de se connecter.
- Échelonnez ou randomisez les dates des mises à jour.
- Utilisez un logiciel antivirus sans agent compatible avec les capacités de VMware NSX Guest Introspection.

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*.
- Choisissez une taille de disque virtuel suffisante pour permettre une croissance future, mais qui n'est pas trop importante.
- Utilisez des partages de fichiers centralisés ou App Volumes pour le contenu généré par l'utilisateur et les applications installées par l'utilisateur.
- Activez la récupération d'espace pour que vCenter Server récupère automatiquement l'espace utilisé par les données périmées ou supprimées d'un système d'exploitation invité.

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 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.

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 VMware Horizon.

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 stratégies organisationnelles liées au stockage des données.

Les recommandations présentées dans le tableau suivant concernent un poste de travail de machine virtuelle Windows 10 standard.

Tableau 4-2. Exemple de machine virtuelle de poste de travail pour Windows 10

Élément	Exemple
Système d'exploitation	Windows 10 (avec le dernier Service Pack)
RAM	4 Go
CPU virtuel	2
Capacité de disque système	24 Go (un peu moins que la norme)
Type d'adaptateur SCSI virtuel	Sélectionnez LSI Logic SAS ou VMware Paravirtual (PVSCSI). L'utilisation de PVSCSI peut nécessiter des étapes supplémentaires en fonction de la version de Windows à installer. Pour plus d'informations, reportez-vous à l'article Configuration des disques pour utiliser les contrôleurs VMware Paravirtual SCSI (PVSCSI) (1010398) de la base de connaissances VMware.
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 2012 R2 64 bits
RAM	24 Go
CPU virtuel	4
Capacité de disque système	40 Go
Type d'adaptateur SCSI virtuel	Sélectionnez LSI Logic SAS ou VMware Paravirtual (PVSCSI). L'utilisation de PVSCSI peut nécessiter des étapes supplémentaires en fonction de la version de Windows à installer. Pour plus d'informations, reportez-vous à l'article Configuration des disques pour utiliser les contrôleurs VMware Paravirtual SCSI (PVSCSI) (1010398) de la base de connaissances VMware.
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.

Nœud ESXi

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

VMware Horizon est plus rentable lorsque vous optimisez le taux de consolidation, qui est le nombre de machines virtuelles (utilisées en tant que postes de travail ou hôtes RDS) hébergées sur un hôte ESXi. Le taux de consolidation est généralement déterminé par la quantité de CPU, de RAM et de stockage disponible pour l'hôte ESXi, ainsi que la quantité requise par machine virtuelle en tenant compte des ressources de capacité supplémentaire requises pour les

composants d'infrastructure. Bien que de nombreux facteurs affectent la sélection du serveur, si vous effectuez une optimisation uniquement pour le prix d'acquisition, vous devez rechercher des configurations de serveur qui disposent d'un équilibre approprié de puissance de traitement, de mémoire et de stockage. Utilisez les instructions suivantes :

- 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 les exigences de calcul de CPU pour chaque machine virtuelle, consultez la section Estimation des exigences de CPU pour les postes de travail de machine virtuelle.
- Considérez la capacité de mémoire en termes de RAM de poste de travail virtuel et de RAM d'hôte. 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 VMware Horizon, la fonctionnalité View Storage Accelerator est activée par défaut, ce qui permet à des hôtes ESXi de mettre en cache des données de disque de machine virtuelle communes. View Storage Accelerator peut améliorer les performances et réduire le besoin de bande passante d'E/S de stockage supplémentaire pour gérer des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus. Cette fonctionnalité nécessite jusqu'à 32 Go de RAM par hôte ESXi. Pour plus d'informations sur View Storage Accelerator, consultez la section « Configuration de View Storage Accelerator pour vCenter Server » dans le document *Installation d'Horizon*.
- Enfin, prenez en considération des exigences de cluster et de basculement. Pour plus d'informations sur la détermination des exigences de haute disponibilité sur les clusters vSphere, reportez-vous à la section Déterminer des exigences de haute disponibilité.

