Sécurité de vCloud Director

VMware Cloud Director 9.5
vCloud Director 9.1

vmware®

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Introduction 1

VMware vCloud Director est un système flexible destiné à fournir des services de Cloud Computing. Il met à profit et étend les technologies centrales de virtualisation et gestion de VMware pour la prise en charge des environnements cloud.

Étant donné que le système a été développé et testé en ayant à l'esprit les fonctionnalités d'architecture mutualisée, d'évolutivité et différents problèmes de sécurité, la façon dont il est déployé peut avoir un impact significatif sur la sécurité de l'ensemble du système. Ce document décrit certaines menaces possibles auxquelles le système est confronté, ainsi que les fonctionnalités de sécurité fournies par l'ensemble de la pile logicielle VMware et les composants connexes qu'elle utilise, tels que les bases de données.

Aucun ensemble de consignes ne peut couvrir tous les cas d'utilisation client possibles. Chaque déploiement de vCloud Director peut avoir son propre environnement informatique, qui peut présenter des différences dans la topologie réseau, les systèmes et les normes de sécurité internes, les exigences des clients et les cas d'utilisation. Nous allons vous donner des instructions générales pour accroître la sécurité globale du système. Dans les situations appropriées, nous vous fournirons des scénarios d'utilisation plus spécifiques ainsi que des conseils adaptés à ces cas particuliers. Néanmoins, les recommandations spécifiques de ce guide que vous choisirez de suivre dépendront finalement de votre propre environnement de déploiement, ainsi que des menaces que vous considérez comme un risque pour votre entreprise et que vous souhaitez limiter.

En général, les menaces qu'encourt vCloud Director se répartissent en deux blocs : les menaces internes et les menaces externes. Les menaces internes impliquent généralement des problèmes liés à l'architecture mutualisée tandis que les menaces externes ciblent la sécurité de l'environnement cloud hébergé, mais ces classements ne sont pas absolus. Des menaces internes peuvent viser la sécurité de l'environnement d'hébergement, par exemple.

Outre les recommandations données dans ce document, vous devez consulter les avertissements de sécurité à l'adresse http://www.vmware.com/security/advisories.html et vous inscrire aux alertes par e-mail à l'aide du formulaire de cette page. Des conseils de sécurité supplémentaires et les derniers avis pour vCloud Director seront publiés sur cette page.

Portée des recommandations

Les recommandations fournies dans ce guide ne concernent que la gestion des problèmes de sécurité spécifiques à vCloud Director. En tant qu'application Web hébergée sur une plate-forme Linux, vCloud Director est sensible aux vulnérabilités en matière de sécurité de ces deux catégories, lesquelles sont toutes documentées par ailleurs.

Il est également important de savoir que le déploiement sécurisé d'un logiciel ne constitue qu'une partie du processus de sécurité global ; celui-ci comprend la sécurité physique, la formation, les procédures opérationnelles, la stratégie en matière de correctifs, les plans d'escalade et réponse, la récupération d'urgence et bien d'autres domaines. La plupart de ces domaines connexes ne sont pas abordés dans ce guide.

Menaces

2

Les menaces de sécurité contre vCloud Director peuvent être classées comme menaces internes provenant de l'intérieur du système et de ses locataires ou comme menaces externes provenant de l'extérieur du système. Cette dernière catégorie inclut les menaces contre l'infrastructure créée pour héberger un groupe de serveurs vCloud Director et les menaces contre le logiciel vCloud Director installé.

Menaces internes et à l'architecture mutualisée

vCloud Director est conçu pour fournir aux locataires l'accès géré aux ressources réseau, de calcul et de stockage de VMware vSphere ® . Les utilisateurs du locataire peuvent se connecter à vCloud Director et disposent généralement de droits pour déployer et/ou utiliser des machines virtuelles, utiliser l'espace de stockage, exécuter des applications et (dans une certaine mesure) partager des ressources avec d'autres utilisateurs.

L'une des fonctionnalités clés de vCloud Director bloque la visibilité et l'accès directs à la plupart des ressources de niveau système, y compris les informations sur l'hôte physique telles que les adresses IP, les adresses Mac, le type de CPU, l'accès à ESXi, les emplacements de stockage physique, etc., pour les utilisateurs non administratifs. Toutefois, les utilisateurs peuvent toujours tenter d'accéder aux informations sur l'infrastructure du système dans laquelle leurs applications cloud sont exécutées. S'ils y parviennent, ils sont susceptibles de lancer des attaques contre les niveaux inférieurs du système.

Même au niveau des ressources virtualisées, les utilisateurs peuvent tenter d'utiliser leur accès légitime pour obtenir un accès non autorisé à certaines parties du système qui leur sont restreintes, telles que des ressources appartenant à une autre organisation. Ils peuvent notamment tenter une escalade de privilèges pour obtenir l'accès aux actions réservées aux administrateurs. Les utilisateurs peuvent également tenter des actions qui, de manière intentionnelle ou non, perturbent les performances et la disponibilité globales du système, provoquant dans des cas extrêmes un « déni de service » pour d'autres utilisateurs.

De plus, il existe généralement un nombre élevé d'utilisateurs administratifs. Ceux-ci incluent l'administrateur système d'un site vCloud Director, les administrateurs de l'organisation de locataires, les administrateurs de bases de données et de réseaux et les utilisateurs disposant de droits d'accès à ESXi, à vCenteret aux systèmes d'exploitation invités qui exécutent des outils de gestion. Ces utilisateurs disposent de privilèges plus élevés par rapport aux utilisateurs ordinaires et, généralement, d'une connexion directe aux systèmes internes. Néanmoins, leurs privilèges ne sont pas illimités. Eux aussi risquent potentiellement de tenter une escalade de privilèges ou de réaliser des opérations nuisibles.

Comme expliqué par la suite, la sécurité de vCloud Director contre ces menaces provient de l'architecture, la conception et l'implémentation de vCloud Director, vSphere et VMware NSX®, ainsi que d'autres systèmes de sécurité, et l'infrastructure dans laquelle ces systèmes sont déployés. En raison de la flexibilité et de la nature dynamique de ces systèmes, il est essentiel de suivre les directives de configuration de la sécurité applicables à tous ces composants.

Sécurisation de l'hébergement et menaces externes

Les sources de menaces externes sont des systèmes et des utilisateurs hors du cloud, y compris Internet, qui attaquent vCloud Director via ses interfaces API et Web (console Web vCloud Director et portail de locataires vCloud Director), ainsi que le service de transfert vApp et la console distante de machine virtuelle. Un utilisateur distant sans droit d'accès au système peut tenter d'accéder en tant qu'utilisateur autorisé. Les utilisateurs authentifiés de ces interfaces peuvent également être considérés comme des sources de menaces externes, car ils peuvent tenter d'exploiter les vulnérabilités du système non disponible pour des utilisateurs non authentifiés.

En règle générale, ces utilisateurs tentent d'exploiter des failles dans l'implémentation du système ou son déploiement pour obtenir plus d'informations, acquérir l'accès aux services, ou simplement perturber le fonctionnement du cloud en provoquant une perte de disponibilité du système ou en affectant l'intégrité des informations et du système. Comme l'indique la description de ces attaques, certaines d'entre elles enfreignent les limites des locataires et les couches d'abstraction matérielle que vCloud Director s'efforce d'appliquer. Bien que le déploiement des différentes couches du système affecte l'atténuation de ces menaces, les interfaces externes, y compris les pare-feux, routeurs, réseaux VPN, etc., représentent une préoccupation majeure.

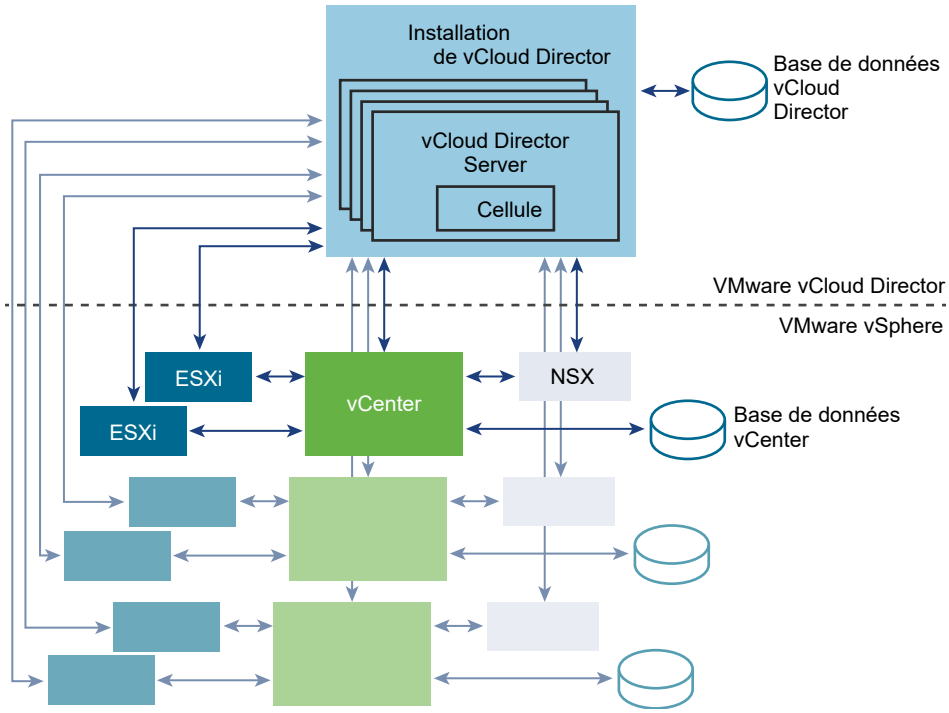
vCloud Director Architecture et options de sécurité

3

vCloud Director fournit l'infrastructure VMware vSphere ® et VMware NSX® en tant que service, pour l'isolation des locataires nécessaire dans un environnement de cloud.

Un groupe de serveurs vCloud Director se compose d'un ou plusieurs serveurs Linux. Chaque serveur du groupe exécute un ensemble de services appelé cellule vCloud Director. Toutes les cellules partagent une même base de données vCloud Director et sont reliées à plusieurs systèmes vCenter Server, aux hôtes ESXi qu'elles gèrent et aux gestionnaires NSX fournissant les services de mise en réseau.

Figure 3-1. Diagramme de l'architecture de vCloud Director



La figure Figure 3-1. Diagramme de l'architecture de vCloud Director illustre un groupe de serveurs vCloud Director unique (installation). Au sein du groupe de serveurs, il peut y avoir plusieurs hôtes de serveur vCloud Director, chacun comportant une seule cellule en cours d'exécution. Globalement, le groupe de serveurs partage la base de données vCloud Director et un partage de fichiers NFS (non illustré). L'abstraction du cloud est créée à l'aide du logiciel vCloud Director et des fonctionnalités

disponibles dans vCenter et NSX, représentées sur le schéma sous la forme d'une connexion au groupe de serveurs. Les organisations vCloud Director et leurs utilisateurs n'interagissent pas directement avec vCenter et NSX pour créer et gérer leurs charges de travail. Pour toute personne étrangère à l'administration système, toutes les interactions avec vCenter et NSX sont présentées sous la forme d'opérations vCloud Director sur des objets vCloud Director. L'autorisation d'accès aux objets vCloud Director et de manipulation repose sur les rôles. Les rôles prédéfinis fournissent un accès de ligne de base aux tâches courantes. Les administrateurs d'organisations peuvent également créer des rôles personnalisés qui bénéficient d'un groupe de droits précis.

Les sous-sections suivantes décrivent la sécurité au niveau de la couche informatique virtuelle, l'abstraction du cloud et la couche de mise en réseau virtuelle.

Ce chapitre contient les rubriques suivantes :

Isolation et sécurité des machines virtuelles

Lorsque nous abordons la sécurité et l'isolation du réseau dans ce document, nous cherchons à évaluer le risque de manque de contrôles de la séparation des réseaux et de l'isolation du trafic réseau et à déterminer les mesures correctives recommandées.

Lorsque nous examinons la segmentation d'un réseau, la notion de zone d'approbation nous vient à l'esprit. Les zones d'approbation constituent un contrôle de sécurité proactif qui surveille l'accès au trafic réseau. Une zone d'approbation est plus ou moins définie comme un segment de réseau dans lequel les données circulent relativement librement, tandis que les données entrantes et sortantes de la zone d'approbation sont soumises à des restrictions plus sévères. Exemples de zones d'approbation :

- Réseaux de périmètre (également appelés zones démilitarisées ou zones DMZ)
- Environnement de données de titulaires du secteur des cartes de paiement (PCI, Payment-card industry)
- Zones spécifiques du site , par exemple, segmentation en fonction des services ou des fonctions
- Zones définies par l'application , par exemple, les trois niveaux d'une application Web

Sécurité et couche de virtualisation sous-jacente

Une grande partie de la sécurité de vCloud Director, notamment la protection des locataires du cloud contre les menaces internes, provient de la conception de sécurité et de la configuration spécifique de la couche de virtualisation sous-jacente. Cela inclut la création et la configuration de vSphere, la sécurité supplémentaire des réseaux définis par logiciel vCloud Director, l'utilisation de la technologie NSX et la sécurité des hôtes ESXi mêmes.

Sécurité et abstraction de vCloud Director

vCloud Director impose une séparation stricte entre les opérations de vSphere et les besoins opérationnels quotidiens des locataires.

L'abstraction de vCloud Director permet à un fournisseur de services de déléguer la création, la gestion et l'utilisation de vApp aux organisations de locataires (ou à un service informatique de déléguer ces fonctionnalités à des équipes du secteur d'activité). Les utilisateurs et les administrateurs d'organisation de locataires n'utilisent ni ne gèrent les fonctionnalités vCenter telles que vMotion, vSAN etc. Les locataires effectuent uniquement le déploiement de leurs charges de travail (vApp) vers des pools de ressources et des profils de stockage, et les connectent à des réseaux VDC d'organisation appartenant à leur organisation. Les utilisateurs et les administrateurs d'organisation ne se connectant jamais à vCenter, il n'existe aucun risque de configuration incorrecte d'une autorisation vCenter qui accorderait des droits excessifs à l'utilisateur. De plus, le fournisseur est libre de changer la composition des pools de ressources et des profils de stockage sans que l'organisation ne doive apporter aucune modification.

Plus important encore, cette abstraction sépare différentes organisations les unes des autres. Même si des réseaux, banques de données ou pools de ressources communs leurs sont affectés, elles ne peuvent pas modifier ni afficher les vApp des autres. (Les vApp connectés au même réseau externe constituent une exception, car ils partagent le même vSwitch.) Bien que cela ne soit pas obligatoire, fournir à chaque organisation de locataires leurs propres banques de données dédiées, réseaux et pools de ressources permet au fournisseur de services d'appliquer une séparation d'autant plus grande entre les organisations.

Limitation de l'accès des locataires aux informations système

Bien que vCloud Director soit conçu pour masquer les opérations de niveau système pour les locataires, certaines fonctionnalités du système peuvent être configurées pour fournir des informations qui peuvent faire l'objet d'une utilisation abusive par un locataire malveillant.

Désactivez l'envoi des données de performances de l'hôte aux invités.	vSphere comprend des compteurs de performance de machine virtuelle sur des systèmes d'exploitation Windows sur lesquels VMware Tools est installé. Par défaut, vSphere n'expose pas les informations relatives à l'hôte à la machine virtuelle invitée. Les informations sur l'hôte physique pouvant faire l'objet d'une utilisation abusive par un locataire malveillant, vous devez vérifier que ce comportement par défaut est appliqué. Pour plus d'informations, reportez-vous à la section Vérification de la désactivation de l'envoi des données de performances de l'hôte aux invités du document *Sécurité de vSphere*.
Limitation de la collecte des mesures de machine virtuelle	vCloud Director peut collecter des mesures qui fournissent des informations actuelles et historiques sur les performances et la consommation de ressources de la machine virtuelle. Certaines mesures incluent des informations sur l'hôte physique, qui peuvent faire l'objet d'un usage abusif par un locataire malveillant ; vous devez donc envisager de

configurer le sous-système de collecte des mesures pour collecter uniquement celles qui ne sont pas la cible d'une utilisation malveillante. Reportez-vous à la section Configuration de la collecte des mesures dans le *Guide de l'administrateur de vCloud Director* pour plus de détails.

Utilisation prudente des extensions

vCloud Director prend en charge plusieurs méthodes d'extensibilité. Tandis que ces méthodes sont conçues pour empêcher les extensions d'acquérir des droits non accordés aux utilisateurs locataires ou d'escalader les privilèges qui leur ont été affectés lors de l'installation, une extension peut créer, de manière intentionnelle ou non, des surfaces d'attaque supplémentaires qu'une personne disposant de connaissances sur l'extension pourrait exploiter. Les fournisseurs de services et les administrateurs de locataires doivent faire preuve d'une grande prudence lors de la fourniture, révision ou installation des extensions. De plus, une gestion soignée des extensions autorisées et l'utilisation de protections appropriées, telles que l'en-tête `X-Content-Type-Options: nosniff` peuvent empêcher les plug-ins de charger du contenu malveillant.

