Guide d'installation et de mise à niveau de vCloud Director

vCloud Director 5.6

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

FR-001288-01

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Guide d’installation et de mise à niveau de VMware vCloud Director

Le *Guide d’installation et de mise à niveau de VMware vCloud Director* explique comment installer ou mettre à niveau le logiciel VMware® vCloud Director® et le configurer pour fonctionner avec VMware vCenter™ en vue de fournir des services VMware vCloud® compatibles VMware.

Public cible

Le *Guide d’installation et de mise à niveau de VMware vCloud Director* est conçu pour toute personne souhaitant installer ou mettre à niveau le logiciel VMware vCloud Director. Les informations contenues dans ce guide sont destinées à des administrateurs système expérimentés maîtrisant Linux, Windows, les réseaux IP et VMware vSphere®.

Présentation de l'installation, la configuration et la mise à niveau de vCloud Director

1

Un vCloud® VMware associe un groupe de serveurs vCloud Director à la plate-forme vSphere. Pour créer un groupe de serveurs vCloud Director, il suffit d'installer le logiciel vCloud Director sur un ou plusieurs serveurs, de connecter les serveurs à une base de données partagée et d'intégrer le groupe de serveurs vCloud Director à vSphere.

La configuration initiale de vCloud Director, incluant des informations de connexion à la base de données et au réseau, est établie lors de l'installation. Lorsque vous mettez à niveau une installation existante vers une nouvelle version de vCloud Director, vous mettez à niveau le schéma de logiciel et de base de données de vCloud Director, en laissant en place les relations existantes entre les serveurs, la base de données et vSphere.

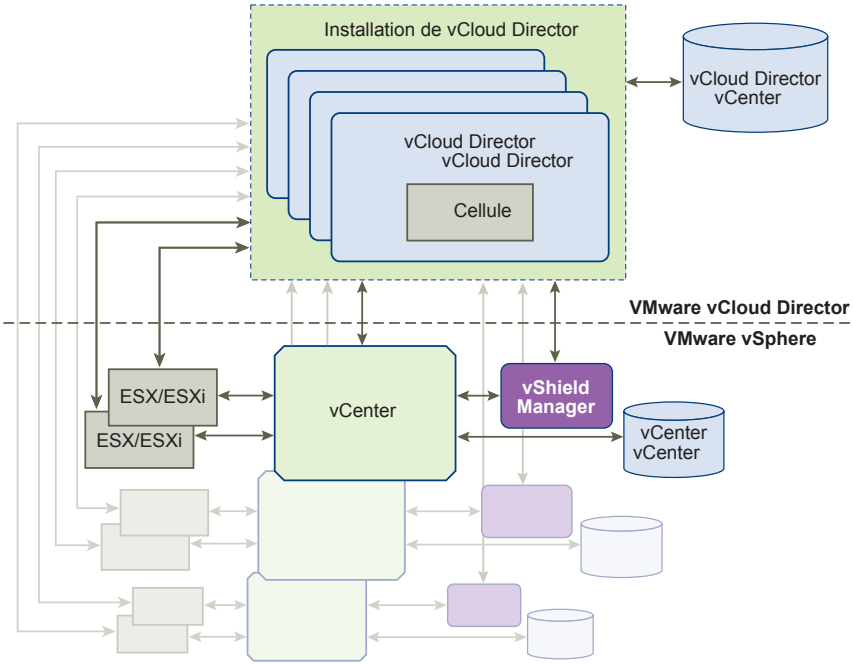
Ce chapitre aborde les rubriques suivantes :

Architecture de vCloud Director

Un groupe de serveurs vCloud Director est constitué d'un ou de plusieurs serveurs vCloud Director. Ces serveurs partagent une base de données commune et sont liés à un nombre arbitraire de systèmes vCenter Server et d'hôtes ESXi. Les services réseau sont fournis aux systèmes vCenter Server et vCloud Director par le composant VMware vShield Manager™ depuis VMware vCloud® Networking and Security™ ou par le composant VMware NSX Manager™ depuis VMware NSX™ pour vSphere®.

Une installation typique crée un groupe de serveurs vCloud Director comprenant plusieurs serveurs. Chaque serveur dans le groupe exécute un ensemble de services appelé cellule vCloud Director. Tous les membres du groupe partagent la même base de données. Chaque cellule du groupe se connecte à plusieurs systèmes vCenter Server, aux hôtes qu'ils gèrent et à chaque dispositif vShield Manager ou NSX Manager configuré pour prendre en charge chacun des systèmes vCenter Server.

Figure 1-1. Diagramme de l'architecture vCloud Director pour une installation qui utilise vShield Manager



Le processus d'installation et de configuration de vCloud Director crée les cellules, les connecte à la base de données partagée et établit les premières connexions à un système vCenter Server, au dispositif vShield Manager ou NSX Manager associé à ce système vCenter Server et à ses hôtes. Un administrateur système peut ensuite utiliser la console Web vCloud Director pour ajouter à tout moment des systèmes vCenter Server, le dispositif vShield Manager ou NSX Manager associé au système vCenter Server ajouté et les hôtes du système vCenter Server ajouté au groupe de serveurs vCloud Director.

Planification de la configuration

vSphere fournit les capacités de stockage, de calcul et de mise en réseau à vCloud Director. Avant de commencer l'installation, évaluez la capacité vSphere et vCloud Director dont vous avez besoin et planifiez votre configuration en fonction.

Les exigences en matière de configuration dépendent de nombreux facteurs, tels que le nombre d'organisations que compte le Cloud, le nombre d'utilisateurs que compte chaque organisation et le niveau d'activité de ces utilisateurs. Les recommandations suivantes peuvent servir de point de départ pour la plupart des configurations :

- Allouez un serveur vCloud Director (cellule) à chaque système vCenter Server devant être accessible dans votre Cloud.
- Assurez-vous que tous les serveurs vCloud Director sont conformes à la configuration minimale requise en termes de mémoire et de stockage. Pour plus de détails, consultez « Configuration matérielle et logicielle requise pour installer vCloud Director », page 9
- Configurez la base de données vCloud Director comme indiqué dans« Installation et configuration d'une base de données vCloud Director », page 15.

Configuration matérielle et logicielle requise pour installer vCloud Director

Chaque serveur d'un groupe de serveurs vCloud Director doit répondre à certaines exigences tant au niveau du matériel que des logiciels. En outre, tous les membres du groupe doivent pouvoir accéder à une base de données prise en charge. Chaque groupe de serveurs doit accéder à un serveur vCenter Server, un dispositif vShield Manager ou NSX Manager et un ou plusieurs hôtes ESXi.

Plates-formes prises en charge

Les informations actuelles concernant les plates-formes VMware prises en charge par cette édition de vCloud Director sont disponibles dans les *matrices d'interopérabilité des produits VMware* situées dans VMware Partner Central. Connectez-vous à VMware Partner Central à l'aide des informations de votre compte partenaire VMware.

Configuration vSphere requise

Les serveurs et les hôtes à utiliser avec vCloud Director doivent avoir une configuration spécifique.