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

Configuration de machine virtuelle vCenter Server

Lorsque vous déployez VMware Horizon dans un environnement vSphere, vous devez déployer et configurer vCenter Server.

Vous pouvez installer vCenter Server sur le même cluster d'hôtes ESXi que celui sur lequel votre infrastructure Horizon et vos charges de travail s'exécuteront, ou sur un cluster différent. Pour plus d'informations sur le dimensionnement du système vCenter Server en fonction du nombre attendu de machines virtuelles qu'il gérera, reportez-vous à la section Configuration matérielle requise pour vCenter Server Appliance.

Nombre maximal d'instances d'Horizon Connection Server et configuration

Vous pouvez installer l'Horizon Connection Server sur un serveur physique ou dans une machine virtuelle.

Exemple de configuration du Serveur de connexion

Cet exemple utilise une machine virtuelle avec les spécifications répertoriées dans l'exemple de machine virtuelle du 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 4-4. 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 *Installation d'Horizon*.
RAM	10 Go
CPU virtuel	4
Capacité de disque système	70 Go
Type d'adaptateur SCSI virtuel	Sélectionnez LSI Logic SAS ou VMware Paravirtual (PVSCSI). L'utilisation de PVSCSI peut nécessiter des étapes supplémentaires en fonction de la version de Windows à installer. Pour plus d'informations, reportez-vous à l'article Configuration des disques pour utiliser les contrôleurs VMware Paravirtual SCSI (PVSCSI) (1010398) de la base de connaissances VMware.
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*.

Nombre maximal de connexions pour le Serveur de connexion

L'article https://kb.vmware.com/s/article/2150348 de la base de connaissances VMware fournit des informations sur les limites testées concernant le nombre de connexions simultanées qu'un déploiement de VMware Horizon peut recevoir.

Des connexions PCoIP Secure Gateway sont requises si vous utilisez 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 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 dispositifs Unified Access Gateway pour les connexions RDP en dehors du réseau d'entreprise et pour la redirection USB et l'accélération de la redirection multimédia (MMR) avec une connexion PCoIP ou Blast Secure Gateway.

Bien que le dispositif Unified Access Gateway puisse prendre en charge un maximum de 2 000 connexions simultanées, vous pouvez choisir d'en utiliser 2 ou 4. La quantité requise de mémoire et d'utilisation du CPU peut indiquer la nécessité d'ajouter des dispositifs Unified Access Gateway supplémentaires par instance du Serveur de connexion pour répartir la charge.

Bien que 5 instances du Serveur de connexion (correctement configurées) puissent gérer 20 000 connexions, vous pouvez envisager d'utiliser 6 ou 7 Serveurs de connexion à des fins de planification de la disponibilité et recevoir les 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 4 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 3 dispositifs Unified Access Gateway, à équilibrage de charge sur les deux instances du Serveur de connexion. De cette façon, si l'une devient indisponible, les 2 dispositifs restants peuvent 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 VMware Horizon

VMware vous recommande d'utiliser 2 vCPU et 4 Go de RAM pour que les dispositifs Unified Access Gateway prennent en charge le nombre maximal de connexions lorsqu'ils sont utilisés avec VMware Horizon.

Tableau 4-5. Configuration matérielle requise pour Unified Access Gateway

Élément	Exemple
Système d'exploitation	OVA
RAM	4 Go
CPU virtuel	2
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)
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'VMware Horizon peuvent utiliser des clusters VMware HA pour se protéger contre les pannes du serveur physique.

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'VMware Horizon 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'VMware Horizon, consultez l'article de la base de connaissances de VMware https://kb.vmware.com/s/article/2150348.

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*. 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 de postes de travail non persistants peut comporter des exigences d'objectif de point de récupération (RPO) différentes de celles d'un pool de postes de travail persistants. Pour un pool non persistant, nous recommandons aux utilisateurs de se connecter à un poste de travail différent si celui 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 l'objectif 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.

Considérations relatives à la conception du stockage et de la 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.