Sécurité et couche réseau virtuelle

La mise en réseau de vCloud Director utilise les fonctionnalités SDN (Software-Defined Networking) de vSphere et NSX pour fournir aux locataires un accès sécurisé aux ressources réseau partagées. Les responsabilités du fournisseur de services sont limitées à la fourniture de connexions externes et de l'infrastructure de mise en réseau requise pour rendre ces connexions utilisables par les locataires et permettre l'allocation de ressources réseau au niveau du système à des pools de réseaux pour qu'elles puissent être consommées par les locataires.

Cette brève présentation des vCloud Director vise à établir le contexte dans lequel nous pouvons débattre des exigences de mise en réseau au niveau fournisseur et au niveau locataire du point de vue de la configuration de sécurité. Ces fonctions sont décrites en détail dans la documentation de vCloud Director disponible à l'adresse http://docs.vmware.com.

Ressources réseau au niveau fournisseur

En règle générale, un fournisseur de services est responsable de la création d'une ou plusieurs connexions entre vCloud Director et un réseau externe, tel qu'Internet ou le réseau d'entreprise d'un client. Ce type de réseau constitue essentiellement une connexion de réseau IP de base. Il ne fournit aucune confidentialité si des paquets transmis via celui-ci sont interceptés au niveau physique, ni aucune fonction d'isolation de réseau VLAN ou VXLAN pour vCloud Director.

Pour activer la mise en réseau d'une organisation de locataires, le fournisseur de services doit créer un ou plusieurs pools de réseaux qui agrègent des ressources à partir des dvSwitch et des groupes de ports ESXi dans un formulaire qui peut être accessible aux organisations de locataires. Un réseau externe ne consomme aucune ressource à partir d'un pool de réseaux. Un pool de réseaux reposant sur le VLAN ou d'un VLAN fournit une isolation à l'aide des VLAN sur un vNetwork Distributed Switch. Un réseau VXLAN

vCloud Director peut également fournir une isolation en encapsulant des paquets de couche 2 dans d'autres paquets de couche 2 (MAC-in-MAC) dans le noyau ESXi, qui peut ainsi diriger les paquets, lors de l'annulation de leur encapsulation, vers les machines virtuelles invitées appropriées, connectées aux réseaux créés sur ce type de pool.

Le fournisseur de services est également responsable de la création et de la gestion de l'infrastructure NSX située entre les réseaux que les locataires créent pour eux-mêmes et les ressources de niveau système telles que des commutateurs et des groupes de ports fournis par ESXi. À partir de ces ressources, les organisations de locataires peuvent créer leurs propres réseaux.

Réseaux VDC d'organisation

Un réseau VDC d'organisation permet aux machines virtuelles dans le VDC d'organisation de communiquer entre elles et d'accéder aux autres réseaux, y compris aux réseaux VDC d'organisation et aux réseaux externes, directement ou via une passerelle Edge qui peut fournir des services de pare-feu et NAT.

- Un réseau VDC d'organisation direct se connecte directement à un réseau externe. Seul un administrateur système peut créer un réseau VDC d'organisation direct.
- Un réseau VDC d'organisation acheminé se connecte à un réseau externe via une passerelle Edge. Un réseau VDC d'organisation acheminé requiert également le VDC conteneur pour inclure un pool de réseaux. Lorsqu'un administrateur système a provisionné un VDC d'organisation avec une passerelle Edge et l'a associé à un pool de réseaux, l'administrateur de l'organisation ou les administrateurs système peuvent créer des réseaux VDC d'organisation acheminés dans ce VDC.
- Un réseau VDC d'organisation isolé ne requiert aucune passerelle Edge ni réseau externe, mais requiert d'associer le VDC conteneur à un pool de réseaux. Lorsqu'un administrateur système a créé un VDC d'organisation avec un pool de réseaux, les administrateurs de l'organisation ou système peuvent créer des réseaux VDC d'organisation isolés dans ce VDC.

Tableau 3-1. Types de réseaux VDC d'organisation et spécifications associées

Connexion à un réseau VDC d'organisation	Description	Spécifications
Connexion directe à un réseau externe	Fournit une connectivité directe de couche 2 aux machines virtuelles et réseaux hors du VDC d'organisation. Les machines situées à l'extérieur de ce VDC d'organisation peuvent se connecter directement aux machines à l'intérieur du VDC d'organisation.	Le cloud doit contenir un réseau externe.
Connexion acheminée vers un réseau externe	Fournit un accès contrôlé aux machines virtuelles et aux réseaux en dehors de l'organisation VDC via une passerelle Edge. Les administrateurs système et les administrateurs d'organisation peuvent configurer des paramètres de traduction d'adresse réseau (NAT) et de pare-feu sur la passerelle pour rendre certaines machines virtuelles du VDC accessibles à partir d'un réseau externe.	Le VDC doit contenir une passerelle Edge et un pool de réseaux.
Aucune connexion à un réseau externe	Fournit un réseau privé isolé auquel les machines dans le VDC d'organisation VDC peuvent se connecter. Ce réseau ne fournit aucune connectivité entrante ni sortante aux machines situées à l'extérieur de ce VDC d'organisation.	Le VDC doit contenir un pool de réseaux.

Par défaut, seules les machines virtuelles dans le VDC d'organisation qui contient le réseau d'organisation peuvent l'utiliser. Lorsque vous créez un réseau VDC d'organisation, vous pouvez indiquer qu'il est partagé. Un réseau VDC d'organisation partagé peut être utilisé par toutes les machines virtuelles dans l'organisation.

Réseaux vApp

Chaque vApp contient un réseau vApp. Un réseau vApp est un réseau logique qui contrôle le mode de connexion entre les machines virtuelles et de celles-ci à des réseaux VDC d'organisation dans un vApp. Les utilisateurs peuvent créer et mettre à jour des réseaux vApp et les connecter à des réseaux VDC d'organisation, directement ou avec une protection NAT et par pare-feu.

Sécurité de l'infrastructure

4

La majeure partie de ce guide concerne la protection de vCloud Director lui-même, mais la sécurité système globale requiert également la sécurisation de l'infrastructure dont vCloud Director dépend, y compris vSphere, NSX, la plate-forme Linux de la cellule et la base de données vCloud Director.

L'application de correctifs de sécurité en vigueur à chacun de ces composants d'infrastructure avant l'installation est une étape clé et une surveillance continue pour conserver ces composants à un niveau de correctif actualisé est également essentielle.

Sécurisation de votre Infrastructure VMware

La sécurisation de vSphere et de NSX est une première étape essentielle pour la sécurisation de vCloud Director. Les administrateurs doivent vérifier les listes de vérification disponibles sur https://www.vmware.com/security/hardening-guides.html et consulter également les informations de sécurité plus détaillées disponibles dans les documents suivants :

Sécurité de vSphere	*Sécurité de vSphere*. https://docs.vmware.com/fr/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html
Sécurité de NSX	*Sécurisation de VMware NSX for vSphere*. https://communities.vmware.com/docs/DOC-27674et https://communities.vmware.com/docs/DOC-28142.

Sécurisation des plates-formes de votre cellule

Les cellules vCloud Director sont exécutées sur un système d'exploitation basé sur Linux en tant qu'utilisateur sans privilèges (`vcloud.vcloud`) créé pendant l'installation. La liste des systèmes d'exploitation de plate-forme de cellule pris en charge est incluse dans le *Notes de mise à jour de vCloud Director*. La sécurisation de la plate-forme de cellule, qu'elle soit physique ou virtuelle, est un élément essentiel de la sécurisation de vCloud Director.

Des procédures standard de renforcement de la sécurité doivent être appliquées à la plate-forme de la cellule, y compris la désactivation des services réseau inutiles, la suppression des modules inutiles, la limitation de l'accès racine à distance et l'application de stratégies de mots de passe forts. Essayez d'utiliser un service d'authentification centralisé tel que Kerberos. Envisagez l'installation d'outils de surveillance et de détection des intrusions.

Il est possible d'installer des applications supplémentaires et de provisionner des utilisateurs supplémentaires sur l'instance du système d'exploitation de la cellule, mais il est recommandé de ne pas le faire. L'élargissement de l'accès au système d'exploitation de la cellule peut réduire la sécurité.

Protection des fichiers sensibles après l'installation

Pendant l'installation, vCloud Director écrit des données d'installation, y compris les mots de passe, dans des fichiers du système de fichiers local de l'hôte Linux de la cellule. Ces fichiers, `global.properties` et `responses.properties`, qui se trouvent tous deux sous `$VCLOUD_HOME/etc`, contiennent des informations sensibles que vous devez réutiliser lorsque vous ajoutez des serveurs à un groupe de serveurs. Le fichier `responses.properties` contient les réponses fournies par l'administrateur lors de l'exécution du script de configuration. Ce fichier contient une version chiffrée du mot de passe de la base de données vCloud Director et les mots de passe du keystore du système. Un accès non autorisé à ce fichier pourrait donner à un attaquant l'accès à la base de données vCloud Director avec les mêmes autorisations que l'utilisateur de base de données spécifié dans le script de configuration. Le fichier `global.properties` contient également des informations d'identification chiffrées qui ne doivent être accessibles qu'à l'administrateur de la cellule.

Lors de leur création, les fichiers `responses.properties` et `global.properties` sont protégés par les contrôles d'accès sur le dossier `$VCLOUD_HOME/etc` et sur les fichiers eux-mêmes. Ne modifiez pas les autorisations sur ces fichiers ou ce dossier sous peine d'octroyer trop d'accès, ce qui réduirait la sécurité, ou de trop limiter l'accès, ce qui empêcherait le logiciel vCloud Director de fonctionner. Afin que les contrôles d'accès fonctionnent correctement, l'accès physique et logique aux serveurs vCloud Director doit être strictement limité aux personnes ayant besoin de se connecter et uniquement avec les niveaux d'accès minimum requis. Cela implique de limiter l'utilisation du compte racine via `sudo` et d'appliquer d'autres meilleures pratiques qui sortent du cadre de ce document. En outre, les sauvegardes des serveurs doivent être strictement protégées et chiffrées avec des clés gérées séparément des sauvegardes elles-mêmes.

Pour plus de détails, reportez-vous à la section Protection et réutilisation du fichier de réponse dans le *Guide d'installation et de mise à niveau de vCloud Director*.

Informations d'identification administratives

Assurez-vous que les informations d'identification utilisées pour un accès administratif à la cellule, à vSphere, à la base de données vCloud Director, aux pare-feux externes et aux autres périphériques suivent les normes adéquates de complexité du mot de passe. Envisagez une stratégie d'expiration et de rotation des mots de passe chaque fois que possible. Sachez, toutefois, que sur une base de données expirée ou modifiée, le mot de passe vSphereou NSX rend tout ou partie de l'infrastructure cloud non fonctionnelle jusqu'à ce que vCloud Director soit mis à jour avec les nouveaux mots de passe.

Il est important, pour assurer une « défense en profondeur », de faire varier les mots de passe d'administration pour les différents serveurs de l'environnementvCloud Director, y compris les cellules vCloud Director, la base de données vCloud Director, les serveurs vSphere et le gestionnaire NSX. Cela permet d'éviter que si un ensemble d'informations d'identification est compromis (par exemple, du fait d'un employé mécontent quittant l'entreprise), les autres systèmes du reste de l'infrastructure ne soient automatiquement compromis.

Pour plus d'informations sur la gestion des comptes et des informations d'identification des administrateurs et des locataires, reportez-vous à la sectionGestion des comptes utilisateur

Ce chapitre contient les rubriques suivantes :

Sécurité de la base de données

De manière générale, la sécurité de la base de données dépasse la portée de ce document. Comme pour tous les autres systèmes utilisés dans votre déploiement cloud, vous devez sécuriser correctement la base de données vCloud Director en appliquant les meilleures pratiques du secteur.

Le compte d'utilisateur de base de données vCloud Director doit avoir uniquement les privilèges système répertoriés dans les directives de configuration de la base de données appropriées spécifiées dans *Guide d'installation et de mise à niveau de vCloud Director*. L'utilisateur de la base de données vCloud Director ne doit pas se voir accorder de privilèges sur les autres bases de données de ce serveur ou d'autres privilèges d'administration système. Cela violerait le principe du moindre privilège sur le serveur de base de données et donnerait à l'utilisateur plus de droits que nécessaire.

Nous vous recommandons de consulter les documents suivants pour des informations sur la sécurité des bases de données.

Microsoft SQL Server

Bonnes pratiques de sécurité de SQL Server sur http://download.microsoft.com/download/8/f/a/8fabacd7-803e-40fc-adf8-355e7d218f4c/sql_server_2012_security_best_practice_whitepaper_apr2012.docx.

Note vCloud Director ne prend pas en charge les connexions SSL à une base de données Microsoft SQL Server.

Oracle

Oracle Database Security Guide (Guide de sécurité des bases de données Oracle) à l'adresse https://docs.oracle.com/cd/B28359_01/network.111/b28531.pdf.

Note vCloud Director 9.5 ne prend pas en charge les bases de données Oracle.

vCloud Director 9.1 prend en charge les bases de données Oracle, mais pas les connexions HTTPS et SSL à une base de données Oracle.

PostgreSQL

En plus de l'activation de SSL pour les connexions PostgreSQL, nous vous recommandons de consulter les documents Administration du serveur PostgreSQL et Sécurité totale dans une base de données PostgreSQL sur IBM developerWorks.

Sécurité du système

5

Le fournisseur de services et les administrateurs système sont responsables de la sécurité de chaque groupe de serveurs vCloud Director.

La sécurisation d'un groupe de serveurs vCloud Director contre des attaques externes requiert l'application de types de mesures de défense communes à tous les services Web, y compris la sécurisation des points de terminaison HTTPS à l'aide de certificats signés et le placement d'un pare-feu d'applications Web entre le système et le réseau Internet. De plus, vous devez vous assurer de configurer les services dont vCloud Director dépend, y compris le broker AMQP RabbitMQ et une base de données Apache Cassandra facultative, de manière à réduire les risques d'endommagement de ces systèmes par des acteurs externes.

Ce chapitre contient les rubriques suivantes :

Configuration requise pour la sécurité réseau

Pour fonctionner de façon sécurisée, vCloud Director nécessite un environnement réseau sécurisé. Configurez et testez cet environnement réseau avant de commencer l'installation de vCloud Director.

Connectez tous les serveurs vCloud Director à un réseau sécurisé et surveillé. Les connexions réseau de vCloud Director requièrent les conditions supplémentaires suivantes :

- Ne connectez pas vCloud Director directement à l'Internet public. Protégez toujours les connexions réseau de vCloud Director avec un pare-feu. Seul le port 443 (HTTPS) doit être ouvert pour les connexions entrantes. Les ports 22 (SSH) et 80 (HTTP) peuvent également être ouverts pour les connexions entrantes si besoin. En outre, l'`cell-management-tool` requiert un accès à l'adresse de boucle de la cellule. Tout autre trafic entrant provenant d'un réseau public, y compris les demandes JMX (port 8999), doit être rejeté par le pare-feu.

Tableau 5-1. Ports qui doivent autoriser les paquets entrants provenant des hôtes vCloud Director

Port	Protocole	Commentaires
111	TCP, UDP	Mappeur de port NFS utilisé par le service de transfert
920	TCP, UDP	rpc.statd NFS utilisé par le service de transfert
61611	TCP	AMQP
61616	TCP	AMQP

- Ne connectez pas les ports utilisés pour les connexions sortantes au réseau public.

Tableau 5-2. Ports qui doivent autoriser les paquets sortants provenant des hôtes vCloud Director

Port	Protocole	Commentaires
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	Mappeur de port NFS utilisé par le service de transfert
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	Connexions vCenter, NSX Manager et ESXi utilisant le port standard. Si vous avez choisi un port différent pour ces services, désactivez la connexion au port 443 et activez la connexion vers ce port.
514	UDP	Facultatif. Active l'utilisation de syslog.
902	TCP	Connexions vCenter et ESXi.
903	TCP	Connexions vCenter et ESXi.
920	TCP, UDP	NFS rpc.statd utilisé par le service de transfert.
1433	TCP	Port de base de données Microsoft SQL Server par défaut.
5672	TCP, UDP	Facultatif. Messages AMQP des extensions de tâche.