- Les réseaux vCenter que vous prévoyez d'utiliser en tant que réseaux externes ou pools de réseaux vCloud Director doivent être disponibles pour tous les hôtes de tout cluster devant être utilisés par vCloud Director. Si vous rendez ces réseaux disponibles pour tous les hôtes d'un centre de données, il vous sera plus facile d'ajouter de nouveaux serveurs vCenter à vCloud Director.
- Les vSphere Distributed Switches doivent être utilisés pour le clôturage entre hôtes et l'allocation de pools de réseaux.
- Les clusters vCenter utilisés avec vCloud Director doivent configurer le DRS de stockage avec un niveau d'automatisation défini sur **Entièrement automatisé**. Cette configuration exige un stockage partagé connecté à tous les hôtes ESXi dans un cluster DRS. vCloud Director peut tirer pleinement parti de Storage DRS, notamment du provisionnement rapide, avec vCenter 5.1 ou version ultérieure.
- Les serveurs vCenter doivent approuver leurs hôtes. Tous les hôtes dans tous les clusters gérés par vCloud Director doivent être configurés pour nécessiter des certificats d'hôte vérifiés. Vous devez en particulier déterminer, comparer et sélectionner des empreintes correspondantes pour tous les hôtes. Consultez la section Configurer les paramètres SSL dans la documentation *vCenter Server et gestion des hôtes*.

Licences vSphere requises

vCloud Director requiert les licences vSphere suivantes :

- VMware DRS, sous licence vSphere Enterprise et Enterprise Plus.
- VMware Distributed Switch et dvFilter, sous licence vSphere Enterprise Plus. Cette licence permet de créer et d'utiliser des réseaux isolés vCloud Director.

Systèmes d'exploitation serveurs pris en charge par vCloud Director

Tableau 1-1. Systèmes d'exploitation serveurs pris en charge par vCloud Director

Système d'exploitation (64 bits seulement)	Mises à jour
CentOS 6	4
Red Hat Enterprise Linux 5	4-10
Red Hat Enterprise Linux 6	1-5

Espace disque requis

Chaque serveur vCloud Director requiert environ 1 350 Mo d'espace disque libre destiné aux fichiers d'installation et aux journaux.

Mémoire requise

Chaque serveur vCloud Director doit disposer d'au moins 4 Go de mémoire.

Packages logiciels Linux

Chaque serveur vCloud Director doit inclure des installations de plusieurs packages logiciels Linux communs. Ces packages sont généralement installés par défaut avec le logiciel du système d'exploitation. En cas de packages manquants, le programme d'installation échoue et affiche un message de diagnostic.

Tableau 1-2. Packages logiciels requis

Nom du package	Nom du package	Nom du package
alsa-lib	libICE	module-init-tools
bash	libSM	net-tools
chkconfig	libstdc	pciutils
coreutils	libX11	procps
findutils	libXau	redhat-lsb
glibc	libXdmcp	sed
grep	libXext	tar
initscripts	libXi	which
krb5-libs	libXt	
libgcc	libXtst	

Remarque Plusieurs procédures de configuration des connexions réseau et de création de certificats SSL requièrent l'utilisation de la commande Linux `nslookup` disponible dans le package Linux `bind-utils`.

Bases de données vCloud Director prises en charge

vCloud Director prend en charge les bases de données Oracle et Microsoft SQL Server. Les informations à jour sur les bases de données prises en charge par cette édition de vCloud Director sont disponibles dans les *matrices d'interopérabilité des produits VMware* situées dans VMware Partner Central. Connectez-vous à VMware Partner Central à l'aide des informations de votre compte partenaire VMware.

Pour plus d'informations sur les configurations de serveur de base de données recommandées, consultez « Installation et configuration d'une base de données vCloud Director », page 15

Serveurs LDAP pris en charge

Tableau 1-3. Serveurs LDAP pris en charge

Plate-forme	Serveur LDAP	Méthodes d'authentification
Windows Server 2003	Active Directory	Simple, SSL simple, Kerberos, Kerberos SSL
Windows Server 2008	Active Directory	Simple
Windows 7 (2008 R2)	Active Directory	Simple, SSL simple, Kerberos, Kerberos SSL
Linux	OpenLDAP	Simple, SSL simple

Systèmes d'exploitation clients pris en charge

Consultez le *Guide de l'utilisateur de vCloud Director* pour obtenir une liste des systèmes d'exploitation clients pris en charge.

Bases de données prises en charge pour le stockage des données des mesures historiques

Vous pouvez configurer votre installation vCloud Director de façon à stocker les mesures que vCloud Directorcollecte sur les performances et la consommation de ressources de la machine virtuelle. Les données concernant les mesures historiques sont stockées dans une base de données KairosDB dépendant de Cassandra. Pour plus d'informations, reportez-vous à la section Chapitre 6, « Installer et configurer le logiciel de base de données facultatif pour stocker et récupérer les mesures historiques de performances de machine virtuelle », page 71.

vCloud Director prend en charge les versions suivantes de KairosDB et Cassandra.

- KairosDB 0.9.1
- Cassandra 1.2 et 2.0

Navigateurs qui prennent en charge vCloud Director

La console Web vCloud Director est compatible avec les versions récentes de Google Chrome, de Mozilla Firefox et de Microsoft Internet Explorer.

Remarque La console Web de vCloud Director est uniquement compatible avec les navigateurs 32 bits. Lorsque les spécifications d'un navigateur indiquent qu'il est pris en charge sur une plate-forme 64 bits, il s'agit en fait d'un navigateur 32 bits fonctionnant sur une plate-forme 64 bits.

Prise en charge des navigateurs sur les plates-formes Linux

Sur ces plates-formes Linux, la console Web vCloud Director est compatible avec la version la plus récente de Mozilla Firefox et Google Chrome, et avec les versions qui les précèdent immédiatement.

Tableau 1-4. Navigateurs pris en charge et systèmes d'exploitation compatibles sur les plates-formes Linux

Plate-forme	Google Chrome	Mozilla Firefox
CentOS 6.*x*	OUI	OUI
Red Hat Enterprise Linux 6.*x*	OUI	OUI
Ubuntu 12.*x*	OUI	OUI

Prise en charge des navigateurs sur les plates-formes Windows

Sur les plates-formes Windows, la console Web vCloud Director est compatible avec au moins une version de Microsoft Internet Explorer. Certaines plates-formes Windows sont également compatibles avec la version la plus récente de Mozilla Firefox et Google Chrome, et avec les versions qui les précèdent immédiatement.

Tableau 1-5. Navigateurs pris en charge et systèmes d'exploitation compatibles sur les plates-formes Microsoft Windows

Plate-forme	Google Chrome	Mozilla Firefox	Internet Explorer 8.*x*	Internet Explorer 9.*x*	Internet Explorer 10.*x*
Windows XP Pro	OUI	OUI	OUI	Non	Non
Windows Server 2003 Enterprise Edition	OUI	OUI	OUI	Non	Non
Windows Server 2008	OUI	OUI	OUI	OUI	OUI
Windows Server 2008 R2	OUI	OUI	OUI	OUI	OUI
Windows Vista	OUI	Non	OUI	OUI	OUI
Windows 7	OUI	OUI	OUI	OUI	OUI
Windows 8	OUI	OUI	Non	Non	OUI

Prise en charge des navigateurs sur les plates-formes Macintosh

Sur les plates-formes Macintosh, la console Web vCloud Director est compatible avec la version la plus récente de Mozilla Firefox et Google Chrome, et avec les versions qui les précèdent immédiatement.

Versions prises en charge d'Adobe Flash Player

La console Web vCloud Director nécessite Adobe Flash Player 11,2 ou une version supérieure. Seule la version 32 bits est prise en charge.

Versions prises en charge de Java

La version JRE 1.6.0 Update 10 ou ultérieure doit être installée et activée sur les clients vCloud Director. Seule la version 32 bits est prise en charge.