- Considérations relatives au stockage partagé

  Les critères de conception du stockage sont un des éléments les plus importants pour la réussite d'une architecture VMware Horizon.

- Considérations de bande passante de stockage

  Dans un environnement VMware Horizon, 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.

Considérations relatives au stockage partagé

Les critères de conception du stockage sont un des éléments les plus importants pour la réussite d'une architecture VMware Horizon.

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 SAN Fibre Channel, SAN iSCSI 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.

Vous pouvez utiliser VMware vSAN qui virtualise les disques SSD locaux physiques et les disques durs 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. Pour plus d'informations sur vSAN, reportez-vous à la documentation de vSphere à l'adresse https://docs.vmware.com/fr/VMware-vSphere/index.html. Pour plus d'informations sur les meilleures pratiques, reportez-vous au livre blanc technique Meilleures pratiques de VMware Horizon on VMware vSAN.

Pour plus d'informations sur la configuration du stockage pour Horizon, reportez-vous à la section « Gestion du stockage pour les postes de travail virtuels » du document *Configuration des postes de travail virtuels dans Horizon*.

Considérations de bande passante de stockage

Dans un environnement VMware Horizon, 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 VMware Horizon, 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 VMware Horizon 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.

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 stratégies de fermeture de session au cours d'une phase pilote pour déterminer si l'interruption ou la mise hors tension des machines virtuelles, lorsque des utilisateurs ferment leur session, provoque une tempête d'E/S.

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

Considérations de bande passante réseau

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

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.

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, reportez-vous aux sections « Paramètres généraux PCoIP » et « Paramètres de stratégie VMware Blast » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Blocs constitutifs VMware Horizon

Un bloc constitutif est une construction logique qui peut contenir un certain nombre de machines virtuelles. Un bloc constitutif est composé de serveurs physiques, d'une infrastructure vSphere, de serveurs VMware Horizon, d'un stockage partagé et de postes de travail de machine virtuelle

pour les utilisateurs finaux. L'évolutivité de chaque bloc est déterminée par le nombre de machines virtuelles que vous déployez par vCenter Server.

Tableau 4-6. Exemple de bloc constitutif Horizon sur un réseau local pour 4 000 postes de travail de machine virtuelle

Élément	Exemple
Clusters vSphere	1
Commutateur de réseau à 80 ports	1
Système de stockage partagé	1
vCenter Server	1 (peut être exécuté dans le bloc lui-même)
Base de données	Serveur de base de données MS SQL Server, Oracle ou PostgreSQL (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)

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

Espaces Horizon

Un espace Horizon est une unité d'organisation déterminée par les limites d'extensibilité de VMware Horizon. Vous pouvez créer un espace Horizon avec un certain nombre de blocs constitutifs. Chaque espace Horizon est une unité de gestion et dispose d'une interface utilisateur de gestion d'Horizon Console distincte.

Exemple d'espace utilisant deux blocs constitutifs

Tableau 4-7. Exemple d'un espace Horizon basé sur un LAN composé de 2 blocs constitutifs