Tableau 5-2. Ports qui doivent autoriser les paquets sortants provenant des hôtes vCloud Director (suite)

Port	Protocole	Commentaires
61611	TCP	AMQP
61616	TCP	AMQP

- Acheminez le trafic entre les serveurs vCloud Director et les serveurs suivants sur un réseau privé dédié.
  - Serveur de base de données vCloud Director
  - RabbitMQ
  - Cassandra
- Si possible, acheminez le trafic entre les serveurs vCloud Director, vSphere et NSX sur un réseau privé dédié.
- Les commutateurs virtuels et les commutateurs virtuels distribués qui prennent en charge les réseaux fournisseurs doivent être isolés les uns des autres. Ils ne peuvent pas partager le même segment de réseau physique de couche 2.
- Utilisez NFSv4 pour le stockage du service de transfert. La version NFS la plus courante, NFSv3, ne propose pas de chiffrement de transit, ce qui peut permettre, dans certaines configurations, l'espionnage en vol ou la falsification des données en cours de transfert. Les menaces inhérentes à NFSv3 sont décrites dans le livre blanc de SANS intitulé Sécurité de NFS dans des environnements approuvés et non approuvés. Des informations supplémentaires sur la configuration et sécurisation du service de transfert vCloud Director sont disponibles dans l'article 2086127 de la base de connaissances VMware.

Certificats

vCloud Director utilise le protocole HTTPS (TLS ou SSL) pour sécuriser tout le trafic réseau sur tous les points de terminaison externes. Le protocole HTTPS est également pris en charge pour de nombreux points de terminaison internes, y compris AMQP et LDAP. Il joue un rôle particulièrement important dans la fourniture d'un certificat signé par une autorité de certification reconnue pour les points de terminaison externes. Les points de terminaison internes sont moins vulnérables et, dans la plupart des cas, ils peuvent être suffisamment sécurisés avec des certificats d'entreprise, voire des certificats auto-signés.

Tous les certificats doivent avoir un champ de nom commun correspondant au nom de domaine complet du serveur sur lequel ils sont installés. En général, cela signifie que le serveur est enregistré dans le DNS (il possède donc un nom de domaine complet bien défini et unique) et que vous vous y connectez à l'aide d'un nom de domaine complet et non d'une adresse IP. Si vous ne prévoyez pas de vous y connecter à l'aide de l'adresse IP, le certificat doit inclure le champ `subjectAltName` qui correspond à l'adresse IP de l'hôte.

Des informations supplémentaires sont disponibles dans la RFC 6125 et la RFC 5280. Vous devez également consulter votre autorité de certification.

Certificats destinés à des points de terminaison publics

Les points de terminaison exposés à un réseau d'entreprise ou à un autre réseau public, comme Internet, doivent être protégés par un certificat signé par une autorité de certification racine bien connue. Ces points de terminaison incluent :

- L'adresse HTTPS de la cellule et l'adresse proxy de la console. Vous devez configurer les deux adresses et fournir les détails relatifs à leur certificat et à leur keystore en cours d'installation.
- Des équilibrages de charge à terminaison SSL. Reportez-vous à Équilibrage de charge et terminaison de SSL.

En général, les certificats auto-signés ne doivent pas être importés, n'importe quel client SSL pouvant vérifier la chaîne d'approbation jusqu'à la racine. Les certificats de niveau inférieur (certificats d'autorité de certification d'entreprise ou certificats auto-signés) ne peuvent pas être vérifiés de cette manière. Ils ont été créés par votre équipe de sécurité locale qui peut vous indiquer l'emplacement à partir duquel les importer.

Certificats destinés aux points de terminaison privés (internes)

Les points de terminaison se trouvant sur des réseaux privés, ceux qui sont inaccessibles à partir des réseaux publics et qui ont généralement été créés spécifiquement pour être utilisés par les composants vCloud Director, comme la base de données et AMQP, peuvent utiliser des certificats signés par une autorité de certification d'entreprise, voire utiliser des certificats auto-signés, si nécessaire. Ces points de terminaison incluent :

- Les connexions internes à vSphere et à NSX.
- Les points de terminaison AMQP assurant la connexion de vCloud Director et de RabbitMQ.
- Les connexions de base de données PostgreSQL (facultatives).

Disposer d'un certificat signé réduit le risque qu'une application malveillante parvenant à accéder à un réseau privé puisse se faire passer pour un composant vCloud Director légitime.

Protocoles et suites de chiffrement pris en charge

vCloud Director prend en charge plusieurs protocoles HTTPS, y compris TLS et SSL. TLS v1.0 n'est pas, par défaut, pris en charge, car il présente des vulnérabilités connues. Après l'installation, vous pouvez utiliser l'outil de gestion de cellules pour configurer l'ensemble de protocoles et de suites de chiffrement que le système prend en charge pour les connexions HTTPS. Reportez-vous aux *Notes de mise à jour de vCloud Director* pour plus d'informations.

Configuration de certificats vSphere

Dans vSphere 6.0 et versions ultérieures, l'autorité de certification VMware (VMCA) fournit à chaque hôte ESXi et à chaque service vCenter Server avec un certificat signé par VMCA par défaut. Vous pouvez remplacer les certificats existants par de nouveaux certificats signés par l'autorité de certification VMware, définir l'autorité de certification VMware comme autorité de certification secondaire ou remplacer tous les certificats par des certificats personnalisés. Reportez-vous à la section Certificats de sécurité vSphere du guide de *Sécurité vSphere* pour plus d'informations sur la création et le remplacement des certificats utilisés par vCenter et ESXi.

Configuration de vCloud Director pour vérifier les certificats vCenter

Pour configurer vCloud Director pour vérifier les certificats vCenter, créez un keystore Java au format JCEKS contenant les certificats approuvés utilisés pour signer les certificats vCenter. (Les certificats destinés aux serveurs vCenter individuels ne se trouvent pas dans ce magasin, uniquement les certificats de l'autorité de certification utilisés pour les signer.)

Une commande semblable à celle-ci importe un certificat à encodage PEM à partir de `/tmp/cacert.pem` dans un keystore nommé `myca.ks` :

```
$ keytool –import –alias default –keystore myca.ks –file /tmp/cacert.pem –storepass password –
storetype JCEKS
```

Une commande semblable à celle-ci ajoute un autre certificat (`/tmp/cacert2.pem` dans cet exemple) dans le même keystore :

```
$ keytool –importcert–keystore myca.ks –storepass password –file /tmp/cacert2.pem –storetype JCEKS
```

Une fois que vous avez créé le keystore, connectez-vous à vCloud Director en tant qu'administrateur système. Dans la section **Paramètres système** de l'onglet **Administration**, cliquez sur **Général**, puis accédez au bas de la page.

Sélectionnez **Vérifier les certificats vCenter et vSphere SSO** et **Vérifier les certificats NSX Manager**. Cliquez sur le bouton **Parcourir** pour rechercher votre keystore Java, puis cliquez sur **Ouvrir**. Entrez le mot de passe du keystore et cliquez sur **Appliquer**.

Lorsque l'opération est terminée, vos certificats approuvés et d'autres informations sont chargés vers la base de données vCloud Director. Ainsi, il vous suffit d'effectuer cette opération une seule fois pour toutes les cellules.

Une fois cette option activée, tous les certificats vCenter et NSX Manager sont vérifiés, chaque dispositif vCenter et NSX Manager doit donc disposer d'une chaîne de certificats appropriée et d'un certificat correspondant à son nom de domaine complet. Si ce n'est pas le cas, les connexions à vCenter et à NSX échoueront.

Important Si vous avez modifié des certificats après avoir ajouté des dispositifs vCenter et NSX Manager à vCloud Director, vous devez forcer la reconnexion aux serveurs.

Mise à jour des certificats et des clés pour les cellules vCloud Director

Chaque serveur vCloud Director exige deux certificats SSL, un pour le service HTTP et un pour le service de proxy de la console, dans un fichier keystore Java. Vous devez fournir le chemin d'accès à ces keystores lorsque vous installez vCloud Director. Les certificats signés offrent le niveau de confiance le plus élevé.

La commande `certificates` de l'outil de gestion des cellules automatise le processus de remplacement des certificats existants par de nouveaux. Utilisez la commande `certificates` pour remplacer les certificats auto-signés par des certificats signés ou pour remplacer les certificats arrivant à expiration par de nouveaux certificats. Pour créer un keystore JCEKS contenant des certificats signés, reportez-vous à la section Création et importation d'un certificat SSL signé du *Guide d'installation et de mise à niveau de vCloud Director*.

Pour remplacer les certificats SSL pour un point de terminaison ou pour les deux, utilisez une commande au format suivant :

```
cell-management-tool certificates options
```

Pour plus d'informations, reportez-vous à la section Remplacement des certificats pour les points de terminaison HTTP et de proxy de console du *Guide de l'administrateur de vCloud Director*.

Pare-feux

Les cellules vCloud Director doivent être accessibles aux locataires et aux administrateurs système, qui se connectent généralement de l'extérieur du périmètre réseau du fournisseur de services. L'approche recommandée pour rendre les services vCloud Director disponibles à l'extérieur consiste à placer un pare-feu d'applications Web entre Internet (ou un autre réseau d'entreprise) et chaque point de terminaison vCloud Director public.

Les pare-feux de réseau segmentent les réseaux physiques et/ou virtuels de telle sorte que seul un ensemble limité et bien défini de trafic, sur des ports et avec des protocoles spécifiques, transite entre eux. Ce document ne définit pas les bases du déploiement de pare-feu en général et ne couvre pas les détails de la configuration d'un pare-feu. Ces sujets sortent du cadre de ce guide. En revanche, ce guide identifie les emplacements où il est conseillé de placer les pare-feux réseau par rapport aux différents composants d'un déploiement vCloud Director.

Note Les connexions de gestion peuvent être davantage limitées par des restrictions sur les adresses IP dans le réseau ou selon les VPN de locataires. Ce niveau de protection peut être approprié dans certains déploiements, mais sort du cadre de ce document.

Comme les cellules vCloud Director se trouvent dans la zone DMZ, leur accès aux services dont elles ont besoin doit également être régulé par un pare-feu de réseau. En particulier, il est recommandé que l'accès à la base de données vCloud Director, à vCenter Server, aux hôtes ESXi, à AMQP et aux services de sauvegarde ou similaires soit limité à un réseau interne inaccessible depuis le côté public du pare-feu. Reportez-vous à la section Configuration requise pour la sécurité réseau pour obtenir une liste des ports qui doivent être ouverts sur ce pare-feu.

Bloquer le trafic malveillant

Il est recommandé d'appliquer un certain nombre de règles de pare-feu pour protéger le système contre les menaces réseau :

- Suppression des paquets qui semblent provenir d'adresses non routables (usurpation d'adresse IP)
- Suppression des paquets TCP mal formés
- Limitation du taux de demandes, en particulier de demandes SYN, pour assurer la protection contre les attaques par submersion SYN (tentative de déni de service)
- Envisagez de refuser le trafic sortant du pare-feu qui ne provient pas d'une demande entrante.

Ces règles, ainsi que d'autres, sont généralement appliquées par les pare-feu d'applications Web et peuvent être appliquées par défaut par le pare-feu de réseau que vous choisissez de déployer. Consultez la documentation de votre pare-feu pour obtenir des instructions de configuration spécifiques et connaître ses capacités par défaut.

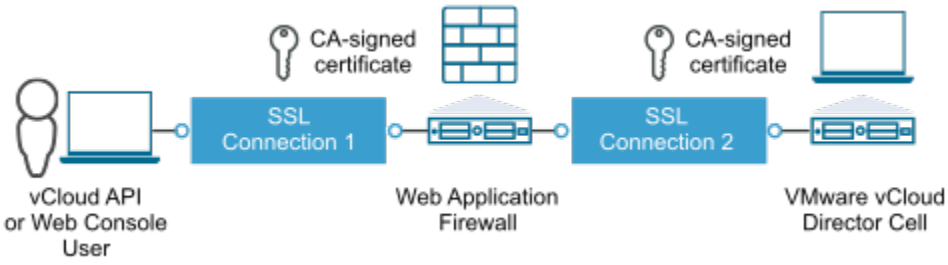
Équilibrage de charge et terminaison de SSL

Vous devez protéger les points de terminaison publics vCloud Director avec un pare-feu d'application Web (WAF). Lorsqu'il est utilisé conjointement avec un équilibrage de charge, configurez le WAF pour permettre l'inspection et le blocage du trafic malveillant en terminant la connexion HTTPS sur le WAF, ce qui permet au WAF d'effectuer l'établissement de liaison à l'aide de son propre certificat et de rediriger les demandes acceptables vers la cellule ayant un en-tête `X-Forwarded-For`.

Les demandes client adressées à vCloud Director doivent être effectuées vers un point de terminaison HTTPS. (Une connexion HTTP vers la cellule est prise en charge mais n'est pas sécurisée.) Même lorsque les communications entre le client distant et le WAF sont sécurisées avec le protocole HTTPS, il est nécessaire que les communications entre le WAF et la cellule soient également effectuées sur HTTPS.

Le diagramme simple suivant, qui laisse de côté l'équilibrage de charge, montre les deux connexions TLS ou SSL qui existent en cas d'utilisation de la terminaison TLS ou SSL, l'une entre l'ordinateur de l'utilisateur et le WAF, et l'autre entre le pare-feu et la cellule vCloud Director.

Figure 5-1. Configuration de TLS/SSL avec WAF



Terminaison TLS/SSL et certificats

Lorsque vous configurez la terminaison TLS ou SSL, il est non seulement important d'installer un certificat signé par une autorité de certification sur le WAF afin que l'identité du serveur puisse être garantie pour les applications clientes, telles que l'API vCloud et la Console Web, mais il convient également d'utiliser un certificat signé par une autorité de certification sur les cellules, même si elles sont uniquement visibles par le WAF. Les certificats auto-signés, même si le WAF les accepte, conviennent uniquement si chaque certificat est accepté manuellement au moment du déploiement ; cependant, cela limite la flexibilité du groupe de serveurs vCloud Director, du fait que chaque cellule doit être configurée manuellement (et reconfigurée au moment lors du renouvellement des certificats).

Enfin, si l'équilibrage de charge est indépendant du WAF, il doit également utiliser un certificat signé par une autorité de certification. Les procédures pour ajouter des chemins de chaînes de certificats pour les points de terminaison de l'équilibrage de charge sont documentées dans la section Personnaliser les points de terminaison publics dans le *Guide de l'administrateur de vCloud Director*.

En-tête X-Forwarded-For

`X-Forwarded-For` est un en-tête largement utilisé, pris en charge par de nombreux serveurs proxy et pare-feux. Il est recommandé d'activer la génération de cet en-tête au niveau du pare-feu si possible.

Lorsqu'un pare-feu est présent devant la cellule, celle-ci peut demander l'adresse IP du client afin de la consigner ; mais elle obtiendra généralement plutôt l'adresse du pare-feu. Cependant, si l'en-tête `X-Forwarded-For` est présent dans la requête que reçoit la cellule, celle-ci consigne cette adresse en tant qu'adresse du client et consigne l'adresse du pare-feu sous forme de champ `proxyAddress` séparé dans le journal.

Sécurisation d'AMQP (RabbitMQ)

AMQP (Advanced Message Queuing Protocol) est une norme ouverte de file d'attente de messages qui prend en charge une messagerie flexible pour les systèmes d'entreprise. vCloud Director utilise le courtier AMQP RabbitMQ pour fournir le bus de messages utilisé par les services d'extension, les extensions d'objet et les notifications de tâches bloquantes.

Les messages publiés sur RabbitMQ contiennent des informations sensibles. Exposer le trafic AMQP entre les cellules vCloud Director peut mettre en péril la sécurité du système et de ses locataires. Les points de terminaison AMQP doivent être configurés pour utiliser SSL. Les ports AMQP doivent être bloqués au niveau du pare-feu du système. Les clients tiers qui consomment les messages AMQP doivent être autorisés à fonctionner dans la zone DMZ. Tout code qui consomme des messages vCloud Director doit faire l'objet d'un audit de l'équipe de sécurité du fournisseur de services.

Pour plus d'informations sur RabbitMQ et son fonctionnement avec vCloud Director, reportez-vous à l'entrée de blog vCat-SP à l'adresse https://blogs.vmware.com/vcat/2015/08/vcloud-director-for-service-providers-vcd-sp-and-rabbitmq-security.html

Protéger le Service AMQP avec SSL

Pour utiliser SSL avec le service AMQP vCloud Director, sélectionnez **Utiliser SSL** dans la section **Paramètres du courtier AMQP** de la page **Extensibilité** de la console Web vCloud Director et fournissez l'un des éléments suivants :

- un chemin d'accès vers un certificat SSL
- un chemin d'accès vers un magasin d'approbations JCEKS, un nom d'utilisateur et un mot de passe

Reportez-vous à Configurer un courtier AMQP dans le *Guide de l'administrateur de vCloud Director* pour connaître la procédure complète.

Important Bien qu'une option **Accepter tous les certificats** soit disponible, nous vous recommandons de ne pas la sélectionner si la sécurité est une préoccupation. Accepter tous les certificats sans les vérifier ouvre la voie aux attaques de type « intermédiaire » (man in the middle).