Versions des protocoles TLS et SSL et suites de chiffrement prises en charge

vCloud Director requiert que les clients utilisent SSL. Les protocoles de serveur SSL suivants sont pris en charge :

- TLS versions 1.0, 1.1 et 1.2
- SSL version 3

Les suites de chiffrement prises en charge comprennent celles disponibles avec les signatures RSA, DSS ou Elliptic Curve et les ciphers DES3, AES-128 ou AES-256.

Résumé des conditions de configuration réseau de vCloud Director

Pour fonctionner de façon sécurisée et fiable, vCloud Director doit s'appuyer sur un réseau également sécurisé et fiable prenant en charge la résolution (ainsi que la résolution inverse) des noms d'hôtes, un service d'heure réseau et d'autres services. Avant de commencer l'installation de vCloud Director, vérifiez que le réseau respecte ces conditions requises.

Le réseau qui connecte les serveurs vCloud Director, le serveur de base de données, les serveurs vCenter Server et les composants vCloud Networking and Security ou NSX pour vSphere associés doit remplir plusieurs critères :

Adresses IP

Chaque serveur vCloud Director requiert deux adresses IP pour pouvoir prendre en charge deux connexions SSL différentes. Une connexion est destinée au service HTTP. L'autre est destinée au service de proxy de la console. Vous pouvez utiliser des alias IP ou plusieurs interfaces réseau pour créer ces adresses. Vous ne pouvez pas utiliser la commande Linux `ip addr add` pour créer la seconde adresse.

Adresse du proxy de la console

L'adresse IP configurée en tant qu'adresse du proxy de la console ne doit pas être située derrière un équilibreur de charge configuré pour la terminaison SSL ou un proxy inverse. Toutes les demandes au proxy de la console doivent être transmises directement à l'adresse IP du proxy de la console.

Service d'heure réseau

Vous devez utiliser un service d'heure réseau, tel que NTP pour synchroniser les horloges de tous les serveurs vCloud Director, notamment celle du serveur de base de données. Le décalage maximal autorisé entre les horloges des serveurs synchronisés ne doit pas dépasser 2 secondes.

Fuseaux horaire des serveurs

Tous les serveurs vCloud Director, y compris le serveur de base de données, doivent être configurés pour se trouver dans le même fuseau horaire.

Résolution des noms d'hôtes

Tous les noms d'hôte que vous définissez pendant l'installation et la configuration doivent pouvoir être résolus par DNS en utilisant la recherche directe ou inversée du nom de domaine qualifié complet ou du nom d'hôte non qualifié. Par exemple, pour un hôte `vcloud.example.com`, les deux commandes suivantes doivent aboutir sur un hôte vCloud Director :

```
nslookup vcloud
nslookup vcloud.example.com
```

En outre; si l'hôte `vcloud.exemple.com` a l'adresse IP 192.168.1.1, la commande suivante doit retourner `vcloud.example.com`:

```
nslookup 192.168.1.1
```

Stockage du serveur de transfert

Pour fournir un espace de stockage temporaire pour les envois, les téléchargements et les éléments de catalogue publiés ou faisant l'objet d'abonnements en externe, vous devez rendre un volume NFS ou de stockage partagé accessible à tous les serveurs dans un groupe de serveurs vCloud Director. Ce volume partagé doit avoir un accès en écriture pour la

racine. Chaque membre du groupe de serveurs doit monter ce volume sur le même point de montage, généralement `/opt/vmware/vcloud-director/data/transfer`. L'espace de ce volume est consommé de deux façons :

- Les transferts (envois et téléchargements) occupent cet espace de stockage pendant tout le transfert et ils sont supprimés à la fin de celui-ci. Les transferts qui ne progressent pas pendant 60 minutes sont marqués comme étant expirés et sont effacés du système. Étant donné que les images transférées peuvent être volumineuses, il est conseillé d'allouer au moins plusieurs centaines de giga-octets à ce type d'opération.
- Les éléments de catalogues qui sont publiés en externe et permettent la mise en cache du contenu publié occupent ce stockage tant qu'ils existent. (Les éléments de catalogues qui sont publiés en externe mais qui ne permettent pas la mise en cache n'occupent pas ce stockage.) Si vous activez des organisations dans votre cloud pour créer des catalogues qui sont publiés en externe, partez du principe que des centaines, voire des milliers d'éléments de catalogue nécessiteront de l'espace sur ce volume et que chaque élément aura la taille d'une machine virtuelle en format OVF compressé.

Remarque Si possible, le volume utilisé pour le stockage du serveur de transfert doit avoir une capacité facilement extensible.

Recommandations concernant 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. Tout autre trafic entrant provenant d'un réseau public doit être rejeté par le pare-feu.

Tableau 1-6. 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	ActiveMQ
61616	TCP	ActiveMQ

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

Tableau 1-7. 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, vShield Manager, NSX Manager et ESX
514	UDP	Facultatif. Active l'utilisation de syslog.
902	TCP	Connexions vCenter et ESX.
903	TCP	Connexions vCenter et ESX.
920	TCP, UDP	NFS rpc.statd utilisé par le service de transfert.
1433	TCP	Port de base de données Microsoft SQL Server par défaut.
1521	TCP	Port de base de données Oracle par défaut.
5672	TCP, UDP	Facultatif. Messages AMQP des extensions de tâche.
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- Routez le trafic entre les serveurs vCloud Director et le serveur de base de données vCloud Director via un réseau privé dédié, si possible.
- 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 niveau 2.

Installation et configuration d’une base de données vCloud Director

Les cellules de vCloud Director utilisent une base de données pour stocker les informations partagées. Cette base de données doit exister avant que vous puissiez effectuer l’installation et la configuration du logiciel vCloud Director.

Remarque Quel que soit le logiciel de base de données que vous choisissez, vous devez créer un schéma de base de données distinct, destiné à vCloud Director. vCloud Director ne peut pas partager un schéma de base de données avec un autre produit VMware.

Configuration d’une base de données Oracle

Les bases de données Oracle doivent répondre à des exigences de configuration spécifiques en vue de les utiliser avec vCloud Director. Installez et configurez une instance de base de données et créez le compte d'utilisateur de base de données vCloud Director avant d'installer vCloud Director.

Procédure

1 Configurez le serveur de base de données.

Un serveur de base de données configuré avec une mémoire de 16 Go, un espace de stockage de 100 Go et 4 CPU devrait suffire pour la plupart des clusters vCloud Director.

2 Créez l’instance de base de données.

Utilisez une commande au format suivant pour créer un espace de tables CLOUD_DATA unique :

```
Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1500M
autoextend on;
```

3 Créez le compte d’utilisateur de la base de données vCloud Director.

La commande suivante crée le nom d’utilisateur de la base de données `vcloud` avec le mot de passe `vcloudpass`.

```
Create user $vcloud identified by $vcloudpass default tablespace CLOUD_DATA;
```

Remarque Lorsque vous créez le compte d’utilisateur de la base de données vCloud Director, vous devez spécifier CLOUD_DATA comme espace de tables par défaut.

4 Configurez les paramètres de base de données, de processus et de transaction.

La base de données doit être configurée pour autoriser au moins 75 connexions par cellule vCloud Director, plus environ 50 pour Oracle. Vous pouvez calculer les autres paramètres de configuration en fonction du nombre de connexions, où *C* représente le nombre de cellules dans le cluster vCloud Director.