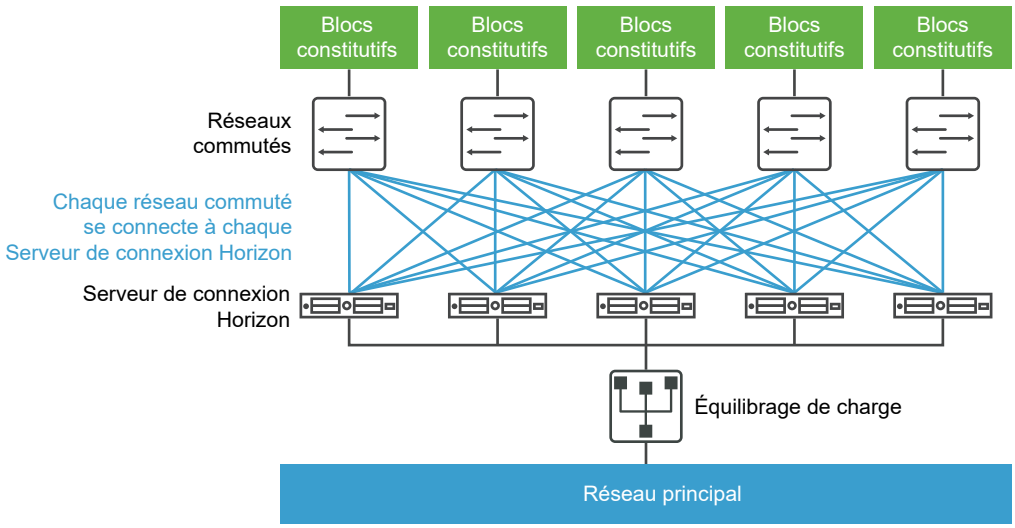
Élément	Nombre
Blocs constitutifs d'un espace Horizon	2
vCenter Server	2
Serveur de base de données	2 serveurs de base de données MS SQL Server, Oracle ou PostgreSQL (1 serveur de base de données autonome dans chaque bloc constitutif)
Serveurs de connexion	7 (5 pour les connexions de l'intérieur du réseau d'entreprise et 2 pour les connexions de l'extérieur)
vLAN	Reportez-vous à la section Tableau 4-6. Exemple de bloc constitutif Horizon sur un réseau local pour 4 000 postes de travail de machine virtuelle.
Module Ethernet 10 Gbits	1
Commutateur de réseau modulaire	1

En fonction de la configuration spécifique, chaque vCenter Server peut prendre en charge un grand nombre de machines virtuelles. Cette prise en charge permet de disposer de grands blocs constitutifs de postes de travail de machine virtuelle. Toutefois, la taille de bloc réelle est également soumise à d'autres limites propres à VMware Horizon.

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.

Figure 4-1. Schéma d'un espace pour des postes de travail de machine virtuelle



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

Dans la section précédente, l'espace Horizon était composé de plusieurs blocs constitutifs. Chaque bloc constitutif prenait en charge 5 000 machines virtuelles avec une seule instance de vCenter Server. Cette rubrique illustre une architecture basée sur l'utilisation d'une seule instance de vCenter Server pour gérer 10 000 postes de travail.

Même s'il est possible de n'utiliser qu'une seule instance de vCenter Server pour 10 000 postes de travail, cela crée une situation impliquant un point de défaillance unique. La perte de cette instance de vCenter Server unique 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 VMware Horizon, un stockage partagé et 5 clusters de 2 000 postes de travail virtuels chacun.

Tableau 4-8. Exemple d'un espace Horizon basé sur un réseau local avec une seule instance de vCenter Server

Élément	Exemple
Clusters vSphere	6 (5 clusters avec un pool d'Instant Clones par cluster et 1 cluster d'infrastructure)
vCenter Server	1
Serveur de base de données	1 serveur de base de données MS SQL Server, Oracle ou PostgreSQL (autonome)
Serveur Active Directory	1 ou 2
Instances du Serveur de connexion	5
Dispositifs Unified Access Gateway	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)

Avantages à utiliser plusieurs vCenter Server dans un groupe

Avant d'essayer de gérer un grand nombre de machines virtuelles avec une seule instance de vCenter Server, vous devez prendre en compte les considérations suivantes.

- Durée des fenêtres de maintenance de votre entreprise
- Capacité de tolérance aux pannes des composants d'VMware Horizon
- 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	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. 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 VMware Horizon à grande échelle, cette opération d'approvisionnement peut prendre beaucoup de temps.
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 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, VMware Horizon 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 unitaire de panne dans toutes les conceptions de VMware Horizon.

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 possiblité 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'VMware Horizon 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 l'Horizon Connection Server 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 VMware Horizon 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 instance seule de vCenter Server dans une conception de VMware Horizon à grande échelle offre certains avantages irréfutables, tels qu'un emplacement unique permettant de gérer des machines virtuelles d'image standard, un affichage unique de vCenter Server permettant de faire correspondre l'affichage d'Horizon Console 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 rapport aux inconvénients, tels que la lourdeur des tâches administratives pour gérer des images de machine virtuelle d'image standard 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.