Bloquer les Ports AMQP au niveau du pare-feu du système

Comme indiqué dans Configuration requise pour la sécurité réseau, plusieurs ports AMQP doivent être accessibles sur le réseau de gestion. Aucun point de terminaison AMQP ne doit être accessible à partir des réseaux publics ou d'entreprise.

Sécurisation de Cassandra (base de données de mesures de machine virtuelle)

Cassandra est une base de données open source que vous pouvez utiliser pour fournir au magasin de sauvegarde une solution haute performance évolutive pour la collecte des données chronologiques telles que des mesures de machine virtuelle. Les données envoyées et stockées dans le cluster Cassandra peuvent être sensibles et doivent être protégées.

En plus d'être placée sur un réseau de gestion dédié, votre infrastructure Cassandra doit être sécurisée avec le protocole SSL.

Activation du chiffrement client-nœud Cassandra

Reportez-vous à la page Chiffrement client-nœud de Cassandra pour plus d'informations sur l'installation des certificats SSL et l'activation du chiffrement.

Nous vous recommandons d'utiliser des certificats signés par une autorité de certification reconnue. De cette manière, aucune configuration supplémentaire n'est requise dans vCloud Director. Si vous utilisez des certificats auto-signés, vous devez les importer manuellement dans vCloud Director. Utilisez la commande `import-trusted-certificates` de l'outil de gestion des cellules comme indiqué à la section Importation de certificats SSL à partir de services externes dans le *Guide de l'administrateur de vCloud Director*

Sécurisation de l'accès à JMX

Comme indiqué dans le *Guide de l'administrateur de vCloud Director*, chaque cellule de vCloud Director présente un nombre de MBeans via l'interface JMX, pour permettre une gestion opérationnelle du serveur et fournir un accès aux statistiques internes. L'accès à l'interface JMX doit impérativement faire l'objet d'un contrôle strict, car elle peut présenter des informations sensibles sur le système exécuté et affecter son fonctionnement.

Authentification JMX

L'interface JMX est accessible uniquement par les administrateurs système de vCloud Director, qui doivent s'authentifier auprès de JMX avec les mêmes informations d'identification qui leur permettent d'accéder à vCloud Director. Cette fonctionnalité n'est pas configurable.

Limite des connexions à JMX

JMX est une interface de gestion destinée uniquement aux administrateurs système ; il n'existe donc aucune raison pour la présenter hors du réseau de gestion de vCloud Director. Si une troisième adresse IP est allouée au système exclusivement à des fins de gestion, liez JMX directement à cette adresse IP. Par défaut, le connecteur JMX de vCloud Director est lié à l'adresse IP principale spécifiée lors de la configuration du système. Pour remplacer cette valeur par défaut, insérez la propriété suivante sous `/opt/vmware/vcloud-service-director/etc/global.properties` :

```
vcloud.cell.ip.management=Adresse IP ou nom d'hôte du réseau de gestion à laquelle/auquel le
connecteur JMX doit être lié
```

La configuration la plus sécurisée lie le connecteur JMX à l'adresse de l'hôte local :

```
vcloud.cell.ip.management=127.0.0.1
```

Quels que soient les périphériques de routage et de pare-feu employés, les adresses IP allouées à ce réseau de gestion et au port JMX (par défaut = 8999) ne doivent pas être autorisées à traverser les limites du réseau des utilisateurs Internet ou de l'organisation.

Avec ce paramètre défini dans `global.properties`, JMX est accessible uniquement depuis le système vCloud Director local. Aucune connexion externe vers le port JMX ne pourra être établie, quelle que soit la configuration de routage du réseau.

Sécurisation des communications JMX

Si JMX est présenté uniquement à l'adresse de l'hôte local (`127.0.0.1`), vous pouvez sécuriser les communications JMX à l'aide du protocole SSH comme mécanisme de tunnel lors de chaque accès à JMX.

Si vos exigences de gestion n'autorisent pas l'utilisation de cette configuration et que JMX doit être présenté hors de la cellule de vCloud Director, JMX doit être sécurisé avec le protocole HTTPS, que vous pouvez configurer en définissant la variable d'environnement suivante :

```
# export VCLOUD_JAVA_OPTS="-Dcom.sun.management.jmxremote.ssl=true \
-Djavax.net.keyStore=pathTokeystore \
-Djavax.net.sll.keyStorePassword=password \
-Djavax.net.ssl.keyStoreType=storeType"
```

Vous devez ensuite redémarrer vCloud Director.

Les clients JMX doivent désormais se connecter à l'aide du protocole HTTPS, mais ils doivent avoir accès au certificat d'autorité de certification. Par exemple, pour `jconsole`, vous devez importer le certificat d'autorité de certification dans un keystore sur la machine qui exécutera `jconsole`. Puis, démarrez `jconsole` avec les arguments de ligne de commande suivantes :

```
# jconsole -J-Djavax.net.ssl.trustStoreType=store type \
-J-Djavax.net.ssl.trustStore=pathTokeystore \
-J-Djavax.net.ssl.trustStorePassword=password
```

Les certificats auto-signés (déconseillés dans un déploiement de production) rendrait ce processus complexe, car chaque certificat auto-signé doit se trouver dans un keystore sur la machine exécutant le client JMX. La prise en charge des certificats signés par une autorité de certification est plus simple ici, car seul le certificat de l'autorité de certification est requis au niveau de la machine exécutant le client JMX.

Configuration du réseau de gestion

Le réseau de gestion vCloud Director est un réseau privé utilisé par l'infrastructure cloud et qui fournit l'accès aux systèmes clients utilisés pour exécuter des fonctions d'administration dans vCloud Director.

Les systèmes qui se connectent au réseau de gestion incluent le serveur de base de données vCloud Director, un serveur NFS pour le stockage de transfert, les serveurs vCenter, un annuaire LDAPv3 facultatif pour authentifier les administrateurs du fournisseur, tous les annuaires LDAPv3 gérés par le fournisseur pour authentifier les utilisateurs de l'organisation et des NSX Managers. Les serveurs vCenter sur ce réseau doivent également accéder à leurs propres serveurs Active Directory.

Configuration requise du réseau de gestion de l'infrastructure virtuelle

Il est important de séparer le réseau de gestion des réseaux de données de machine virtuelle. Cela est d'autant plus essentiel dans un environnement cloud dans lequel le fournisseur et les locataires appartiennent à différentes organisations. Vous ne souhaitez pas rendre le réseau de gestion du fournisseur vulnérable aux attaques des réseaux vApp des organisations. De même, le réseau de gestion doit être séparé de la zone DMZ qui fournit l'accès aux administrateurs de l'organisation. Même s'ils peuvent accéder aux mêmes interfaces que les administrateurs système du fournisseur, le concept de DMZ est important pour la segmentation du trafic public du privé et pour assurer une protection avancée.

Du point de vue de la connectivité physique, le réseau de données de machine virtuelle doit être séparé du réseau de gestion. Il s'agit de la seule méthode permettant de protéger les systèmes de gestion contre les machines virtuelles malveillantes. De même, les cellules de vCloud Director existent physiquement dans la zone DMZ. Dans le diagramme de déploiement physique, les serveurs dans l'espace de gestion qui se connectent aux espaces cloud utilisent un réseau physique séparé, et des règles de pare-feu spécifiques autorisent la transmission du trafic.

Le pare-feu interne qui agit comme intermédiaire entre les connexions de vCenter et vCloud Director à vSphere (et d'autres réseaux) est requis pour l'architecture réseau. La question n'est pas de savoir si différentes machines virtuelles sur un hôte unique peuvent se connecter à la fois à un réseau de zone DMZ et à un réseau privé. Au contraire, il existe des machines virtuelles dans cet espace de gestion, les cellules de cloud, qui se connectent aux deux réseaux. Tandis que le logiciel vCloud Director a été conçu et implémenté suivant une stratégie de sécurité des produits VMware et, compte tenu des exigences de sécurité, il ne s'agit pas d'un pare-feu ; par conséquent il ne doit pas agir lui-même comme intermédiaire entre les réseaux de zone DMZ et de gestion privé. Ce rôle est assuré par le pare-feu.

Autres réseaux associés

Comme l'illustrent les diagrammes de déploiement physiques et logiques, les réseaux de stockage sont eux aussi physiquement séparés. Ce procédé est conforme aux meilleures pratiques vSphere et protège l'espace de stockage du locataire et du fournisseur contre les machines virtuelles malveillantes. Cela s'applique également au réseau de sauvegarde. Techniquement, il s'agit d'une branche désactivée du réseau de gestion. Ses exigences et configuration spécifiques varient selon le logiciel et la configuration de la sauvegarde utilisés.

vMotion n'est pas toujours placé sur un réseau distinct du réseau de gestion ; toutefois, dans le cloud, cela est important du point de vue de la séparation des fonctions. vMotion s'applique généralement en clair, et s'il est placé sur le réseau de gestion, il permet à un administrateur de fournisseur ou à un autre utilisateur ayant accès à ce réseau de « flairer » le trafic vMotion, ce qui enfreint la confidentialité des organisations. C'est pourquoi vous devez créer un réseau physique distinct pour vMotion de charges de travail cloud.

Audit et journalisation

La possibilité d'enregistrer et de contrôler les activités des utilisateurs est une partie importante de la sécurité système globale. La plupart des organisations disposent de règles déterminant les personnes

autorisées à accéder aux logiciels et aux ressources matérielles associées, et à y apporter des modifications. La tenue d'un journal d'audit des activités importantes permet à l'organisation de vérifier la conformité avec les règles, de détecter d'éventuelles violations et d'initier des mesures correctives. Certaines entreprises sont soumises à des lois et réglementations externes requérant la surveillance et la vérification ininterrompues des règles d'autorisation et d'accès.

Un journal d'audit peut également être utile pour détecter des tentatives, réussies ou non, d'accès illicite au système, de sondage de ses informations ou de perturbation de son fonctionnement. Savoir qu'une attaque a été tentée et en connaître les détails participent à la limitation des dommages et au blocage de futures attaques.

Que cela s'avère ou non nécessaire, examiner régulièrement les journaux à la recherche d'activités suspectes, inhabituelles ou non autorisées est une bonne pratique en matière de sécurité. L'analyse régulière des journaux facilite également l'identification des pannes et des erreurs de configuration système, et le respect des contrats de niveau de service.

vCloud Director inclut deux types de journaux :

Journaux de diagnostic Les journaux de diagnostics sont tenus dans le répertoire de journaux de chaque cellule. Ces journaux peuvent être utiles pour la résolution de problèmes, mais ne sont pas destinés à la conservation d'une piste d'audit des interactions système significatives. Chaque cellule vCloud Director crée plusieurs fichiers journaux de diagnostic décrits dans la section Affichage des journaux vCloud Director du *Guide de l'administrateur de vCloud Director*.

Journaux d'audit Les journaux d'audit enregistrent des actions significatives, notamment les connexions et déconnexions. Le journal d'audit système est conservé dans la base de données vCloud Director et peut être surveillé via l'interface utilisateur Web. Chaque administrateur d'organisation et l'administrateur système ont accès au journal correspondant à leur domaine de contrôle spécifique.

Nous recommandons l'utilisation de l'utilitaire `syslog` pour conserver ces journaux et d'autres journaux vCloud Director. Par ailleurs, vous devez envisager l'utilisation de vRealize Log Insight, qui prend en charge la collecte à distance d'autres journaux, tels que les journaux de demandes, qui ne reposent pas sur `log4j`.

Utilisation de Syslog avec vCloud Director

Conformément à la description donnée dans le *Guide d'installation et de mise à niveau de vCloud Director*, un serveur `syslog` peut être configuré pendant l'installation. L'exportation de journaux vers un serveur `syslog` est recommandée pour plusieurs raisons :

- Les journaux de base de données ne sont pas conservés plus de 90 jours, tandis que les journaux transmis via `syslog` peuvent être conservés aussi longtemps que nécessaire.
- Les journaux d'audit de toutes les cellules peuvent ainsi être consultés simultanément dans un emplacement central.

- Les journaux d'audit sont protégés contre le risque de perte sur le système local suite à une panne, un manque d'espace disque, une compromission, etc.
- Les opérations d'analyse de problèmes semblables à ceux répertoriés ci-dessus sont prises en charge.
- Il s'agit de la méthode utilisée par bon nombre de systèmes de gestion des journaux et de systèmes de gestion des événements et des informations de sécurité (SIEM) pour s'intégrer dans vCloud Director. Cela permet :
  - La corrélation des événements et des activités entre vCloud Director, vSphere et NSX, et même les couches matérielles physiques de la pile.
  - L'intégration d'opérations de sécurité cloud avec le reste des opérations de sécurité du fournisseur de cloud ou de l'entreprise, à travers les infrastructures de cloud, physiques et virtuelles.
- La journalisation sur un système distant autre que le système sur lequel la cellule est déployée empêche l'altération des journaux. La compromission de la cellule n'autorise pas nécessairement l'accès aux informations du journal d'audit ou leur altération.

Si vous n'avez pas configuré une destination `syslog` pour la journalisation au moment de l'installation initiale, vous pouvez la configurer ultérieurement en accédant à chaque cellule et en modifiant le fichier `$VCLOUD_HOME/etc/global.properties` avant de redémarrer la cellule.

Reportez-vous à la section Configuration requise pour la sécurité réseau pour obtenir une liste des ports qui doivent rester ouverts de l'hôte vCloud Director au serveur `syslog`. Les détails de configuration du serveur `syslog` sont propres au système et non couverts par ce document. Il est recommandé de configurer le serveur `syslog` avec la redondance, afin que les événements essentiels soient toujours consignés.

La discussion ci-dessus couvre uniquement l'envoi du journal d'audit à un serveur `syslog`. Les organisations menant des opérations de sécurité et des opérations informatiques peuvent également bénéficier du regroupement et de la gestion centralisés des journaux de diagnostics mentionnés ci-dessus. Il existe un grand nombre de méthodes de collecte de ces journaux, notamment la planification d'une tâche destinée à les copier régulièrement dans un emplacement centralisé, la définition d'un enregistreur supplémentaire dans le fichier `log4j.properties` (`$VCLOUD_HOME/etc/log4j.properties`) sur un serveur syslog central ou l'utilisation d'un utilitaire de collecte de journaux comme vRealize Log Insight pour surveiller et copier les fichiers journaux en un emplacement centralisé. La configuration de ces options dépend du système que vous préférez utiliser dans votre environnement et n'est pas couverte par ce document.

Important Nous recommandons l'utilisation d'une infrastructure `syslog` TLS. Le protocole `syslog` (UDP) par défaut ne permet ni le chiffrement en transit, ni l'obtention d'un accusé de réception/le contrôle de la transmission. L'absence de chiffrement expose les données des journaux à l'espionnage (les informations présentes dans les journaux pourraient être utilisées pour lancer d'autres attaques), et l'absence de contrôle de la transmission pourrait permettre à une personne malveillante de falsifier les données de journalisation. Pour plus d'informations, consultez la Section 4 de la RFC 5426.

Journalisation des diagnostics et substitution des journaux

Le fichier journal de demandes Jetty (`$VCLOUD_HOME/logs/`*`aaaa_mm_jj.`* `request.log`) est contrôlé par programmation par le serveur Jetty (HTTP), mais ne présente aucune limite de taille maximale. Il existe, par conséquent, un risque de croissance illimitée des fichiers journaux. Une entrée de journal est ajoutée au fichier actuel pour chaque demande HTTP servie par Jetty. C'est pourquoi nous recommandons l'utilisation de `logrotate` ou de méthodes similaires pour contrôler la taille des journaux et le nombre d'anciens fichiers journaux à conserver.

Les autres fichiers journaux de diagnostic sont limités à une taille maximale totale de 400 Mo. Assurez-vous que vous disposez d'un espace disque suffisant pour héberger ces fichiers, outre la taille de l'espace autorisé pour les journaux de demandes Jetty. Comme indiqué plus haut, la journalisation centralisée garantit l'absence de risque de perte de précieuses informations de diagnostic une fois la taille maximale totale de 400 Mo de fichiers journaux atteinte, et les fichiers substitués et supprimés.

NTP et journaux

Le *Guide d'installation et de mise à niveau de vCloud Director* identifie le protocole NTP comme une exigence fondamentale pour toutes les cellules vCloud Director. Autre avantage à l'utilisation du protocole NTP : les messages de journaux de toutes les cellules présentent des horodatages synchronisés. Bien entendu, les outils de gestion des journaux et les systèmes SIEM comportent leurs propres horodatages pour faciliter la coordination des journaux de plusieurs sources, mais ces horodatages correspondent à l'heure à laquelle ils ont été reçus par ces systèmes, pas à l'heure de consignation initiale des événements.

Autres journaux

Les autres systèmes connectés à vCloud Director et utilisés par ce dernier créent des journaux d'audit qui doivent être regroupés dans le cadre de vos processus d'audit. Parmi ces journaux, citons ceux provenant de NSX Manager, de la base de données vCloud Director, de vCenter Server et des hôtes vSphere. Les détails des fichiers journaux de chaque système et leur objectif ne sont pas couverts par ce document. vous pouvez les trouver dans la documentation relative à ces produits.