Paramètre de configuration Oracle	Valeur des cellules *C*
CONNECTIONS	75**C*+50
PROCESSES	= CONNECTIONS
SESSIONS	= PROCESSES*1.1+5
TRANSACTIONS	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

5 Créez le compte d’utilisateur de la base de données vCloud Director.

N’utilisez pas le compte de l’administrateur système Oracle comme compte d’utilisateur de la base de données vCloud Director. Vous devez créer un compte d’utilisateur dédié pour la base de données. Accordez les privilèges système suivants au compte :

- CONNECTER
- RESSOURCE
- CRÉER UN DÉCLENCHEUR
- CRÉER UN TYPE
- CRÉER UNE VUE
- CRÉER UNE VUE MATÉRIALISÉE

- CRÉER UNE PROCÉDURE
- CRÉER UNE SÉQUENCE

6 Notez le nom du service de la base de données. Vous en aurez besoin lors de la configuration des connexions au réseau et à la base de données.

Pour rechercher le nom du service de base de données, ouvrez le fichier `$ORACLE_HOME/network/admin/tnsnames.ora` sur le serveur de base de données et recherchez une entrée de format :

```
(SERVICE_NAME = orcl.example.com)
```

Configuration d'une base de données Microsoft SQL Server

Les bases de données SQL Server doivent répondre à des exigences de configuration spécifiques en vue de les utiliser avec vCloud Director. Installez et configurez une instance de base de données, puis créez le compte d'utilisateur de la base de données vCloud Director avant d'installer vCloud Director.

Les performances de la base de données vCloud Director sont déterminantes pour les performances et l'évolutivité de vCloud Director. vCloud Director utilise le fichier `tmpdb` de SQL Server pour stocker des volumes importants de résultats, trier des données et gérer des données simultanément lues et modifiées. La taille de ce fichier peut énormément augmenter lorsque vCloud Director traite simultanément plusieurs charges de travail. Il est conseillé de créer le fichier `tmpdb` sur un volume dédié avec des performances élevées de lecture et d'écriture. Pour plus d'informations sur le fichier `tmpdb` et les performances de SQL Server, consultez http://msdn.microsoft.com/en-us/library/ms175527.aspx.

Prérequis

- Vous devez être familier avec les commandes, l'exécution des scripts, et les opérations de Microsoft SQL Server.
- Pour configurer Microsoft SQL Server, ouvrez une session sur l'ordinateur hôte SQL Server avec des informations d'identification d'administrateur. Vous pouvez configurer le serveur SQL de sorte qu'il fonctionne avec l'identité LOCAL_SYSTEM ou une identité disposant d'un privilège permettant d'exécuter un service Windows.

Procédure

1 Configurez le serveur de base de données.

Un serveur de base de données configuré avec une mémoire de 16 Go, un espace de stockage de 100 Go et 4 CPU devrait suffire pour la plupart des clusters vCloud Director.

2 Spécifiez l'authentification en mode mixte lors de la configuration de SQL Server.

L'authentification Windows n'est pas prise en charge pour l'utilisation de SQL Server avec vCloud Director.

3 Créez l'instance de base de données.

Le script suivant crée les fichiers de base de données et de journalisation et spécifie la séquence d'assemblage appropriée.

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE = 100MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\vcloud.ldf', SIZE = 1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
```

Les valeurs indiquées pour SIZE sont des suggestions. Mais des valeurs plus importantes peuvent être nécessaires.

4 Définissez le niveau d'isolation des transactions.

Le script suivant définit le niveau d'isolation de la base de données sur READ_COMMITTED_SNAPSHOT.

```
USE [vcloud]
GO
ALTER DATABASE [vcloud] SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcloud] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
```

Pour en savoir plus sur l'isolation des transactions, consultez http://msdn.microsoft.com/en-us/library/ms173763.aspx.

5 Créez le compte d'utilisateur de la base de données vCloud Director.

Le script suivant crée le nom d'utilisateur de la base de données `vcloud` avec le mot de passe `vcloudpass`.

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
   DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

6 Attribuez des autorisations au compte d'utilisateur de la base de données vCloud Director.

Le script suivant attribue le rôle `db_owner` à l'utilisateur de la base de données créé dans Étape 5.

```
USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

Création de certificats SSL

vCloud Director utilise SSL pour sécuriser les communications entre les clients et les serveurs. Avant d'installer et de configurer un groupe de serveurs vCloud Director, vous devez créer deux certificats pour chaque membre du groupe et importer les certificats dans des keystores hôtes.

Chaque serveur vCloud Director nécessite deux adresses IP pour qu'il puisse prendre en charge deux points d'extrémité SSL différents. Chaque point de terminaison requiert son propre certificat SSL. Les certificats pour ces deux points de terminaison doivent inclure un nom distinct X.500 et une extension de nom alternatif d'objet X.509.

Procédure

1 Répertoriez les adresses IP pour ce serveur.

Utilisez une commande, telle que `ifconfig` pour détecter les adresses IP de ce serveur.

2 Pour chaque adresse IP, exécutez la commande suivante afin de récupérer le nom de domaine complet auquel l'adresse IP est liée.

```
nslookup ip-address
```

3 Notez chaque adresse IP, le nom de domaine complet qui y est associé et indiquez si vCloud Director doit utiliser l'adresse du service HTTP ou le service proxy de la console.

   Vous avez besoin des noms de domaine complets pour créer les certificats, et des adresses IP pour configurer les connexions au réseau et à la base de données. Si d'autres noms DNS peuvent accéder à l'adresse IP, notez-les également, car vous devrez les indiquer au moment de spécifier un autre nom de l'objet.

4 Créez les certificats.

   Vous pouvez utiliser des certificats signés par une autorité de certification de confiance ou des certificats autosignés.

   Remarque Les certificats signés offrent le niveau de confiance le plus élevé.

Création et importation d'un certificat SSL signé

Les certificats signés offrent le niveau de confiance le plus élevé pour les communications SSL.

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 pouvez utiliser des certificats signés par une autorité de certification de confiance ou des certificats autosignés. Les certificats signés offrent le niveau de confiance le plus élevé.

Important Ces exemples spécifient une taille de clé de 2 048 bits, mais vous devez évaluer les conditions de sécurité de votre installation avant de choisir une taille de clé appropriée. Les tailles de clés inférieures à 1 024 bits ne sont plus prises en charge par la publication spéciale NIST 800-131A.

Pour créer et importer des certificats auto-signés, consultez « Création d'un certificat SSL autosigné », page 22.

Prérequis

- Générer la liste des noms de domaine complets et leur adresse IP associée sur ce serveur.
- Choisir une adresse à utiliser pour le service HTTP et une adresse à utiliser pour le service de proxy de la console. Reportez-vous à « Création de certificats SSL », page 18.
- Vérifiez que vous avez accès à un ordinateur sur lequel un environnement d'exécution Java version 7 est installé, afin de pouvoir créer le certificat à l'aide de la commande `keytool`. Le programme d'installation de vCloud Director place une copie de `keytool` dans `/opt/vmware/vcloud-director/jre/bin/keytool`. Toutefois, vous pouvez effectuer cette procédure sur tout ordinateur doté d'un environnement d'exécution Java version 7. L'utilisation de certificats créés avec `keytool` provenant de toute autre source n'est pas prise en charge par vCloud Director. Le processus d'installation et de configuration est plus facile lorsque vous créez et importez les certificats avant d'installer et de configurer le logiciel vCloud Director. Les exemples de ligne de commande suivants supposent que `keytool` réside dans le chemin d'accès de l'utilisateur. Dans ces exemples, *motdepasse* représente le mot de passe du keystore.
- Les certificats pour ces deux points de terminaison doivent inclure un nom distinct X.500 et une extension de nom alternatif d'objet X.509. Familiarisez-vous avec la commande `keytool`, en particulier ses options `-dname` et `-ext`.