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. Vous pouvez utiliser la fonctionnalité Architecture Cloud Pod pour connecter des espaces s'exécutant sur site, sur un cloud public ou un mélange des deux. Pour plus d'informations, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon*.

Planification des fonctions de sécurité

5

VMware Horizon offre une sécurité réseau renforcée pour protéger les données d'entreprise sensibles. Pour renforcer la sécurité, vous pouvez intégrer VMware Horizon à certaines solutions d'authentification utilisateur tierces et implémenter la fonctionnalité d'autorisations limitées.

Important VMware Horizon peut effectuer des opérations cryptographiques à l'aide d'algorithmes compatibles FIPS (Federal Information Processing Standard, norme de traitement d'informations fédérales) 140-2. Il est possible d'activer l'utilisation de ces algorithmes en installant VMware Horizon 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*.

Ce chapitre contient les rubriques suivantes :

Comprendre les connexions client

Horizon Client et Horizon Console 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 ou d'Unified Access Gateway. La connexion Horizon Console est créée lorsqu'un administrateur entre l'URL Horizon Console 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 consultent une page sécurisée telle qu'Horizon Console.

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 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 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 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 sur les dispositifs virtuels Unified Access Gateway, consultez le document *Déploiement et configuration de VMware 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 VMware Horizon 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 dispositif Unified Access Gateway.

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 PCoIP Secure Gateway et Blast Extreme utilise Blast Secure Gateway sur 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 de VMware 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

VMware Horizon utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs. Pour une sécurité améliorée, vous pouvez intégrer VMware Horizon 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 d'Horizon Connection Server et sur le poste de travail distant à l'aide de Kerberos. 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 `vdmadmin` pour configurer le filtrage de domaines, qui limite les domaines qu'une instance du Serveur de connexion recherche et qu'elle affiche aux utilisateurs. Pour plus d'informations, consultez le document *Administration d'Horizon*.

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.
- VMware Horizon fournit également une interface d'extension standard ouverte pour permettre aux fournisseurs de solutions tiers d'intégrer des extensions d'authentification avancées dans VMware Horizon.

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 distants de l'extérieur du réseau d'entreprise, sur Internet.

VMware Horizon 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 d'Horizon Connection Server et sur le poste de travail distant à l'aide de Kerberos. 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*.

- 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.

  Lorsque vous sélectionnez **Autoriser l'ouverture de session en tant qu'utilisateur actuel**, vous pouvez activer les paramètres utilisateur suivants :

  - Autoriser les clients hérités : prise en charge des clients plus anciens. Les versions 2006 et 5.4, et les versions antérieures d'Horizon Client sont considérées comme des clients plus anciens.
  - Autoriser le recours NTLM : utilise l'authentification NTLM au lieu de Kerberos lorsqu'il n'existe aucun accès au contrôleur de domaine. Vous devez activer les paramètres de stratégie de groupe NTLM dans la configuration d'Horizon Client.
  - Désactiver les liaisons de canal : couche de sécurité supplémentaire permettant de sécuriser l'authentification NTLM. Par défaut, les liaisons de canal sont activées sur le client.
  - Intégration de l'authentification unique réelle : activez ce paramètre sur le Serveur de connexion pour autoriser SSO sur le poste de travail à l'aide de l'authentification unique réelle. Par exemple, en mode imbriqué, l'authentification unique réelle permet de se connecter à un client imbriqué, puis une connexion de poste de travail secondaire est effectuée. Pour plus d'informations sur le mode imbriqué, reportez-vous à la section *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.
    - Désactivé : l'utilisateur doit entrer des informations de connexion si le client n'a pas reçu d'informations d'identification d'ouverture de session.