Sécurité des locataires

6

Le fournisseur de services, les administrateurs système et les administrateurs d'organisation sont responsables de la sécurité de chaque organisation de locataires de vCloud Director.

La sécurisation d'une organisation de locataires de vCloud Director contre les attaques externes consiste en grande partie à fournir une sécurité de niveau système adéquate, pour empêcher les attaquants externes d'accéder aux ressources de locataires. Le fournisseur de services doit également savoir si un locataire peut en attaquer un autre, ou simplement le gêner. Les vecteurs d'attaque interlocataire potentiels comprennent l'écoute des détails des ressources de calcul, de stockage et de réseau au niveau du système. Des interférences, intentionnelles ou non, surviennent lorsque des ressources système sont partagées entre plusieurs locataires (qui peuvent être réciproquement méfiants) et qu'un seul locataire peut consommer une quantité des ressources suffisante pour que le niveau de service attendu par les autres locataires soit refusé. Cette situation est souvent appelée problème de « voisin bruyant ».

Comme indiqué dans le Chapitre 3 vCloud Director Architecture et options de sécurité , vCloud Director est conçu pour activer le partage transparent de ressources système entre un grand nombre de locataires. En général, un fournisseur de services est libre de déployer des ressources système de manière à optimiser l'efficacité du système, tout en minimisant le risque d'interruption de service. Chaque fois que des ressources sont partagées entre des organisations de locataires, le fournisseur de services doit prévoir les potentiels effets de ce type de partage sur les différentes opérations de locataires et le risque d'attaques interlocataires.

Ce chapitre contient les rubriques suivantes :

Sécurité réseau pour les organisations de locataires

Bien que les organisations vCloud Director sont responsables de la sécurité de leur propre réseau, le fournisseur de services doit protéger les réseaux externes à l'aide d'un pare-feu.

Dans le système vCloud Director, les réseaux VXLAN et VLAN appliquent la séparation du trafic de paquets, ce qui équivaut à utiliser des réseaux physiques distincts. Ils fournissent également une gamme d'options de routage et de pare-feu qui permettent aux organisations de contrôler avec précision l'accès à leurs charges de travail à partir de systèmes externes et celles dans l'organisation. Ces fonctions sont décrites en détail dans la documentation de vCloud Director disponible à l'adresse http://docs.vmware.com. Pour l'essentiel, un fournisseur de services qui a conçu une protection efficace pour le système même (y compris un pare-feu d'applications Web, des équilibrages de charge à interruption SSL et des certificats numériques correctement signés) ne doit pas jouer un rôle actif dans l'établissement ou la gestion de la sécurité des réseaux VDC d'organisation.

Accès externe aux charges de travail de locataires

Lors de la configuration de l'accès aux charges de travail d'organisation (vApp) à partir du réseau Internet ou d'entreprise, le fournisseur de services doit tenir compte de la configuration requise du pare-feu de l'infrastructure de vSphere déployée et utilisée par vCloud Director. Il est probable que certains vApp doivent accéder à Internet ou être accessibles à distance, via RDP, SSH, etc., à des fins de gestion, ou via HTTP ou d'autres protocoles pour les utilisateurs finaux de ces services. C'est pourquoi, il est recommandé de disposer de deux réseaux de données de machine virtuelle différents (voir les diagrammes d'architecture à la section Allocation et isolation de ressources) pour différentes utilisations ; chacun réseau requiert une protection par pare-feu.

Les machines virtuelles qui doivent être accessibles hors du cloud (p. ex., à partir d'Internet) sont connectées à un réseau public ou un réseau privé avec acheminement NAT, avec le transfert de port configuré pour les services exposés. Le réseau externe auquel ces réseaux VDC d'organisation sont connectés auraient besoin d'un pare-feu de protection qui autorise le trafic convenu sur ce réseau de zone DMZ. En d'autres termes, le fournisseur de services doit s'assurer que tous les ports et protocoles ne sont pas autorisés à établir une connexion sur le réseau de zone DMZ externe. En même temps, il doit s'assurer qu'un trafic suffisant est autorisé pour permettre aux vApp des organisations de fournir les services pour lesquels ils sont conçus. Cela généralement inclut les ports 80/TCP et 443/TCP, mais des protocoles et ports supplémentaires peuvent être ajoutés. Le fournisseur de services doit déterminer la meilleure méthode pour parvenir à un équilibre, puisque, du point de vue de la sécurité, les protocoles et ports inutiles doivent être bloqués.

En général, il est recommandé de connecter les vApp qui nécessitent une accessibilité vers et depuis Internet à un réseau VDC d'organisation configuré pour autoriser uniquement les types requis de connexions entrantes et sortantes. Cela permet à l'organisation de contrôler les règles de transfert de port et de pare-feu de NSX. Ce type de configuration n'élimine pas la nécessité d'un pare-feu de réseau pour séparer le réseau externe utilisé par ces réseaux VDC d'organisation, car ces réseaux VDC d'organisation publics ne disposent d'aucune protection par pare-feu de vCloud Director. Le pare-feu distinct est nécessaire pour créer une zone DMZ (Cette fonction peut toutefois être exécutée par une instance Edge NSX distincte.).

De même, un réseau VDC d'organisation privé avec acheminement NAT est utilisé pour un réseau de données de machine virtuelle qui permet aux machines virtuelles d'accéder à Internet. Comme indiqué plus haut, une instance Edge NSX fournit les fonctionnalités NAT et de pare-feu à ce réseau interne de données de machine virtuelle. Une fois encore, la partie externe du réseau acheminé doit se trouver dans la zone DMZ pour permettre à un pare-feu de réseau distinct de séparer la zone DMZ de la connexion Internet.

Allocation et isolation de ressources

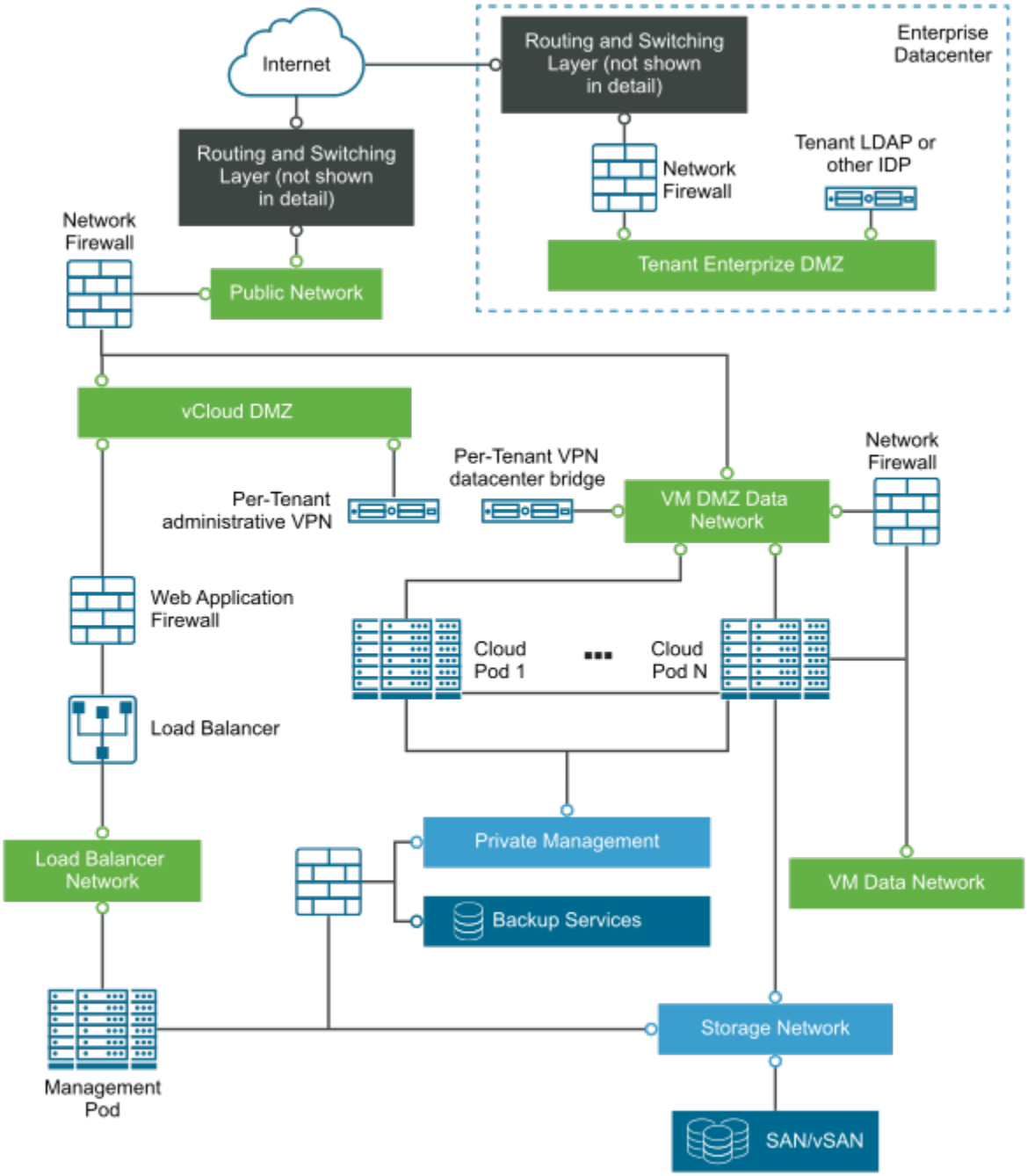
Le déploiement de fournisseurs de services standard de vCloud Director prévoit de partager les ressources vSphere entre plusieurs organisations de locataires. Cela offre aux organisations une flexibilité maximale et permet au fournisseur d'optimiser l'utilisation des ressources de calcul, de réseau et de stockage provisionnées. Des exemples de diagrammes de déploiement logiques et physiques sont présentés ci-dessous.

La suite de cette sous-section donne une vue générale des composants, tandis que les sous-sections suivantes décrivent les recommandations spécifiques concernant la configuration des pools de ressources, des banques de données, de la mise en réseau et des autres composants.

Déploiement de ressources partagées

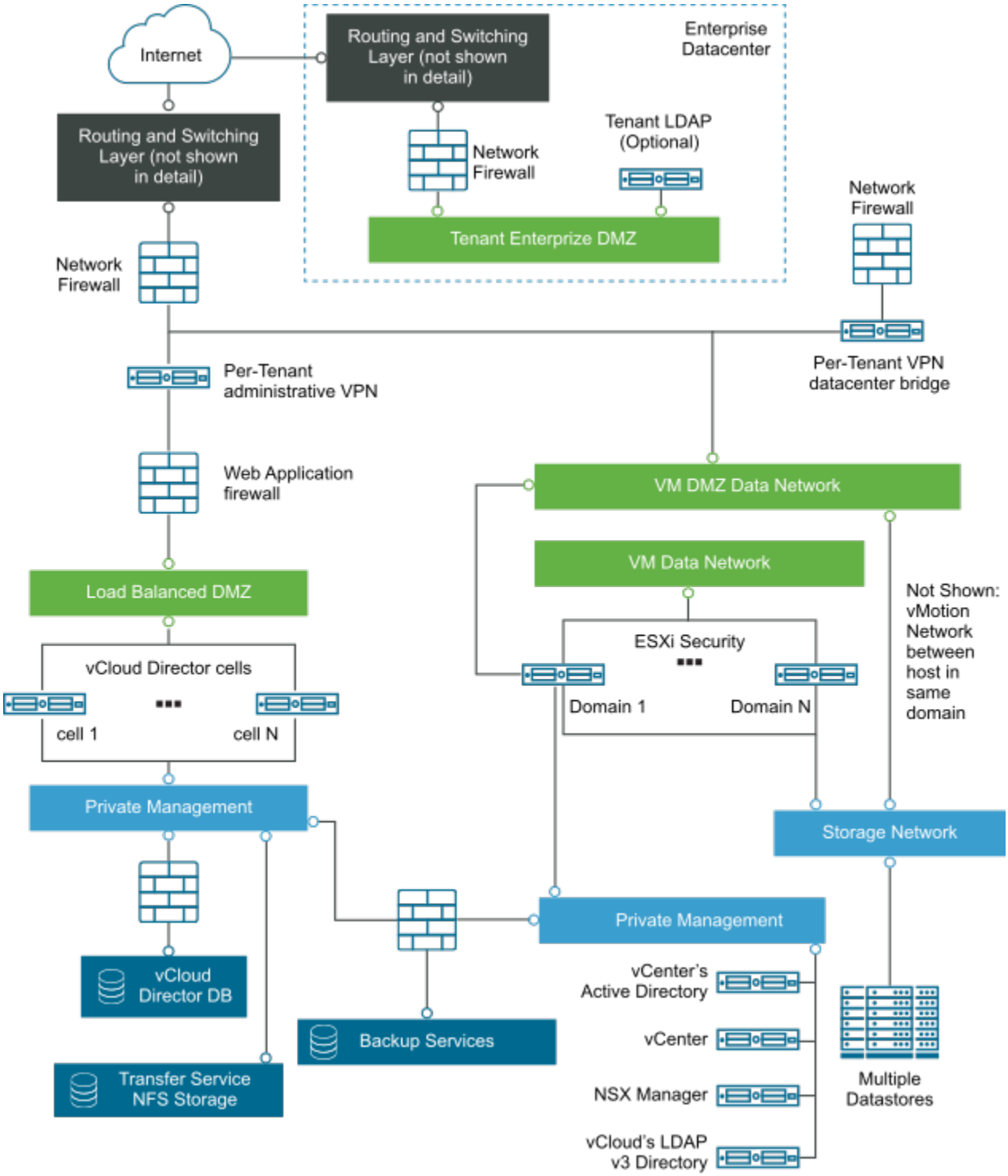
La Figure 6-1. Diagramme de déploiement physique et la Figure 6-2. Diagramme de déploiement logique sont deux vues de la même installation de vCloud Director. Dans ces figures, le terme « espace » est utilisé pour désigner un groupe de ressources (machines physiques ou virtuelles) dédié à la gestion du système (« espace de gestion ») ou aux charges de travail des locataires (« espace cloud »).

Figure 6-1. Diagramme de déploiement physique



Dans la Figure 6-2. Diagramme de déploiement logique, le côté gauche affiche les cellules vCloud Director dans une zone DMZ équilibrée en charge. La zone DMZ contient également un WAF et éventuellement un VPN administratif par locataire. Ce VPN peut être configuré par un fournisseur de services pour chaque organisation afin de limiter plus strictement les utilisateurs et les adresses IP qui peuvent accéder aux services présentés par le WAF. Un locataire peut également configurer un VPN pour connecter les charges de travail et les données sur site aux machines virtuelles dans le cloud. Ce document n'explique pas comment configurer ce type de VPN.

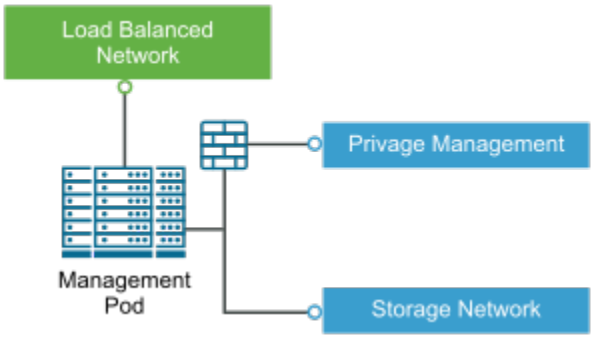
Figure 6-2. Diagramme de déploiement logique



Les éléments de gestion privé requis par vCloud Director, notamment vCenter, NSX ou encore la base de données vCloud Director, par exemple, se trouvent derrière les cellules. Leurs connexions sont strictement contrôlées par les pare-feu du diagramme, car ces services ne doivent pas être accessibles à partir d'autres machines de la zone DMZ ou directement sur Internet.

La Figure 6-3. Réseaux d'espaces de gestion représente uniquement l'espace de gestion. Elle indique qu'il est nécessaire de connecter à cet espace au moins deux, voire trois réseaux physiques distincts. Cela inclut le réseau DMZ équilibré en charge, le réseau de gestion privé et un réseau de stockage dédié en option avec une configuration spécifique au fournisseur.