- Rassemblez les informations requises pour l'argument de l'option keytool `–dname`.

Tableau 1-8. Informations requises par l'option keytool `–dname`

Sous-partie du nom distinct X.500	mot clé keytool	Description	Exemple
commonName	CN	Nom de domaine complet associé à l'adresse IP de ce point de terminaison.	CN=vcd1.example.com
organizationalUnit	OU	Nom d'une unité d'organisation, comme un département ou une division, au sein de l'organisation à laquelle ce certificat est associé.	OU=Ingénierie
organizationName	O	Nom de l'organisation à laquelle ce certificat est associé	O=Exemple de corporation
localityName	L	Nom de la ville dans laquelle l'organisation est située.	L=Palo Alto
stateName	T	Nom de l'état ou de la province où l'organisation est située.	S=California
pays	C	Nom du pays dans lequel l'organisation est située.	C=US

Procédure

1 Créez un certificat non approuvé (sans confiance) pour le service HTTP.

Cet exemple de commande crée un certificat non approuvé dans un fichier keystore nommé `certificates.ks`. Les options `keytool` ont été placées sur des lignes distinctes pour davantage de clarté. Les informations du nom distinct X.500 fournies dans l'argument de l'option `–dname` utilisent les valeurs indiquées dans les conditions requises. Les valeurs DNS et IP indiquées dans l'argument de l'option `–ext` sont des valeurs type. Assurez-vous d'inclure tous les noms DNS pour lesquels ce point de terminaison est accessible, y compris celui que vous avez spécifié pour la valeur `commonName` (CN) dans l'argument de l'option `–dname`. Vous pouvez également inclure les adresses IP, tel qu'indiqué ici.

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

IMPORTANT Le fichier keystore et le répertoire dans lequel il est stocké doivent être accessible par l'utilisateur `vcloud.vcloud`. Le programme d'installation vCloud Director crée cet utilisateur et ce groupe.

2 Créez un certificat non approuvé pour le service de proxy de la console.

Cette commande ajoute un certificat non approuvé au fichier keystore créé dans Étape 1. Les options `keytool` ont été placées sur des lignes distinctes pour davantage de clarté. Les informations du nom distinct X.500 fournies dans l'argument de l'option `–dname` utilisent les valeurs indiquées dans les conditions requises. Les valeurs DNS et IP indiquées dans l'argument de l'option `–ext` sont des valeurs type. Assurez-vous d'inclure tous les noms DNS pour lesquels ce point de terminaison est accessible, y compris celui que vous avez spécifié pour la valeur `commonName` (CN) dans l'argument de l'option `–dname`. Vous pouvez également inclure les adresses IP, tel qu'indiqué ici.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 Créez une demande de signature du certificat associé au service HTTP.

La commande suivante crée une demande de signature de certificat dans le fichier `http.csr`.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass passwd –certreq –alias http –
file http.csr
```

4 Créez une demande de signature de certificat pour le service de proxy de la console.

La commande suivante crée une demande de signature de certificat dans le fichier `consoleproxy.csr`.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass passwd –certreq –alias
consoleproxy –file consoleproxy.csr
```

5 Envoyez les demandes de signature à votre autorité de certification.

Si votre autorité de certification requiert que vous spécifiiez un type de serveur Web, utilisez Jakarta Tomcat.

6 Une fois que vous avez reçu les certificats signés, importez-les dans le fichier keystore.

a Importez le certificat racine de l'autorité de certification dans le fichier keystore.

La commande suivante importe le certificat racine à partir du fichier `root.cer` dans le fichier keystore `certificates.ks`.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias root
–file root.cer
```

b (Facultatif) Si vous avez reçu des certificats intermédiaires, importez-les dans le fichier keystore.

La commande suivante importe les certificats intermédiaires à partir du fichier `intermediate.cer` dans le fichier keystore `certificates.ks`.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias
intermediate –file intermediate.cer
```

c Importez le certificat destiné au service HTTP.

La commande suivante importe le certificat à partir du fichier `http.cer` dans le fichier keystore `certificates.ks`.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias http
–file http.cer
```

d Importez le certificat destiné au service de proxy de la console.

La commande suivante importe le certificat à partir du fichier `consoleproxy.cer` dans le fichier keystore `certificates.ks`.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias
consoleproxy –file consoleproxy.cer
```

7 Pour vérifier que tous les certificats ont été importés, affichez le contenu du fichier keystore.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –list
```

8 Répétez cette procédure sur tous les serveurs vCloud Director du groupe de serveurs.

Suivant

Si vous avez créé le fichier keystore `certificates.ks` sur un ordinateur autre que le serveur sur lequel vous avez généré la liste des noms de domaine complets et les adresses IP associées, copiez à présent le fichier keystore sur ce serveur. Vous aurez besoin du chemin d'accès au keystore lorsque vous exécuterez le script de configuration. Reportez-vous à « Configuration des connexions au réseau et à la base de données », page 32.

Création d'un certificat SSL autosigné

Les certificats autosignés constituent un moyen pratique de configurer SSL pour vCloud Director dans des environnements où les considérations de confiance ne sont pas primordiales.

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 pouvez utiliser des certificats signés par une autorité de certification de confiance ou des certificats autosignés. Les certificats signés offrent le niveau de confiance le plus élevé.

IMPORTANT Ces exemples spécifient une taille de clé de 2 048 bits, mais vous devez évaluer les conditions de sécurité de votre installation avant de choisir une taille de clé appropriée. Les tailles de clés inférieures à 1 024 bits ne sont plus prises en charge par la publication spéciale NIST 800-131A.

Pour créer et importer des certificats signés, consultez « Création et importation d'un certificat SSL signé », page 19.

Prérequis

- Générer la liste des noms de domaine complets et leur adresse IP associée sur ce serveur.
- Choisir une adresse à utiliser pour le service HTTP et une adresse à utiliser pour le service de proxy de la console. Reportez-vous à « Création de certificats SSL », page 18.
- Vérifiez que vous avez accès à un ordinateur sur lequel un environnement d'exécution Java version 7 est installé, afin de pouvoir créer le certificat à l'aide de la commande `keytool`. Le programme d'installation de vCloud Director place une copie de `keytool` dans `/opt/vmware/vcloud-director/jre/bin/keytool`. Toutefois, vous pouvez effectuer cette procédure sur tout ordinateur doté d'un environnement d'exécution Java version 7. L'utilisation de certificats créés avec `keytool` provenant de toute autre source n'est pas prise en charge par vCloud Director. Le processus d'installation et de

configuration est plus facile lorsque vous créez et importez les certificats avant d'installer et de configurer le logiciel vCloud Director. Les exemples de ligne de commande suivants supposent que `keytool` réside dans le chemin d'accès de l'utilisateur. Dans ces exemples, *motdepasse* représente le mot de passe du keystore.

- Les certificats pour ces deux points de terminaison doivent inclure un nom distinct X.500 et une extension de nom alternatif d'objet X.509. Familiarisez-vous avec la commande `keytool`, en particulier ses options `–dname` et `–ext`.
- Rassemblez les informations requises pour l'argument de l'option keytool `–dname`.

Tableau 1-9. Informations requises par l'option keytool `–dname`

Sous-partie du nom distinct X.500	mot clé keytool	Description	Exemple
commonName	CN	Nom de domaine complet associé à l'adresse IP de ce point de terminaison.	CN=vcd1.example.com
organizationalUnit	OU	Nom d'une unité d'organisation, comme un département ou une division, au sein de l'organisation à laquelle ce certificat est associé.	OU=Ingénierie
organizationName	O	Nom de l'organisation à laquelle ce certificat est associé	O=Exemple de corporation
localityName	L	Nom de la ville dans laquelle l'organisation est située.	L=Palo Alto
stateName	T	Nom de l'état ou de la province où l'organisation est située.	S=California
pays	C	Nom du pays dans lequel l'organisation est située.	C=US

Procédure

1 Créez un certificat non approuvé (sans confiance) pour le service HTTP.

Cet exemple de commande crée un certificat non approuvé dans un fichier keystore nommé `certificates.ks`. Les options `keytool` ont été placées sur des lignes distinctes pour davantage de clarté. Les informations du nom distinct X.500 fournies dans l'argument de l'option `–dname` utilisent les valeurs indiquées dans les conditions requises. Les valeurs DNS et IP indiquées dans l'argument de l'option `–ext` sont des valeurs type. Assurez-vous d'inclure tous les noms DNS pour lesquels ce point de terminaison est accessible, y compris celui que vous avez spécifié pour la valeur `commonName` (CN) dans l'argument de l'option `–dname`. Vous pouvez également inclure les adresses IP, tel qu'indiqué ici.

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
```

```
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

IMPORTANT Le fichier keystore et le répertoire dans lequel il est stocké doivent être accessible par l'utilisateur `vcloud.vcloud`. Le programme d'installation vCloud Director crée cet utilisateur et ce groupe.

2 Créez un certificat non approuvé pour le service de proxy de la console.

Cette commande ajoute un certificat non approuvé au fichier keystore créé dans Étape 1. Les options `keytool` ont été placées sur des lignes distinctes pour davantage de clarté. Les informations du nom distinct X.500 fournies dans l'argument de l'option `–dname` utilisent les valeurs indiquées dans les conditions requises. Les valeurs DNS et IP indiquées dans l'argument de l'option `–ext` sont des valeurs type. Assurez-vous d'inclure tous les noms DNS pour lesquels ce point de terminaison est accessible, y compris celui que vous avez spécifié pour la valeur `commonName` (CN) dans l'argument de l'option `–dname`. Vous pouvez également inclure les adresses IP, tel qu'indiqué ici.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 Pour vérifier que tous les certificats ont été importés, affichez le contenu du fichier keystore.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –list
```