- Facultatif : les informations d'identification du client sont utilisées, le cas échéant. Sinon l'authentification unique réelle est utilisée. Il s'agit du paramètre recommandé si les options Authentification unique réelle et Connexion en tant qu'utilisateur actuel sont activées.
- Activé : l'authentification unique réelle est utilisée pour se connecter au poste de travail.

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.

Note La fonctionnalité de déverrouillage récursif peut être lente lorsque vous utilisez l'option Se connecter en tant qu'utilisateur actuel avec l'authentification NTLM si Horizon Client ne peut pas accéder aux contrôleurs de domaine. Pour atténuer ce problème, activez le paramètre de stratégie de groupe **Toujours utiliser NTLM pour les serveurs** dans le dossier **Configuration de VMware Horizon Client > Paramètres de sécurité > Paramètres NTLM** dans l'Éditeur de gestion de stratégie de groupe.

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.

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'VMware Horizon peut comporter deux instances du Serveur de connexion. La première instance prend en charge les utilisateurs internes. La deuxième instance est couplée avec un dispositif Unified Access Gateway 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 dispositif Unified Access Gateway 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 ».

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 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

VMware Horizon 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 VMware Horizon pour se connecter à des postes de travail distants.

Consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon* 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 des Stratégies de carte à puce pour les paramètres d'environnement utilisateur dans une application ou un poste de travail publié, ainsi que pour les paramètres d'environnement d'ordinateur qui s'appliquent lors du démarrage de l'ordinateur ou de la reconnexion de session.

Vous pouvez créer des stratégies pour les paramètres d'environnement utilisateur qui contrôlent une gamme de comportements. Les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur sont appliquées lors de la connexion et peuvent être actualisées lors de la reconnexion d'une session. Pour réappliquer les stratégies de carte à puce Horizon lorsqu'un utilisateur se reconnecte à une session, vous pouvez configurer une tâche déclenchée.

Vous pouvez créer des stratégies pour les paramètres d'environnement de l'ordinateur que Dynamic Environment Manager applique lorsque les ordinateurs des utilisateurs finaux démarrent. Les stratégies de carte à puce Horizon pour les paramètres d'environnement ordinateur sont appliquées lors du démarrage de l'ordinateur et peuvent être actualisées lors de la reconnexion d'une session.

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 nécessite Dynamic 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*.

Pour plus d'informations sur l'utilisation de Stratégies de carte à puce pour contrôler le comportement des fonctionnalités sur un poste de travail Linux distant, reportez-vous à la section *Configuration des postes de travail Linux dans Horizon*.

Implémentation de meilleures pratiques pour sécuriser des systèmes client

Implémentez les meilleures pratiques pour sécuriser des systèmes client.

- Configurez les systèmes clients pour qu'ils passent en veille après une certaine période d'inactivité et exigez que les utilisateurs entrent un mot de passe avant le réveil de 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 obtenir une référence succincte à toutes les fonctionnalités de sécurité fournies par VMware Horizon, reportez-vous au document *Sécurité d'Horizon*.

Affectation de rôles d'administrateur

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

L'autorisation d'effectuer des tâches dans Horizon Console 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 Console.

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 Console. 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 Console inclut un ensemble de rôles prédéfinis. Les administrateurs peuvent également créer des rôles personnalisés en combinant des privilèges sélectionnés.

Comprendre les protocoles de communication

Les composants de VMware Horizon utilisent plusieurs protocoles différents pour échanger des messages.

Le tableau suivant répertorie les ports par défaut utilisés par chaque protocole. Vous pouvez modifier les numéros de port. Par exemple, vous devrez peut-être modifier les numéros de port pour vous conformer aux stratégies d'organisation ou pour éviter la contention.

Tableau 5-1. Ports par défaut

Protocole	Port
JMS	Port TCP 4001 Port TCP 4002
HTTP	Port TCP 80
HTTPS	Port TCP 443
MMR/CDR	Port TCP 9427 Les fonctionnalités suivantes utilisent ce port. ■ Redirection multimédia Windows ■ Redirection du lecteur client ■ Optimisation de Microsoft Teams ■ Redirection multimédia HTML ■ Redirection de l'imprimante VMware ■ Redirection USB
RDP	Port TCP 3389 **Note** Si l'instance du Serveur de connexion est configurée pour des connexions clientes directes, ces protocoles se connectent directement depuis le client au poste de travail distant et ne sont pas envoyés par tunnel via le composant Serveur Horizon Secure Gateway.
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.