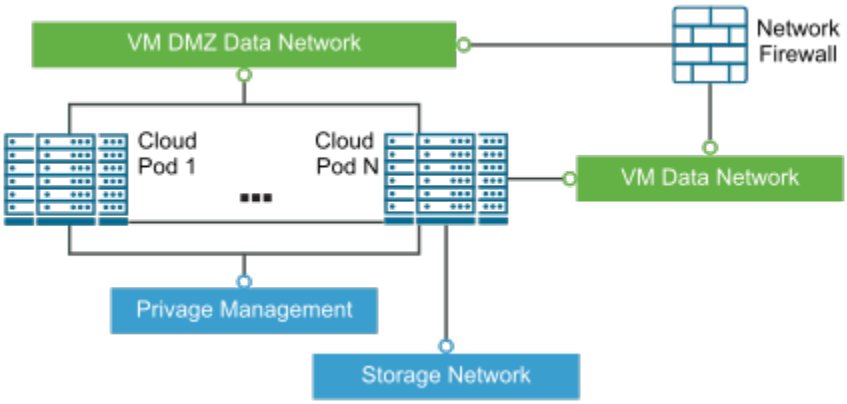
Figure 6-3. Réseaux d'espaces de gestion



Par rapport aux hôtes vSphere regroupés dans différents domaines de sécurité, ils ont chacun des réseaux externes présentés en tant que réseau de données de machine virtuelle DMZ pour une utilisation en tant que réseaux VDC d'organisation publique et réseaux de données de machine virtuelle pour les réseaux VDC d'organisations privées qui peuvent être routés vers un réseau externe.

La Figure 6-4. Réseaux d'espaces cloud représente les espaces cloud. Il affiche quatre réseaux physiques. Toutefois, le réseau de stockage est spécifique aux technologies matérielles et de stockage spéciales choisies. Si les pools de ressources ne couvrent pas les clusters, vous n'avez pas besoin de fournir un réseau de données de machine virtuelle physique. Dans le cas contraire (si les pools de ressources couvrent les clusters), ce document recommande d'utiliser un réseau physique distinct pour le trafic vMotion.

Figure 6-4. Réseaux d'espaces cloud



Il est également supposé que les technologies de sécurité de centre de données classique comme IDS/IPS, SIEM, la gestion de la configuration, la gestion des correctifs, la gestion de la vulnérabilité, les antivirus et les systèmes de gestion GRC seront appliquées à vCloud Director et vSphere, aux systèmes qui y sont associés ainsi qu'aux réseaux et aux infrastructures de stockage qui les prennent en charge. Ce document ne traite pas de ces systèmes.

Partage de ressources et recommandations d'isolation

Dans des conditions normales, un fournisseur de services peut partager des ressources de calcul, de stockage et de mise en réseau entre plusieurs organisations de locataires. Le système applique une isolation par abstraction, des pratiques d'ingénierie sécurisées dans l'hyperviseur et la pile logicielle vCloud Director.

Les organisations de locataires partagent des pools de ressources, des banques de données et des réseaux externes sous-jacents présentés via un seul VDC fournisseur sans affecter (ou détecter) les ressources qu'ils ne possèdent pas. La bonne gestion du stockage de vApp et des baux d'exécution, des quotas de vApp, des limites d'opérations gourmandes en ressources et des modèles d'allocation de VDC d'organisation permet de s'assurer qu'un locataire ne peut pas refuser d'en servir un autre par accident ou délibérément. Par exemple, une configuration très classique consisterait à configurer tous les VDC d'organisation sous le modèle d'allocation de pool de réservation sans jamais surcharger les ressources. Ce document ne traite pas de la gamme complète des options, mais certains points sont abordés dans les sous-sections suivantes.

Domaines de sécurité et VDC fournisseur

Même si l'isolation du logiciel et la configuration de l'organisation sont corrects, il se peut que les organisations de locataires ne souhaitent pas exécuter ou stocker différentes charges de travail sur des ressources spécifiques de calcul, de réseau ou de stockage. Cela n'élève pas l'ensemble du système à un niveau d'environnement hautement sécurisé (thème non abordé dans ce document), mais nécessite de segmenter le cloud en plusieurs domaines de sécurité. Voici quelques exemples spécifiques de charges de travail nécessitant ce traitement :

- Données soumises aux lois sur la confidentialité qui doivent être stockées et traitées dans les zones géographiques prescrites.
- Données et ressources appartenant à des pays ou à des organisations qui, malgré la confiance accordée à l'isolation du cloud, interdisent formellement à leurs VDC de partager des ressources avec d'autre locataires spécifiques telle qu'une société concurrente, par exemple, par mesure de prudence et de défense.

Dans ce type de scénarios, les pools de ressources, les réseaux et les banques de données doivent être segmentés en différents domaines de sécurité à l'aide de différents VDC fournisseur qui permettent de regrouper (ou d'isoler) les vApp qui ont des problèmes similaires. Par exemple, vous pouvez clairement identifier certains VDC de fournisseur comme stockant et traitant des données dans certains pays.

Pools de ressources

Dans un seul VDC de fournisseur, vous pouvez avoir plusieurs pools de ressources qui agrègent les ressources de CPU et de mémoire fournies par l'infrastructure vSphere sous-jacente. Il n'est pas nécessaire de segmenter différentes organisations sur différents pools de ressources du point de vue de la confidentialité et de l'intégrité. Mais il peut y avoir des raisons de le faire du point de vue de la disponibilité. Ce problème de gestion des ressources dépend des modèles d'allocation de VDC d'organisation, des charges de travail, des quotas et des limites attendues et appliquées à ces organisations ainsi que de la vitesse avec laquelle des ressources de calcul supplémentaires peuvent être mises en ligne par le fournisseur. Ce guide ne définit pas les différents modèles d'allocation de ressources ni leur impact sur l'utilisation d'un pool de ressources par chaque organisation, c'est-à-dire que chaque fois que vous autorisez la surcharge des ressources dans un pool utilisé par plusieurs organisations, vous risquez de provoquer des problèmes de qualité de service dans une ou plusieurs organisations. Il est donc impératif de bien surveiller les niveaux de service pour éviter le déni de service d'une organisation, mais il n'est pas nécessaire de séparer les organisations pour des raisons de sécurité afin d'atteindre cet objectif.

Limitation de la consommation partagée des ressources partagées

Dans la configuration par défaut, de nombreuses ressources de calcul et de stockage vCloud Director peuvent être consommées en quantité illimitée par tous les locataires. Le système permet à un administrateur système de gérer et de surveiller la consommation de ces ressources de plusieurs manières. Il est essentiel d'examiner attentivement les zones suivantes pour éviter qu'un « voisin bruyant » affecte le niveau de service de vCloud Director.

Limiter les opérations gourmandes en ressources	Reportez-vous à la section Configurer les limites du système dans le *Guide de l'administrateur de vCloud Director*.
Imposer des quotas sensibles	Reportez-vous aux sections Configurer les paramètres de bail, de quota et de limite de l'organisation et Configurer les limites du système dans le *Guide de l'administrateur de vCloud Director* pour limiter le nombre de VDC qu'un locataire peut créer et le nombre de connexions simultanées par machine virtuelle.
Gérer les baux de stockage et d'exécution	Les baux fournissent un niveau de contrôle sur la consommation des ressources de stockage et de calcul des locataires. Lors de la gestion des ressources partagées, il est essentiel de limiter la durée pendant laquelle un vApp peut rester sous tension ou un vApp hors tension peut consommer du stockage. Reportez-vous à la section Comprendre les baux dans le *Guide de l'administrateur de vCloud Director*.

Réseaux externes

Un fournisseur de services crée des réseaux externes et les rend accessibles aux locataires. Un réseau externe peut être partagé en toute sécurité entre plusieurs réseaux publics, de par leur caractère public. Il convient de rappeler aux locataires que le trafic sur des réseaux externes risque d'être intercepté. Ils doivent donc, si besoin, sécuriser les applications ou le transport de ces réseaux pour en garantir la confidentialité et l'intégrité.

Les réseaux routés privés peuvent partager ces réseaux externes dans les mêmes circonstances, lorsqu'ils sont utilisés pour la connexion à un réseau public. Parfois, un réseau externe peut être utilisé par un réseau VDC d'organisation pour connecter deux vApp différents et leurs réseaux ,ou pour reconnecter un réseau vApp au centre de données d'entreprise. Dans ces cas-là, le réseau externe ne doit pas être partagé entre plusieurs organisations.

Bien entendu, on ne peut pas s'attendre à avoir un réseau physique distinct pour chaque organisation. Au lieu de cela, il est recommandé de connecter un réseau physique partagé à un seul réseau externe clairement identifié comme réseau DMZ. Les organisations sauront ainsi qu'elles ne fournissent pas de protections de confidentialité. Si des communications traversent un réseau externe et nécessitent des protections de confidentialité telles qu'une connexion de centre de données entre un vApp et une entreprise ou un pont entre deux vApp sur un réseau public, par exemple, un VPN peut être déployé. Cela se produit, car pour être accessible, le vApp d'un réseau routé privée doit utiliser le transfert d'adresse IP à l'aide d'une adresse IP pouvant être acheminée sur ce réseau externe. Tout autre vApp qui se connecte à ce réseau physique peut envoyer des paquets à ce vApp, même s'il s'agit d'une autre organisation connectée à un autre réseau externe. Pour éviter cela, un fournisseur de services peut utiliser NSX Distributed Firewall et le routage logique distribué pour appliquer la séparation du formulaire de trafic de plusieurs locataires sur un seul réseau externe. Reportez-vous à la section NSX Distributed Firewall et routage logique dans *VMware vCloud® Architecture Toolkit™ for Service Providers* (vCAT-SP)

Les réseaux VDC d'organisation appartenant à différents locataires peuvent partager le même réseau externe (une liaison montante à partir d'une passerelle Edge, par exemple) tant qu'ils n'y autorisent pas l'accès avec le masquage NAT et IP.

Important vCloud DirectorLa mise en réseau avancée permet aux locataires et aux fournisseurs de services d'utiliser des protocoles de routage dynamique tels qu'OSPF. Lorsque le mécanisme de découverte automatique OSPF est utilisé sans authentification, il peut éventuellement établir des relations de peering entre des passerelles Edge appartenant à différents locataires et démarrer l'échange de routes. Pour éviter cela, n'activez pas OSPF sur les interfaces partagées publiques, sauf si vous activez également l'authentification de OSPF pour empêcher le peering avec des passerelles Edge non authentifiées.

Pools de réseaux

Un pool de réseaux unique peut être utilisé par plusieurs locataires à condition que tous les réseaux du pool soient correctement isolés. Les pools de réseaux reposant sur VXLAN (par défaut) s'appuient sur la configuration des commutateurs physiques et virtuels pour permettre la connectivité au sein d'un VXLAN et l'isolation entre différents réseaux VXLAN. Les pools de réseaux reposant sur un groupe de ports doivent être configurés avec des groupes de ports isolés les uns des autres. Ces groupes de ports peuvent être isolés physiquement via des réseaux VXLAN.

Parmi les trois types de pools de réseaux (groupe de ports VLAN et VXLAN), il est plus facile de partager un pool de réseaux VXLAN vCloud Director. Les pools VXLAN prennent en charge un plus grand nombre de réseaux que les pools de réseaux reposant sur VLAN ou sur un groupe de ports, et l'isolation est appliquée sur la couche du noyau vSphere. Tant que les commutateurs physiques utilisent VXLAN pour isoler le trafic, VXLAN est correctement configuré sur la couche matérielle. Comme indiqué ci-dessus, aucun des réseaux d'un pool de réseaux n'assure la protection de la confidentialité des paquets interceptés (au niveau de la couche physique, par exemple).

Profils de stockage

Les profils de stockage vCloud Director agrègent les banques de données pour que le fournisseur de service puisse proposer des capacités de stockage hiérarchisées en fonction de la capacité, des performances et d'autres attributs. Les organisations de locataire ne peuvent pas accéder aux banques de données individuelles. Un locataire peut alors choisir parmi un ensemble de profils de stockage proposés par le fournisseur de services. Si les banques de données sous-jacentes sont configurées pour être accessibles uniquement depuis le réseau de gestion vSphere, le risque du partage de banques de données est limité à la disponibilité, comme pour les ressources de calcul. Une organisation peut finir par utiliser plus de stockage que prévu, ce qui limite la quantité de stockage disponible pour les autres organisations. Cela s'applique notamment aux organisations qui utilisent le modèle d'allocation de paiement à l'utilisation et le paramètre de stockage illimité par défaut. C'est pourquoi, si vous partagez des banques de données, vous devez définir une limite de stockage, activer le provisionnement dynamique, si possible, et bien surveiller l'utilisation du stockage. Vous devez également bien gérer vos baux de stockage, comme indiqué dans Limitation de la consommation partagée des ressources partagées. Si vous ne partagez pas de banques de données, vous devez dédier correctement le stockage aux profils de stockage que vous mettez à la disposition de chaque organisation. Le stockage risque alors d'être gaspillé en étant alloué à des organisations qui n'en ont pas besoin.

Les objets de banque de données vSphere sont les volumes logiques dans lesquels les VMDK sont stockés. Les administrateurs de vSphere peuvent voir les systèmes de stockage physique à partir desquels ces banques de données sont créées, ce qui nécessite des droits dont ne bénéficient pas l'administrateur ou le locataire de vCloud Director. Les utilisateurs locataires qui créent et téléchargent des vApp se contentent de stocker les VMDK des vApp dans l'un des profils de stockage disponibles sur le VDC d'organisation qu'ils utilisent.

C'est pourquoi les machines virtuelles voient uniquement le stockage consommé par leurs VMDK, sauf si elles disposent d'une connectivité réseau à ces systèmes de stockage. Cela n'est pas recommandé par ce guide. Un fournisseur peut offrir un accès au stockage externe des vApp en tant que service réseau, mais il doit être séparé des LUN attribués aux hôtes vSphere qui sauvegardent le cloud.

De même, les organisations de locataires ne voient que les profils de stockage disponibles dans leur VDC d'organisation, et même cette vue est limitée à l'abstraction vCloud Director. Elles ne peuvent pas parcourir les banques de données du système. Elles ne voient que ce qui est publié dans les catalogues ou utilisé par les vApp qu'elles gèrent. Si les profils de stockage des VDC d'organisation ne partagent pas de banques de données, les organisations ne peuvent pas avoir d'impact sur leur stockage respectif (sauf peut-être si elles utilisent trop de bande passante réseau pour les E/S de stockage). Même s'ils le font, les restrictions et les abstractions ci-dessus assurent un isolement approprié entre les organisations. Les administrateurs de vCloud Director peuvent activer vSphere Storage I/O Control sur des banques de données spécifiques pour limiter la capacité d'un locataire à utiliser trop de bande passante d'E/S de stockage. Reportez-vous à la section Configurer la prise en charge de Storage I/O Control dans un VDC fournisseur dans le *Guide de l'administrateur de vCloud Director*.

Gestion des comptes utilisateur

La gestion des utilisateurs et leurs informations d'identification est essentielle à la sécurité d'un système. Il est essentiel d'appliquer les meilleures pratiques de gestion des utilisateurs et de leurs mots de passe, car toutes les authentifications vers et dans le système vCloud Director utilisent les nom d'utilisateur et mot de passe.

Cette rubrique vise à définir les fonctionnalités et limitations de la gestion des utilisateurs et des mots de passe dans vCloud Director et fournit des recommandations sur la sécurisation de la gestion et de l'utilisation tenant compte de ces contraintes.

Limitations des comptes utilisateur locaux

vCloud Director met à disposition un fournisseur d'identité autonome pour les comptes utilisateur créés et gérés dans la base de données vCloud Director. N'étant pas par nature vulnérable dans un système configuré avec un accès réseau limité à la base de données (reportez-vous à la section Configuration du réseau de gestion), ces comptes ne fournissent pas les types de fonctions de gestion de mot de passe exigées par certains secteurs d'activité (p. ex., la norme de sécurité des données PCI). Pour éviter toute attaque de force brute, les comptes locaux doivent être soumis à une limite de tentatives de mot de passe et à des règles de verrouillage de compte.

Les fournisseurs de services doivent examiner attentivement les avantages et les risques que présentent l'utilisation de comptes locaux pour les administrateurs système et doivent soigneusement contrôle les adresses IP source autorisées à s'authentifier auprès de l'URL cloud d'une organisation si des comptes administrateur système locaux sont configurés. Nous conseillons vivement d'éliminer, ou tout au moins de limiter, l'utilisation de ce fournisseur d'identité pour les comptes administrateur système.

Une nouvelle installation de vCloud Director crée un compte administrateur système local. Dans la configuration par défaut, vCloud Director requiert qu'au moins un compte administrateur système demeure local. Un fournisseur de services qui a activé l'organisation du système pour utiliser le service SSO (fournisseur d'identité SAML) de vSphere ou LDAP, peut configurer vCloud Director pour ne fonctionner avec aucun compte administrateur système local en procédant comme suit :

1 Créez un ou plusieurs comptes pour les administrateurs de votre système dans le service SSO de (fournisseur d'identité SAML) vSphere ou LDAP.

2 Importez ces comptes dans l'organisation du système.

3 Exécutez la commande `manage-config` de l'outil de gestion des cellules pour reconfigurer le système de telle manière qu'aucun compte administrateur système local ne soit requis et qu'aucun administrateur système avec un compte local ne puisse s'authentifier auprès du système.

```
./cell-management-tool manage-config -n local.sysadmin.disabled -v true
```

Notez que cela ne désactive pas les comptes locaux des autres organisations.