4 Répétez cette procédure sur tous les serveurs vCloud Director du groupe de serveurs.

Suivant

Si vous avez créé le fichier keystore `certificates.ks` sur un ordinateur autre que le serveur sur lequel vous avez généré la liste des noms de domaine complets et les adresses IP associées, copiez à présent le fichier keystore sur ce serveur. Vous aurez besoin du chemin d'accès au keystore lorsque vous exécuterez le script de configuration. Reportez-vous à « Configuration des connexions au réseau et à la base de données », page 32.

Installer et configurer vShield Manager pour une nouvelle installation de vCloud Director

vCloud Director varie selon que vShield Manager ou NSX Manager fournit les services réseau au Cloud. Avant de procéder à une nouvelle installation de vCloud Director, vous devez installer et configurer vShield Manager ou NSX Manager et associer une instance unique de vShield Manager ou de NSX Manager à chaque serveur vCenter Server que vous envisagez d'inclure à votre installation de vCloud Director.

vShield Manager est compris avec le téléchargement de VMware vCloud Networking and Security. Les informations actuelles relatives aux versions prises en charge de vShield Manager compatibles avec vCloud Director sont disponibles dans les *matrices d'interopérabilité des produits VMware* qui se trouvent dans VMware Partner Central. Connectez-vous à VMware Partner Central à l'aide des informations de votre compte partenaire VMware. Pour plus d'informations sur les conditions de réseau requises, consultez « Configuration matérielle et logicielle requise pour installer vCloud Director », page 9.

IMPORTANT Cette procédure ne s'applique que dans le cas d'une nouvelle installation de vCloud Director. Si vous mettez à niveau une installation de vCloud Director existante, consultez Chapitre 3, « Mise à niveau de vCloud Director », page 41.

Prérequis

- Vérifiez que chacun de vos systèmes vCenter Server remplit les conditions requises pour l'installation de vShield Manager.
- Exécutez l'installation du dispositif virtuel de vShield Manager décrite dans le *Guide d'installation et de mise à niveau de vShield*.

Procédure

1. Connectez-vous au dispositif virtuel de vShield Manager que vous avez installé et confirmez les paramètres spécifiés lors de l'installation.
2. Associez le dispositif virtuel de vShield Manager que vous avez installé au système vCenter Server que vous envisagez d'ajouter à vCloud Director dans votre installation de vCloud Director.

Suivant

Configurez l'assistance VXLAN dans le dispositif vShield Manager associé. vCloud Director crée des pools de réseaux VXLAN pour fournir des ressources réseau aux VDC fournisseurs. Si l'assistance VXLAN n'est pas configurée dans le dispositif vShield Manager associé, les VDC fournisseurs indiquent une erreur de pool de réseaux ; vous devez créer un type de pool de réseaux différent et l'associer au VDC fournisseur. Pour plus d'informations sur la manière de configurer l'assistance VXLAN, consultez le *Guide d'administration vShield*.

Installer et configurer NSX Manager pour une nouvelle installation de vCloud Director

Pour fournir des services réseau au Cloud, vCloud Director doit être associé à un dispositif vShield Manager ou NSX Manager. Avant de procéder à une nouvelle installation de vCloud Director, vous devez installer et configurer vShield Manager ou NSX Manager et associer une instance unique de vShield Manager ou de NSX Manager à chaque serveur vCenter Server que vous envisagez d'inclure à votre installation de vCloud Director.

NSX est compris dans le téléchargement VMware NSX pour vSphere. Vous trouverez des informations actualisées sur les versions de NSX Manager prises en charge et compatibles avec vCloud Director dans le document *Matrices d'interopérabilité des produits VMware*, sur VMware Partner Central. Connectez-vous à VMware Partner Central à l'aide des informations de votre compte partenaire VMware. Pour plus d'informations sur les conditions de réseau requises, consultez « Configuration matérielle et logicielle requise pour installer vCloud Director », page 9.

IMPORTANT Cette procédure ne s'applique que dans le cas d'une nouvelle installation de vCloud Director. Si vous mettez à niveau une installation de vCloud Director existante, consultez Chapitre 3, « Mise à niveau de vCloud Director », page 41.

Prérequis

- Assurez-vous que tous vos systèmes vCenter Server remplissent les conditions préalables pour installer NSX Manager.
- Exécutez la tâche d'installation du dispositif virtuel NSX Manager décrite dans le *Guide d'installation et de mise à niveau de NSX*.

Procédure

1. Connectez-vous au dispositif virtuel NSX Manager que vous avez installé et confirmez les paramètres indiqués lors de l'installation.
2. Associez le dispositif virtuel NSX Manager installé au système vCenter Server que vous prévoyez d'ajouter à vCloud Director dans votre installation planifiée de vCloud Director.