Tableau 5-1. Ports par défaut (suite)

Protocole	Port
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.

Passerelle de sécurité Horizon

La passerelle de sécurité Horizon est le composant côté serveur pour la connexion HTTPS sécurisée entre des systèmes clients, 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 de redirection multimédia (MMR) est transmis par tunnel via le composant de la passerelle de sécurité Horizon. Lorsque vous configurez des connexions clientes directes, ces protocoles se connectent directement du client au poste de travail distant et ne sont pas transmis par tunnel via le composant de la passerelle de sécurité Horizon.

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 de la redirection multimédia (MMR), mais pour toutes les autres données, PCoIP utilise PCoIP Secure Gateway et Blast Extreme utilise Blast Secure Gateway sur un dispositif Unified Access Gateway.

La passerelle de sécurité Horizon est également responsable du transfert de tout autre trafic Web, y compris l'authentification utilisateur et le trafic de sélection de poste de travail et d'application, des clients vers le Serveur de connexion. La passerelle de sécurité Horizon transmet également le trafic Web du client Horizon Console au composant d'administration Horizon.

Blast Secure Gateway

Les dispositifs Unified Access Gateway incluent 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 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 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 de la redirection multimédia (MMR), 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, les dispositifs Unified Access Gateway fournissent le niveau requis de sécurité et de connectivité. Une connexion VPN n'est donc 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 instance de 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 numérique de certificat.

Si vous optez pour que le client établisse sa connexion à un proxy de terminaison TLS placé entre le client et Blast Secure Gateway, vous pouvez répondre aux exigences de certificat du client et éviter une erreur d'incompatibilité d'empreinte numérique 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 Blast Secure Gateway sur le proxy consiste à fournir le proxy avec son propre certificat TLS, puis à configurer Blast Secure Gateway pour qu'il conseille au client d'attendre et d'accepter le certificat du proxy plutôt que celui de Blast Secure Gateway.

Vous pouvez configurer Blast Secure Gateway dans une instance d'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 Unified Access Gateway.

PCoIP Secure Gateway

Les dispositifs Unified Access Gateway incluent un composant PCoIP Secure Gateway. Lorsque le composant PCoIP Secure Gateway est activé, après l'authentification, les clients qui utilisent PCoIP peuvent établir une autre connexion sécurisée 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 PCoIP Secure Gateway, le trafic PCoIP est transmis par un dispositif Unified Access Gateway aux applications et aux postes de travail distants. Si des clients utilisant PCoIP utilisent également la fonctionnalité de redirection USB ou l'accélération de la redirection multimédia (MMR), vous pouvez activer le composant de la passerelle de sécurité Horizon 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, les dispositifs Unified Access Gateway fournissent le niveau requis de sécurité et de connectivité. Une connexion VPN n'est donc 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.

Horizon LDAP

Horizon LDAP est un annuaire LDAP intégré dans le Serveur de connexion. Il constitue le référentiel de configuration pour toutes les données de configuration de VMware Horizon.

Horizon 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 VMware Horizon.

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

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 VMware Horizon.

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.

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.

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 VMware Horizon 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 5-2. 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
HTTPS	TCP 443	Standard, réplica
PCoIP	TCP 4172 entrant ; UDP 4172 dans les 2 sens	Standard, réplica
HTTPS	TCP 8443 UDP 8443	Standard, réplica Une fois la première connexion à VMware Horizon 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 une instance du Serveur de connexion 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 Horizon Agent

Pour ouvrir les ports réseau par défaut, le programme d'installation d'Horizon Agent configure facultativement des règles de pare-feu Windows sur des postes de travail virtuels et des hôtes RDS.