Note Dans un système sans compte d'administrateur système local, les commandes de l'outil de gestion des cellules qui requièrent les informations d'identification d'administrateur système doivent utiliser l'option `-i --pid` à la place, *pid* étant remplacé par l'ID de processus de la cellule. Reportez-vous à « Référence de l'outil de gestion des cellules » dans le *Guide de l'administrateur de vCloud Director*.

4 Vous pouvez annuler cette modification à l'aide d'une ligne de commande de l'outil de gestion des cellules similaire, ce qui réactive l'accès des administrateurs système disposant de comptes locaux.

```
./cell-management-tool manage-config -n local.sysadmin.disabled -v false
```

Gestion des mots de passe

La plupart des fournisseurs d'identité LDAP, OAUTH et SAML proposent des fonctionnalités ou s'intègrent à des systèmes pour gérer les cas d'oubli de mot de passe d'un utilisateur. Ce document ne couvre pas ce cas de figure. L'outil de gestion des cellules vCloud Director inclut une commande `recover-password` qui peut être utilisée pour récupérer le mot de passe perdu d'un administrateur système. Il n'existe aucune fonctionnalité native de vCloud Director permettant de gérer ce problème pour d'autres utilisateurs locaux. Il est recommandé de sécuriser le stockage de tous les mots de passe des comptes locaux à l'aide d'une méthode approuvée par votre service de sécurité informatique. Certaines organisations verrouillent les mots de passe dans un coffre. D'autres utilisent des programmes de stockage de mots de passe gratuits ou payants. Ce document ne recommande aucune méthode particulière.

Niveau de sécurité des mots de passe

Le niveau de sécurité des mots de passe des utilisateurs du fournisseur d'identité dépend des contrôles fournis par celui-ci et/ou des outils utilisés pour gérer les utilisateurs dans l'annuaire. Par exemple, si vous connectez vCloud Director à Active Directory, les contrôles standard de longueur, complexité et historique des mots de passe Active Directory, associés à Microsoft Active Directory, sont appliqués par l'annuaire même. D'autres fournisseurs d'identité ont tendance à prendre en charge des fonctionnalités similaires. Les détails des contrôles de niveau de sécurité des mots de passe sont propres à l'annuaire et ne sont pas abordés ici de manière plus spécifique.

vCloud Director requiert que les mots de passe des utilisateurs locaux contiennent au minimum six caractères. Cette exigence n'est pas configurable et aucun autre contrôle de complexité ou d'historique des mots de passe n'est disponible. Il est recommandé que tous les utilisateurs, notamment les administrateurs système et de l'organisation, choisissent avec grand soin leurs mots de passe pour se protéger contre les attaques de force brute (voir section relative aux problèmes de verrouillage de compte plus loin).

Protection des mots de passe utilisateur

Les informations d'identification des utilisateurs gérés par un fournisseur d'identité ne sont jamais stockées dans la base de données de vCloud Director. Elles sont transmises à l'aide de la méthode choisie par le fournisseur d'identité. Reportez-vous à la section Configuration des fournisseurs d'identité pour plus d'informations sur la sécurisation de ce canal d'informations.

Les mots de passe des utilisateurs locaux se voient appliquer une valeur et sont hachés avant leur stockage dans la base de données vCloud Director. Les mots de passe en texte brut ne peuvent pas être récupérés à partir de la base de données. Pour authentifier les utilisateurs locaux, le mot de passe présenté est haché et comparé au contenu du champ de leur mot de passe dans la base de données.

Autres mots de passe

En plus des informations d'identification des utilisateurs locaux, la base de données vCloud Director stocke les mots de passe des serveurs vCenter connectés et des NSX Managers. Les modifications apportées à ces mots de passe ne sont pas automatiquement mises à jour dans le système. Vous devez les modifier manuellement à l'aide du script de configuration vCloud Director (pour le mot de passe de la base de données vCloud Director) ou l'interface utilisateur Web de vCenter et NSX.

vCloud Director gère également les mots de passe pour accéder aux clés privées associées à ses certificats TLS/SSL, ainsi que les mots de passe dans la base de données vCloud Director, les serveurs vCenter et les serveurs de NSX Manager comme indiqué plus haut. Ces mots de passe sont chiffrés à l'aide d'une clé unique par installation vCloud Director et stockés dans le fichier `$VCLOUD_HOME/etc/global.properties`. Comme mentionné à la section Protection des fichiers sensibles après l'installation, prenez soin de protéger toute sauvegarde qui contient ce fichier.

Contrôle d'accès basé sur les rôles

vCloud Director implémente un modèle d'autorisation basé sur les rôles. Cette section traite des sources d'identité, types d'utilisateurs, contrôles d'authentification, rôles et droits différents présents dans vCloud Director. Il est important de comprendre ces informations pour sécuriser correctement le système et fournir l'accès appropriés aux personnes adéquates.

Une organisation de locataires vCloud Director peut contenir un nombre arbitraire d'utilisateurs et de groupes. Les utilisateurs peuvent être créés localement par l'administrateur de l'organisation ou importés à partir d'un service d'annuaire externe (LDAP) ou d'un fournisseur d'identité (OAUTH, SAML). Les utilisateurs importés peuvent être membres d'un ou plusieurs groupes. Tous les rôles affectés à plusieurs groupes sont attribués à l'utilisateur qui en est membre. Chaque organisation est créée avec un ensemble de droits par défaut et un ensemble de rôles prédéfinis qui incluent des combinaisons de ces

droits. Un administrateur système peut accorder des droits supplémentaires à une organisation, que les administrateurs peuvent utiliser pour créer des rôles personnalisés locaux pour l'organisation. Les autorisations au sein d'une organisation sont contrôlées via l'attribution de droits et de rôles à des utilisateurs et des groupes.

Aucun utilisateur non authentifié n'est autorisé à accéder aux fonctionnalités vCloud Director via la console Web, le portail de locataires ou l'API vCloud. Chaque utilisateur s'authentifie à l'aide d'un nom d'utilisateur et d'un mot de passe. Vous pouvez configurer des stratégies de tentative de mot de passe et de verrouillage de compte au niveau global et par organisation.

Les rôles sont des regroupements de droits qui fournissent des fonctionnalités à l'utilisateur auquel ils sont attribués. Les rôles prédéfinis sont les suivants :

- Administrateur système
- Administrateur d'organisation
- Auteur du catalogue
- Auteur de vApp
- Utilisateur de vApp
- Accès via la console uniquement

Le *Guide de l'administrateur de vCloud Director* identifie également les droits attribués à chacun de ces rôles. Cette section a pour objectif de vous aider à choisir le rôle approprié pour chaque type d'utilisateur. Par exemple, le rôle d'utilisateur vApp peut être adapté à un administrateur qui doit mettre sous et hors tension des machines virtuelles, mais s'il doit également modifier la quantité de mémoire affectée à une machine virtuelle, le rôle Auteur vApp est plus adapté. Il est possible que ces rôles ne comportent pas les ensembles de droits exacts correspondant à vos organisations de locataires ; les administrateurs d'organisation peuvent toutefois créer des rôles personnalisés. Ce document ne contient pas de description des droits spécifiques que vous pouvez combiner pour créer un rôle personnalisé utile.

Configuration des fournisseurs d'identité

Une organisation de locataires vCloud Director peut définir un fournisseur d'identité qu'elle partage avec d'autres applications ou entreprises. Les utilisateurs s'authentifient vis-à-vis du fournisseur d'identité pour obtenir un jeton qu'ils peuvent ensuite utiliser pour se connecter à l'organisation. Une telle stratégie peut permettre à une entreprise de fournir un accès à plusieurs services indépendants, notamment vCloud Director, avec un seul ensemble d'informations d'identification, dispositif souvent appelé Single Sign-On.

À propos des fournisseurs d'identité

vCloud Director prend en charge les types de fournisseurs d'identité suivants :

OAuth	Une organisation peut définir un fournisseur d'identité externe qui prend en charge l'authentification OAuth, telle que définie dans la RFC 6749 (http://tools.ietf.org/html/rfc6749).
SAML	Une organisation peut définir un fournisseur d'identité externe qui prend en charge la norme SAML (Security Assertion Markup Language) 2.0.
Intégré	Le fournisseur d'identité intégré est un service vCloud Director qui authentifie les utilisateurs qui sont créés localement ou importés à partir de LDAP.

OAuth

Dans n'importe quelle implémentation OAuth, la plupart des décisions de sécurité sont prises au niveau de la couche du serveur d'autorisation OAuth. vCloud Director figure dans le rôle d'un serveur de ressources, qui constitue un consommateur du jeton et est responsable uniquement de la vérification de l'intégrité du jeton.

Pour protéger vos sessions vCloud Director et les ressources sensibles sous-jacentes, le serveur d'autorisation OAuth doit être configuré en toute sécurité avec les derniers correctifs de sécurité installés.

Si le serveur d'autorisation OAuth peut être configuré pour rediriger les utilisateurs vers une URL arbitraire spécifiée par un paramètre de requête, le serveur d'autorisation OAuth doit être configuré pour valider les URL afin d'empêcher un pirate de contrôler les redirections vers des applications tierces. Une liste blanche d'applications légitimes doit être utilisée pour validation lorsqu'elle est disponible.

LDAP

Le fournisseur d'identité intégré vCloud Director prend en charge plusieurs services LDAP courants.

Reportez-vous au *Notes de mise à jour de vCloud Director* pour obtenir la liste des services LDAP pris en charge.

vCloud Director permet à l'administrateur système de définir un service LDAP pour l'ensemble du système qui peut être utilisé par tous les locataires. Les comptes d'utilisateurs locataires sont importés dans la base de données vCloud Director dans laquelle les rôles vCloud Directorsont attribués. Les mots de passe des utilisateurs LDAP sont gérés et mis à jour dans l'annuaire LDAP, au niveau duquel l'authentification s'effectue, à l'aide des paramètres spécifiés dans l'écran de configuration LDAP. Tous les contrôles de l'annuaire LDAP relatifs à l'authentification et aux mots de passe sont conservés, y compris les verrouillages dus à un échec d'authentification, l'expiration de mot de passe, l'historique, la complexité, etc., et sont propres au service LDAP sélectionné. Si une organisation est configurée pour utiliser le système LDAP, ses utilisateurs proviennent de l'unité d'organisation spécifiquement configurée dans les paramètres Service LDAP système vCloud Director de cette organisation.

Les fournisseurs de cloud peuvent autoriser les organisations de locataires à utiliser une unité d'organisation dans le système LDAP ou à héberger leur propre service d'annuaire LDAP. Dans les deux cas, un accès de gestion approprié à cet annuaire doit être fourni pour permettre à l'administrateur de l'organisation de gérer les utilisateurs. L'absence de ce type de contrôle impliquerait une charge supplémentaire pour l'administrateur système et empêcherait l'organisation de contrôler de manière simple et correcte l'accès à ses VDC. Si ces contrôles de gestion sont inexistants, une organisation doit uniquement utiliser un annuaire LDAP privé hébergé et géré par ses soins.

La connectivité entre les cellules de vCloud Director et le serveur LDAP du système ainsi que les serveurs LDAP d'une organisation doit être activée pour permettre au logiciel d'authentifier correctement les utilisateurs. Tel que le recommande ce document, le serveur LDAP du système doit se trouver sur le réseau de gestion privé, séparé de la zone DMZ par un pare-feu. Certains fournisseurs de cloud et la plupart des organisations informatiques exécuteront les serveurs LDAP requis, qui seraient également placés sur un réseau privé, non dans la zone DMZ. Une autre possibilité consiste à héberger et gérer un serveur LDAP d'organisation hors de l'environnement du fournisseur de cloud et sous le contrôle de l'organisation. Dans ce cas, il doit être exposé aux cellules de vCloud Director, potentiellement via la propre zone DMZ du centre de données de l'entreprise.

Quel que soit le cas de figure, les ports appropriés doivent être ouverts via les différents pare-feux à l'emplacement entre les cellules et le serveur LDAP, tel que décrit à la section LDAP via TLS/SSL. De plus, l'exposition du serveur LDAP hébergé par une organisation via sa zone DMZ soulève des préoccupations. Ce service ne doit pas être accessible au grand public ; des mesures doivent donc être appliquées pour limiter l'accès uniquement aux cellules de vCloud Director. Pour cela, une méthode simple consiste à configurer le serveur LDAP et/ou le pare-feu externe pour autoriser uniquement l'accès à partir d'adresses IP appartenant aux cellules de vCloud Director signalées par le fournisseur de cloud. Il existe d'autres solutions , par exemple, l'intégration de systèmes tels que des VPN site-à-site par organisation, qui connectent ces deux ensembles de systèmes, des proxys LDAP ou annuaires virtuels renforcés, ou encore d'autres alternatives non décrites dans de ce document.

En revanche, les fournisseurs de cloud doivent savoir que les serveurs LDAP hébergés par une organisation et gérés par des clients peu scrupuleux peuvent être utilisés lors d'une attaque contre d'autres organisations. Par exemple, une organisation demande le nom d'une organisation qui est celui d'une autre organisation, mais avec une erreur d'orthographe courante, et utilise l'URL de connexion d'apparence similaire lors d'une attaque par hameçonnage. Pour y remédier et se protéger contre d'autres attaques interlocataires similaires, le fournisseur peut limiter les adresses IP source de demandes chaque fois que possible, pour éviter toute tentative de connexion entre des organisations et veiller à différencier clairement les noms d'organisation qu'il attribue.

LDAP via TLS/SSL

Il est vivement recommandé de configurer un annuaire LDAPv3 pour l'authentification utilisateur. vCloud Director doit être configuré pour se connecter à des serveurs LDAP via SSL dans le but de protéger correctement les mots de passe validés au niveau de ces serveurs. Reportez-vous à la section « Configuration d'une connexion LDAP » dans le *Guide de l'administrateur de vCloud Director* pour plus de détails. La configuration LDAP la plus sécurisée spécifie **Utiliser SSL** et requiert un certificat SSL fourni par le service LDAP.

Si le certificat signé du serveur LDAP n'est pas disponible, le certificat de l'autorité de certification qui signe le certificat du serveur LDAP doit être importé dans le système ou le magasin de clés JCE (JCEKS) d'une organisation. Les configurations LDAP qui spécifient un magasin de clés JCE sont également sécurisées, mais elles peuvent faire l'objet d'une configuration incorrecte en cas d'approbation d'un nombre élevé de certificats d'autorité de certification (ou même un nombre élevé de certificats propres au serveur). De plus, il est préférable de choisir un fournisseur LDAP qui prend en charge l'authentification Kerberos.

La connectivité au serveur LDAP est requise. Tandis que le service LDAP brut (non-SSL) s'exécute sur le port 389/TCP, les serveurs qui prennent en charge le service LDAP via SSL utilisent le port 636/TCP par défaut ; toutefois, ce port est également configurable. Notez que vCloud Director prend en charge la méthode du service LDAP hérité via SSL (LDAPS), mais ne prend pas en charge la négociation TLS dans le cadre d'une connexion LDAP à l'aide de la commande StartTLS.

Pour finir, le serveur d'annuaire LDAP doit être correctement configuré avec un certificat SSL. La procédure à suivre n'est pas indiquée dans ce document.

Importation de groupes

L'importation de groupes dans vCloud Director permet d'éviter l'importation manuelle de chaque utilisateur disposant du même rôle. Lorsque les utilisateurs LDAP se connectent, les rôles mappés aux groupes dont ils sont membres sont attribués à leur session. Les appartenances de groupe d'utilisateurs changent suivant les modifications apportées à leurs fonctions dans l'organisation ; c'est pourquoi les rôles attribués à ces utilisateurs changent automatiquement en fonction du mappage groupe-rôle. Cela permet aux organisations d'intégrer facilement des rôles cloud à des groupes/rôles d'organisation internes et aux systèmes qui les provisionnent et les gèrent.

Par exemple, une organisation peut décider d'accorder initialement aux utilisateurs LDAP le rôle Accès via la Console uniquement pour limiter leurs droits. Pour cela, tous les utilisateurs qui requièrent ce rôle de base sont ajoutés à un seul groupe LDAP, et, lors de l'importation de ce groupe, l'administrateur de l'organisation lui attribue le rôle Accès via la Console uniquement. Puis, ces utilisateurs disposant de fonctions supplémentaires à réaliser peuvent être ajoutés à d'autres groupes LDAP, également importés dans vCloud Director et affectés à ces rôles disposant de privilèges supplémentaires. Par exemple, les utilisateurs qui doivent créer des catalogues peuvent être ajoutés au groupe Auteur de catalogue de l'organisation A, dans le serveur LDAP de l'organisation. L'administrateur de l'organisation A peut alors importer le groupe Auteur de catalogue de l'organisation A et le mapper au rôle Auteur de catalogue prédéfini dans vCloud Director. Pour effectuer cette opération, suivez les instructions indiquées à la section Importation d'un groupe dans le *Guide de l'utilisateur de vCloud Director*.