Suivant

Configurez la prise en charge de VXLAN sur le dispositif NSX Manager associé. vCloud Director crée des pools de réseaux VXLAN pour fournir des ressources réseau aux VDC fournisseurs. Si la prise en charge de VXLAN n'est pas configurée sur le dispositif NSX Manager associé, les VDC fournisseurs renvoient une erreur de pool de réseaux, ce qui vous oblige à créer un autre type de pool de réseaux et à l'associer à chaque VDC fournisseur. Pour plus d'informations sur la configuration de la prise en charge de VXLAN, consultez le *Guide d'administration de NSX*.

Installation et configuration d'un courtier AMQP

Le protocole AMQP (Advanced Message Queuing Protocol) est un protocole ouvert pour la mise en file d'attente des messages qui prend en charge les systèmes de messagerie flexibles des entreprises. vCloud Director inclut un service AMQP que vous pouvez configurer de sorte qu'il fonctionne avec un courtier AMQP, comme RabbitMQ. Les opérateurs du Cloud bénéficient ainsi d'un flux de notifications concernant les événements dans le Cloud. Si vous souhaitez utiliser ce service, vous devez installer et configurer un courtier AMQP.

Bien qu'il soit facultatif d'utiliser le courtier AMQP avec vCloud Director, un certain nombre d'intégrations utilisent AMQP pour communiquer avec vCloud Director. Consultez les documents d'installation et de configuration pour plus de détails sur les intégrations que vous envisagez d'utiliser.

Procédure

1 Téléchargez le serveur RabbitMQ depuis http://info.vmware.com/content/12834_rabbitmq.

2 Suivez les instructions d'installation de RabbitMQ pour l'installer sur tout hôte approprié.

Chaque cellule vCloud Director doit pouvoir accéder à l'hôte du serveur RabbitMQ sur le réseau.

3 Au cours de l'installation de RabbitMQ, notez les valeurs que vous devrez fournir pour configurer vCloud Director afin qu'il fonctionne avec cette installation de RabbitMQ.

- Le nom de domaine complet de l'hôte du serveur RabbitMQ, par exemple `amqp.example.com`.
- Un nom d'utilisateur et un mot de passe valides destinés à l'authentification avec RabbitMQ.
- Le port sur lequel le courtier écoute les messages. Le port par défaut est `5672`.
- L'hôte virtuel RabbitMQ. Par défaut « / ».

Suivant

Par défaut, le service AMQP de vCloud Director envoie des messages non chiffrés. Si vous configurez le service pour qu'il chiffre les messages avec SSL, le service vérifie le certificat du courtier à l'aide du magasin d'approbations JCEKS par défaut de l'environnement d'exécution Java sur le serveur vCloud Director. L'environnement d'exécution Java se trouve en général dans le répertoire `$JRE_HOME/lib/security/cacerts`.

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 et un mot de passe

Si vous n'avez pas besoin de valider le certificat du courtier AMQP, vous pouvez sélectionner **Accepter tous les certificats**.

Téléchargement et installation de la clé publique VMware

Le fichier d'installation est signé numériquement. Pour vérifier la signature, vous devez télécharger et installer la clé publique VMware.

Vous pouvez utiliser l'outil Linux `rpm` et la clé publique VMware pour vérifier la signature numérique du fichier d'installation de vCloud Director ou de tout autre fichier signé téléchargé de `vmware.com`. Si vous installez la clé publique sur l'ordinateur lorsque vous envisagez d'installer vCloud Director, la vérification s'effectue au cours de l'installation ou de la mise à niveau. Vous pouvez également vérifier manuellement la signature avant de commencer la procédure d'installation ou de mise à niveau. Utilisez ensuite le fichier vérifié pour toutes les installations ou les mises à niveau.

Remarque Le site de téléchargement publie également une valeur de somme de contrôle (checksum) pour tout fichier téléchargé. La somme de contrôle est publiée sous deux formes courantes. La somme de contrôle vérifie que le contenu du fichier que vous avez téléchargé est le même que le contenu publié. Elle ne vérifie pas la signature numérique.

Procédure

1 Créez un répertoire pour stocker les clés publiques VMware.

2 Utilisez un navigateur Web pour télécharger toutes les clés publiques de l'offre publique VMware depuis le répertoire http://packages.vmware.com/tools/keys.

3 Enregistrez les fichiers des clés dans le répertoire que vous avez créé.

4 Pour chaque clé que vous téléchargez, exécutez la commande suivante pour l'importer.

```
# rpm --import /key_path/key_name
```

key_path est le répertoire dans lequel vous avez enregistré les clés.

key_name est le nom de fichier d'une clé.

Création d'un groupe de serveurs vCloud Director 2

Un groupe de serveurs vCloud Director est constitué d'un ou plusieurs serveurs vCloud Director qui partagent une base de données commune et d'autres détails de configuration. Pour créer un groupe de serveurs, vous installez et configurez le logiciel vCloud Director sur le premier membre du groupe. Cette installation et cette configuration sur le premier membre du groupe créent un fichier de réponses que vous utilisez pour configurer les autres membres du groupe.

Tâches préalables à la création d'un groupe de serveurs vCloud Director

IMPORTANT Cette procédure est uniquement destinée à de nouvelles installations. Si vous mettez à niveau une installation de vCloud Director existante, consultez Chapitre 3, « Mise à niveau de vCloud Director », page 41

Avant de commencer à installer et configurer vCloud Director, vous devez effectuer les tâches suivantes.

1. Vérifiez qu'un système vCenter Server pris en charge fonctionne et qu'il est configuré correctement pour être utilisé avec vCloud Director. Pour plus d'informations sur les versions prises en charge et la configuration requise, consultez « Plates-formes prises en charge », page 9
2. Vérifiez qu'un dispositif vShield Manager ou NSX Manager pris en charge fonctionne, qu'il est associé au système vCenter Server et correctement configuré pour être utilisé avec vCloud Director. Pour plus d'informations sur les versions prises en charge, consultez « Plates-formes prises en charge », page 9. Pour plus de détails sur l'installation et la configuration, consultez « Installer et configurer vShield Manager pour une nouvelle installation de vCloud Director », page 25 et « Installer et configurer NSX Manager pour une nouvelle installation de vCloud Director », page 26.
3. Vérifiez que vous disposez au minimum d'une plate-forme de serveur prise en charge pour exécuter le logiciel vCloud Director et que la plate-forme de serveur est configurée avec un volume de mémoire et de stockage adéquat. Pour plus d'informations sur les plates-formes prises en charge et la configuration requise, consultez « Systèmes d'exploitation serveurs pris en charge par vCloud Director », page 10.
   - Chaque membre d'un groupe de serveurs requiert deux adresses IP : une pour prendre en charge une connexion SSL pour le service HTTP et une autre pour le service de proxy de la console.
   - Chaque serveur doit disposer d'un certificat SSL pour chaque adresse IP. Tous les répertoires du chemin d'accès vers les certificats SSL doivent être lisibles par n'importe quel utilisateur. Reportez-vous à « Création de certificats SSL », page 18.
   - Pour le service de transfert, chaque serveur doit monter un système de fichiers en réseau ou un autre volume de stockage partagé dans le répertoire `/opt/vmware/vcloud-director/data/transfer`. L'utilisateur racine doit pouvoir accéder en écriture à ce volume. Reportez-vous à « Résumé des conditions de configuration réseau de vCloud Director », page 13.