Le programme d'installation d'Horizon Agent configure la règle de pare-feu locale pour les connexions RDP entrantes afin 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 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 pour autoriser l'accès sur le port mis à jour. Pour plus d'informations, reportez-vous au document *Installation d'Horizon*.

Sur les hôtes RDS, les règles de pare-feu Windows pour Horizon Agent 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 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 Microsoft.

Le tableau suivant répertorie les ports TCP et UDP qui sont ouverts lors de l'installation d'Horizon Agent. Les ports sont entrants sauf indication contraire.

Tableau 5-3. Ports TCP et UDP ouverts lors de l'installation d'Horizon Agent

Protocole	Ports
RDP	Port TCP 3389
Redirection USB et synchronisation de fuseau horaire	Port TCP 32111
Redirection multimédia (MMR) et redirection du lecteur client (CDR)	Port TCP 9427 Les fonctionnalités suivantes utilisent ce port : ■ Redirection multimédia Windows ■ Redirection du lecteur client ■ Optimisation de Microsoft Teams ■ Redirection multimédia HTML ■ Redirection de l'imprimante VMware ■ Redirection USB
PCoIP	Pour les hôtes RDS, PCoIP utilise le port TCP 4172 et le port UDP 4172 (bidirectionnel). Pour les postes de travail virtuels, PCoIP utilise les numéros de port sélectionnés dans une plage configurable. Par défaut, PCoIP utilise les ports TCP 4172 à 4173 et les ports UDP 4172 à 4182. Les règles de pare-feu ne spécifient pas de numéros de port. Au lieu de cela, elles suivent dynamiquement les ports ouverts par chaque instance de PCoIP Server. Les numéros de port sélectionnés sont communiqués au client via l'instance du Serveur de connexion.
VMware Blast	Port TCP 22443 Port UDP 22443 (bidirectionnel) **Note** UDP n'est pas utilisé sur les postes de travail Linux.

Tableau 5-3. Ports TCP et UDP ouverts lors de l'installation d'Horizon Agent (suite)

Protocole	Ports
HTML Access	Port TCP 22443
XDMCP	UDP 177 **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.
X11	TCP 6100 **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.

Règles de pare-feu pour Active Directory

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

Par exemple, le Serveur de connexion 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 droits 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 VMware Horizon

6

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

Tableau 6-1. Liste de vérification d'installation et de configuration de VMware Horizon

Étape	Tâche
1	Configurez les utilisateurs et les groupes d'administrateurs requis dans Active Directory. Instructions : *Installation d'Horizon* 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.
4	Installez et configurez le Serveur de connexion Horizon. Aussi, installez la base de données des événements. Instructions : document *Installation d'Horizon*.
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 d'Instant Clone. Instructions : *Configuration des postes de travail virtuels dans Horizon*.
6	(Facultatif) Configurez un hôte RDS et installez les applications devant être utilisées à distance par des utilisateurs finaux. Instructions : *Configuration d'applications et de postes de travail publiés dans Horizon*.
7	Créez des pools de postes de travail virtuels et publiés, des pools d'applications, ou les deux. Instructions : *Configuration des postes de travail virtuels dans Horizon* et *Configuration d'applications et de postes de travail publiés dans Horizon*.
8	Contrôlez l'accès des utilisateurs aux postes de travail. Instructions : *Configuration des fonctionnalités de poste de travail distant dans Horizon*.
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 *Administration d'Horizon*.

Tableau 6-1. Liste de vérification d'installation et de configuration de VMware Horizon (suite)

Étape	Tâche
11	(Facultatif) Configurez des stratégies pour contrôler le comportement de composants de VMware Horizon, de pools d'applications et de postes de travail, et d'utilisateurs finaux. Instructions : *Configuration des fonctionnalités de poste de travail distant dans Horizon*.
13	(Facultatif) Pour une sécurité améliorée, intégrez une solution d'authentification par carte à puce ou d'authentification à deux facteurs RADIUS. Instructions : document *Administration d'Horizon*.