Liste de contrôle

7

Cette liste de contrôle récapitule les tâches de configuration de sécurité des clés décrites dans ce document.

- Outre les instructions données dans ce document, vous devez surveiller les avis de sécurité sur le site http://www.vmware.com/security/advisories/ et vous inscrire pour recevoir les alertes par e-mail en utilisant le formulaire de cette page. Des conseils de sécurité supplémentaires et les derniers avis pour vCloud Director seront publiés sur cette page.
- Les administrateurs doivent appliquer les étapes recommandées dans *Sécurité vSphere* (https://docs.vmware.com/fr/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html), *Sécurisation de VMware NSX pour vSphere* (https://communities.vmware.com/docs/DOC-27674) et le *Guide de configuration de la sécurité NSX-v 6.3.x* (https://communities.vmware.com/docs/DOC-28142) pour vous assurer de la bonne installation de ces produits.
- Appliquez les correctifs de sécurité en cours à la plate-forme cellulaire Linux, la base de données vCloud Director et l'infrastructure virtuelle avant l'installation ; une surveillance continue pour conserver ces composants à un niveau de correctif approprié est également essentielle.
- Des procédures de renforcement de la sécurité standard doivent être appliquées à la plate-forme cellulaire Linux, y compris la désactivation des services inutiles sur le réseau, la suppression des modules inutiles, la restriction de l'accès racine à distance et l'application de stratégies de mot de passe fort. Si possible, utilisez un service d'authentification centralisé comme Kerberos. Envisagez l'installation d'outils de surveillance et de détection d'intrusions.
- Il est possible d'installer des applications supplémentaires et de configurer des utilisateurs supplémentaires sur la plate-forme cellulaire Linux, mais il est recommandé de ne pas le faire. L'élargissement de l'accès au système d'exploitation de la cellule peut réduire la sécurité.
- Mettez le fichier `responses.properties` uniquement à la disposition de ceux en ayant besoin. Lorsqu'il est en cours d'utilisation (lors de l'ajout de cellules à un groupe de serveurs), disposez les contrôles d'accès appropriés à l'emplacement accessible à tous les hôtes cibles. Toute sauvegarde effectuée doit être soigneusement contrôlée et également chiffrée si votre logiciel de sauvegarde prend en charge cette fonction. Une fois le logiciel installé sur tous les hôtes de serveur, toutes les copies du fichier `responses.properties` se trouvant dans ces emplacements accessibles doivent être supprimées.

- Les fichiers `responses.properties` et `global.properties` sont protégés par les contrôles d'accès du dossier `$VCLOUD_ HOME/etc` et des fichiers eux-mêmes. Ne modifiez pas les autorisations des fichiers ou du dossier.
- L'accès physique et logique aux serveurs vCloud Director doit être strictement limité aux personnes ayant besoin de s'y connecter et uniquement avec les niveaux minimaux d'accès requis. Cela implique la restriction de l'utilisation du compte racine via `sudo` et d'autres meilleures pratiques. Toutes les sauvegardes des serveurs doivent être strictement protégées et chiffrées, avec les clés gérées séparément des sauvegardes.
- Pour les exigences relatives à la sécurité des bases de données, consultez les guides de sécurité correspondant au logiciel de base de données vCloud Director que vous avez choisi.
- L'utilisateur de la base de données vCloud Director ne doit pas se voir accorder de privilèges sur les autres bases de données de ce serveur ou d'autres privilèges d'administration système.
- Assurez-vous que les informations d'identification utilisées pour l'accès administratif à la cellule, aux dispositifs vCenter Serverconnectés, à la base de données vCloud Director, aux pare-feu et aux autres périphériques suivent les normes de complexité du mot de passe.
- Il est important, pour une protection fiable, de diversifier les mots de passe d'administration pour les différents serveurs de l'environnement vCloud Director, y compris les cellules, la base de données vCloud Director, ainsi que les dispositifs vCenter Server et NSX.
- Reportez-vous à la page https://docs.vmware.com/fr/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-779A011D-B2DD-49BE-B0B9-6D73ECF99864.html pour plus d'informations sur la création et le remplacement des certificats utilisés par vCenter et ESXi. Cette pratique est vivement recommandée.
- Les certificats vCenter doivent avoir un champ de nom commun correspondant au nom de domaine complet du serveur sur lequel vCenter est installé.
- Configurez vCloud Director pour vérifier les certificats vCenter.
- Les certificats vCenter doivent être signés par une autorité de certification et ont un nom commun correspondant au nom de domaine complet de l'hôte sur lequel la cellule est installée.
- L'approche recommandée pour la mise à disposition des services vCloud Director à l'extérieur consiste à placer les cellules dans un DMZ, avec un pare-feu de réseau séparant Internet des cellules vCloud Director présentes sur le DMZ. Le seul port devant être autorisé à traverser le pare-feu en interface avec Internet est 443/TCP.
- Comme les cellules vCloud Director se trouvent dans la zone DMZ, leur accès aux services dont elles ont besoin doit également être régulé par un pare-feu de réseau. Il est notamment recommandé que l'accès à la base de données vCloud Director, au dispositif vCenter Server, aux hôtes vSphere, aux IDP (y compris LDAP) et à tout service de sauvegarde ou similaire se trouvent de l'autre côté d'un pare-feu séparant le DMZ du réseau interne.

- Les machines virtuelles qui requièrent un accès depuis l'extérieur du cloud (par exemple, à partir d'Internet) seraient connectées soit à un réseau public, soit à un réseau privé avec acheminement NAT, avec transfert de port configuré pour les services exposés. Le réseau externe auquel ces réseaux VDC d'organisation sont connectés auraient besoin d'un pare-feu de protection qui autorise le trafic convenu sur ce réseau de zone DMZ.
- En général, il est recommandé que les vApp ayant besoin d'accessibilité à partir d'Internet soient placés sur un réseau acheminé privé. Cela assure l'application des règles de contrôle de locataire sur le pare-feu et de transfert de port fournies par NSX. Ces règles, ainsi que d'autres, peuvent être appliquées par défaut par le pare-feu de réseau que vous choisissez de déployer. Consultez la documentation de votre pare-feu pour obtenir des instructions de configuration spécifiques et connaître ses capacités par défaut.
- Une doctrine prônant une protection fiable requiert le blocage des API JMX (port 8999/TCP) et JMS (ports 61611/TCP et 61616/TCP) au niveau du pare-feu de réseau qui protège le DMZ auquel les cellules sont connectées.
- Définissez l'URL Web publique, l'adresse proxy de la console publique et l'URL de base de l'API REST publique pour un cloud multicellulaire derrière un pare-feu d'application Web ou un équilibrage de charge.
- Un pare-feu d'application Web (WAF) doit être déployé devant les cellules vCloud Director.
- Lors de tels déploiements, il est recommandé que le pare-feu d'application Web soit configuré de manière à permettre l'inspection et le blocage approprié du trafic malveillant. Cela s'effectue généralement avec la terminaison TLS ou SSL.
- Lorsque vous configurez la terminaison TLS ou SSL, il est important non seulement d'installer un certificat signé par une autorité de certification sur le pare-feu d'application Web (WAF) afin que les applications clientes de l'API vCloud et de la console Web puissent être certaines de l'identité du serveur, mais également d'utiliser un certificat signé par une autorité de certification sur les cellules, même si elles sont uniquement visibles par le WAF.
- Enfin, si l'équilibrage de charge est indépendant du WAF, il doit également utiliser un certificat signé par une autorité de certification.
- Il est recommandé d'activer la génération de l'en-tête `X-Forwarded-For` au niveau du pare-feu, si possible.
- Si le serveur vCloud Director possède une troisième adresse IP attribuée exclusivement à des fins de gestion, liez l'API JMX directement à cette adresse IP. Par défaut, le connecteur JMX vCloud Director est lié aux adresses IP principales spécifiées lors de la configuration. Cette valeur par défaut peut être remplacée par insertion de la propriété suivante dans /opt/vmware/vcloud-service-director/etc/global.properties : `vcloud.cell.ip.management=`*`IP ou nom d'hôte`*`.` correspondant au réseau de gestion auquel le connecteur JMX doit être lié.
- La configuration recommandée et la plus sécurisée implique la liaison du connecteur JMX à l'adresse localhost : `vcloud.cell.ip.management=127.0.0.1`. Si JMX est uniquement exposé à localhost, la

sécurisation des communications JMX est mise en œuvre grâce à l'utilisation de SSH comme mécanisme de tunnel pour tout accès à JMX. Si vos exigences en matière de gestion n'autorisent pas l'utilisation de ce type de configuration localhost et que JMX doive être exposé en dehors du serveur vCloud Director, JMX doit être sécurisé par le protocole TLS ou SSL.

- Derrière les cellules se trouvent les éléments de gestion privés requis par vCloud Director : sa base de données, le dispositif NSX, vCenter Server, le serveur LDAP système, le cas échéant, le serveur Active Directory utilisé par vCenter et les interfaces de gestion des hôtes vSphere. Leurs connexions sont strictement contrôlées par les pare-feu, ces services ne devant pas être accessibles à partir d'autres machines sur le DMZ ou directement à partir d'Internet.
- Il est également supposé que des technologies de sécurité de centre de données classiques, comme IDS/IPS, SIEM, la gestion de la configuration, la gestion des correctifs, la gestion des vulnérabilités, les antivirus et les systèmes de gestion GRC, seront appliquées à la fois sur vCloud Director, ses systèmes associés, vSphere et ses systèmes associés et les réseaux et l'infrastructure de stockage qui les prennent en charge.
- Une bonne gestion des baux, des quotas, des limites et des modèles d'allocation peut garantir l'impossibilité, pour une organisation de locataires, de refuser un service à une autre, accidentellement ou délibérément.
- Dans ces scénarios et dans d'autres, les pools de ressources, les banques de données et les réseaux doivent être segmentés dans différents domaines de sécurité à l'aide de différents VDC fournisseurs par lesquels les vApp ayant des préoccupations similaires peuvent être regroupés (ou isolés).
- Chaque fois que vous autorisez la surattribution des ressources d'un pool utilisé par plusieurs organisations de locataires, vous courez le risque de dégrader la qualité des services pour les autres locataires. Une surveillance appropriée des niveaux de service est impérative pour éviter qu'un locataire « bruyant » déclenche un refus de service. Toutefois, la sécurité ne nécessite pas une séparation des locataires dans des pools de ressources individuels pour remplir cet objectif.
- Parfois, un réseau externe peut être utilisé par un réseau VDC d'organisation pour connecter deux vApp différents et leurs réseaux ,ou pour reconnecter un réseau vApp au centre de données d'entreprise. Dans ces cas, le réseau externe ne doit pas être partagé entre les organisations de locataires.
- Pour les communications traversant un réseau externe et nécessitant également des protections en matière de confidentialité (par exemple, une connexion vApp-centre de données d'entreprise ou un pont vApp-vApp), il est recommandé qu'un dispositif NSX Edge ou autre dispositif VPN virtuel soit déployé dans le réseau VDC d'organisation.
- Si des pools de réseaux doivent être partagés entre locataires, il est plus sûr de partager un pool reposant sur le VXLAN, qui prend en charge bien d'autres réseaux qu'un pool reposant sur le VLAN et met en œuvre l'isolation au niveau de la couche du noyau ESXi.
- Si vous partagez des banques de données sur des profils de stockage, vous devez définir une limite de stockage, activer le provisionnement dynamique si possible et surveiller avec attention l'utilisation de l'espace de stockage. Gérez également soigneusement les baux de l'espace de stockage vApp.

- Les machines virtuelles ne voient jamais d'espace de stockage en dehors de leurs VDMK, sauf si elles disposent d'une connectivité réseau à ces systèmes de stockage. Ce guide recommande qu'elles ne disposent pas de ce type de connectivité. Un fournisseur peut octroyer un accès à l'espace de stockage externe pour les vApp en tant que service réseau, mais il doit être séparé des LUN attribués aux hôtes vSphere soutenant le cloud.
- Comme défini dans *Sécurité vSphere* (https://docs.vmware.com/fr/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html), il est important que le réseau de gestion soit séparé des réseaux de données de machine virtuelle.
- De même, le réseau de gestion doit être séparé du DMZ qui fournit un accès aux administrateurs d'organisation.
- Les réseaux de stockage sont également physiquement séparés. Cette méthode suit les meilleures pratiques vSphere et protège l'organisation de locataires et l'espace de stockage du fournisseur contre les machines virtuelles malveillantes.
- vMotion n'est pas toujours placé sur un réseau distinct du réseau de gestion ; toutefois, dans le cloud, cela est important du point de vue de la séparation des fonctions. vMotion s'exécute généralement en lieu sûr et, s'il est installé sur le réseau de gestion, il permet à un administrateur fournisseur ou à un autre utilisateur disposant d'un accès à ce réseau, d'espionner le trafic vMotion, enfreignant ainsi les règles de confidentialité des locataires. C'est pourquoi vous devez créer un réseau physique distinct pour vMotion de charges de travail cloud.
- Examiner régulièrement les journaux à la recherche d'activités suspectes, inhabituelles ou non autorisées est une bonne pratique en matière de sécurité. L'analyse régulière des journaux facilite également l'identification des pannes et des erreurs de configuration système, et le respect des contrats de niveau de service.
- Un serveur syslog peut être configuré pendant l'installation. Nous recommandons l'utilisation d'une infrastructure syslog TLS. L'exportation de journaux vers un serveur syslog est recommandée pour plusieurs raisons. Il est recommandé que le serveur `syslog` soit configuré avec la redondance, afin que les événements essentiels soient toujours consignés. Les organisations menant des opérations de sécurité et des opérations informatiques peuvent également bénéficier du regroupement et de la gestion centralisés des journaux de diagnostics. Nous recommandons l'utilisation de `logrotate` ou de méthodes similaires pour contrôler la taille des journaux et le nombre d'anciens fichiers journaux à conserver.
- Assurez-vous que vous disposez d'un espace disque suffisant pour héberger les journaux de diagnostics et les journaux de demandes Jetty. La journalisation centralisée garantit l'absence de risque de perte de précieuses informations diagnostiques une fois la taille maximale totale de 400 Mo de fichiers journaux atteinte, et les fichiers substitués et supprimés.
- Les autres systèmes connectés à vCloud Director et utilisés par ce dernier créent des journaux d'audit qui doivent être regroupés dans le cadre de vos processus d'audit. Parmi ces journaux, citons ceux provenant de NSX, de la base de données vCloud Director, de vCenter Server et des hôtes vSphere.

- Une fois le compte d'administrateur système local initial créé, il est vivement recommandé de gérer tous les comptes d'administrateur système par le biais d'un fournisseur d'identité comme LDAP ou le service SSO vSphere.
- Certains fournisseurs de cloud peuvent choisir d'autoriser les organisations à utiliser une unité d'organisation au sein du LDAP système ou à héberger l'annuaire LDAP de l'organisation. Dans les deux cas, un accès de gestion approprié à cet annuaire doit être fourni pour permettre à l'administrateur de l'organisation de gérer les utilisateurs. En l'absence de tels contrôles de gestion, une organisation de locataires doit uniquement utiliser un annuaire LDAP privé qu'elle héberge et gère elle-même.
- Autre problème survenant lorsque l'organisation héberge son propre serveur LDAP : l'exposition en dehors de son DMZ. Ce service ne doit pas être accessible au grand public ; des mesures doivent donc être appliquées pour limiter l'accès uniquement aux cellules de vCloud Director. Pour cela, il suffit de configurer le serveur LDAP et/ou le pare-feu externe de manière à n'autoriser l'accès qu'à partir d'adresses IP appartenant aux cellules vCloud Director.
- Le fournisseur peut prendre des mesures de protection à cet égard et contre des attaques interlocataires similaires, en limitant les adresses IP sources des demandes lorsque cela est possible, ainsi qu'en s'assurant que les noms d'organisation qu'il attribue aux locataires sont toujours bien différents.
- vCloud Director doit être configuré pour se connecter à des serveurs LDAP via SSL afin de protéger correctement les mots de passe validés au niveau de ces serveurs. Lors de la configuration du protocole LDAP sur SSL, n'acceptez pas tous les certificats.
- Les meilleures pratiques en matière de gestion des utilisateurs et de leurs mots de passe doivent être comprises et appliquées.
- Les systèmes de gestion des journaux, les systèmes de gestion des événements et des informations de sécurité (SIEM) ou d'autres systèmes de surveillance doivent être utilisés pour surveiller les tentatives de décodage des mots de passe via des attaques par force brute.
- Il est recommandé de stocker en toute sécurité les mots de passe des administrateurs systèmes et d'organisation, d'une manière approuvée par votre service de sécurité informatique.