- Chaque serveur doit avoir accès à un package de déploiement Microsoft Sysprep. Reportez-vous à « Installer les fichiers Microsoft Sysprep sur les serveurs », page 37.

4 Vérifiez que vous avez créé une base de données vCloud Director et que tous les serveurs dans le groupe peuvent y accéder. Pour obtenir une liste des logiciels de base de données pris en charge, consultez « Bases de données vCloud Director prises en charge », page 10.

   - Vérifiez que vous avez créé un compte de base de données pour l'utilisateur de base de données vCloud Director et que le compte a tous les privilèges de base de données requis. Reportez-vous à « Installation et configuration d'une base de données vCloud Director », page 15.
   - Vérifiez que le service de base de données démarre lorsque le serveur de base de données est redémarré.

5 Vérifiez que tous les serveurs vCloud Director, le serveur de base de données, tous les systèmes vCenter Server et les composants vShield Manager ou NSX Manager associés aux systèmes vCenter Server peuvent résoudre leur nom respectif tel que décrit à la section « Résumé des conditions de configuration réseau de vCloud Director », page 13.

6 Vérifiez que tous les serveurs vCloud Director et le serveur de base de données sont synchronisés par rapport à un serveur d'heure réseau avec les tolérances notées dans « Résumé des conditions de configuration réseau de vCloud Director », page 13.

7 Si vous envisagez d'importer des utilisateurs ou des groupes depuis un service LDAP, vérifiez que chaque serveur vCloud Director peut accéder à ce service.

8 Ouvrez les ports de pare-feu comme il est indiqué dans « Recommandations concernant la sécurité réseau », page 14. Le port 443 doit être ouvert entre vCloud Director et les systèmes vCenter Server.

Ce chapitre aborde les rubriques suivantes :

Installation et configuration du logiciel vCloud Director sur le premier membre d'un groupe de serveurs

Tous les membres d'un vCloud Director partagent la connexion à la base de données et autres détails de configuration que vous spécifiez lors de l'installation et de la configuration du premier membre du groupe. Ces détails sont capturés dans un fichier de réponses que vous devez utiliser lors de l'ajout de membres au groupe.

Le logiciel vCloud Director est distribué en tant que fichier exécutable Linux signé numériquement nommé `vmware-vcloud-director-5.6.0-`*nnnnnn*`.bin`, où *nnnnnn* représente un numéro de build.

Le programme d'installation de vCloud Director vérifie que le serveur cible répond à toutes les conditions requises de la plate-forme et installe le logiciel vCloud Director sur celui-ci. Une fois que le logiciel est installé sur le serveur cible, vous devez exécuter un script qui configure les connexions du serveur au réseau et à la base de données. Ce script crée un fichier de réponses que vous devez utiliser lors de la configuration de membres supplémentaires de ce groupe de serveurs.

Prérequis

- Vérifiez que le serveur cible et le réseau auquel il est connecté remplissent les conditions spécifiées dans « Résumé des conditions de configuration réseau de vCloud Director », page 13.
- Vérifiez que vous possédez les informations d'identification de superutilisateur sur le serveur cible.
- Vérifiez que le serveur cible monte le volume de stockage du service de transfert partagé dans le répertoire `/opt/vmware/vcloud-director/data/transfer`.
- Pour que le programme d'installation vérifie la signature numérique du fichier d'installation, téléchargez et installez la clé publique VMware sur le serveur cible. Si vous avez déjà vérifié la signature numérique du fichier d'installation, il n'est pas nécessaire de la revérifier pendant l'installation. Reportez-vous à « Téléchargement et installation de la clé publique VMware », page 27.

Procédure

1 Connectez-vous au serveur cible en tant qu'utilisateur root.

2 Téléchargez le fichier d'installation sur le serveur cible.

Si vous avez acheté le logiciel sur un CD ou un autre support, copiez le fichier d'installation à un emplacement auquel tous les serveurs cibles peuvent accéder.

3 Vérifiez que la somme de contrôle du téléchargement correspond à celle publiée sur la page de téléchargement.

Les valeurs des sommes de contrôle MD5 and SHA1 sont publiées sur la page de téléchargement. Utilisez l'outil approprié pour vérifier que la somme de contrôle du fichier d'installation téléchargé correspond à celle indiquée sur la page de téléchargement. Une commande Linux de la forme suivante permet d'afficher la somme de contrôle du fichier *installation-file*.

```
[root@cell1 /tmp]# md5sum installation-file
checksum-value installation-file
```

Comparez la valeur *checksum-value* générée par cette commande avec la somme de contrôle MD5 copiée depuis la page de téléchargement.

4 Assurez-vous que le fichier d'installation est exécutable.

Le fichier d'installation nécessite une autorisation d'exécution. Pour vous assurer que cette autorisation est appliquée au fichier d'installation, ouvrez une console, un shell ou une fenêtre de terminal et exécutez la commande Linux suivante, où *fichier-installation* est le chemin d'accès complet au fichier d'installation de vCloud Director.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

5 Dans une console, un shell ou une fenêtre de terminal, exécutez le fichier d'installation.

Pour exécuter le fichier d'installation, tapez son nom de chemin complet, par exemple :

```
[root@cell1 /tmp]# ./installation-file
```

Le fichier comprend un script d'installation et un package RPM intégré.

Remarque Vous ne pouvez pas exécuter le fichier d'installation à partir d'un répertoire dont le chemin d'accès comporte des espaces.

Le programme d'installation affiche un avertissement au format suivant si vous n'avez pas installé la clé publique VMware sur le serveur cible.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

Lorsque le programme d'installation s'exécute, il effectue les opérations suivantes.

a Il vérifie que l'hôte est conforme à toutes les exigences.

b Il vérifie la signature numérique dans le fichier d'installation.

c Il crée l'utilisateur et le groupe `vcloud`.

d Il décompresse le package RPM vCloud Director.

e Il installe le logiciel.

Une fois que le logiciel est installé, le programme d'installation vous invite à exécuter le script de configuration, qui configure les connexions du serveur au réseau et à la base de données.

Suivant

Indiquez si vous voulez exécuter le script de configuration.

- Si vous avez rempli les conditions requises répertoriées dans « Tâches préalables à la création d'un groupe de serveurs vCloud Director », page 29, vous pouvez exécuter maintenant le script de configuration. Tapez **y** et appuyez sur Entrée.
- Si vous n'êtes pas prêt à exécuter le script de configuration maintenant, tapez **n** et appuyez sur Entrée pour quitter le shell.

Pour plus d'informations sur l'exécution du script de configuration, consultez « Configuration des connexions au réseau et à la base de données », page 32.

Configuration des connexions au réseau et à la base de données

Une fois que le logiciel vCloud Director est installé sur le serveur, le programme d'installation vous invite à exécuter un script chargé de configurer les connexions au réseau et à la base de données du serveur.

Vous devez installer le logiciel vCloud Director sur le serveur avant d'exécuter le script de configuration. Le programme d'installation vous invite à exécuter le script une fois l'installation terminée, mais vous pouvez effectuer cette étape plus tard.

Pour exécuter le script plus tard, une fois l'installation du logiciel vCloud Director terminée, ouvrez une session en tant qu'utilisateur racine, ouvrez une console, un shell ou une fenêtre de terminal et tapez :

```
/opt/vmware/vcloud-director/bin/configure
```

Le script de configuration crée les connexions au réseau et à la base de données pour un seul serveur vCloud Director. Il crée également un fichier de réponses dans lequel sont conservées les informations de connexion à la base de données pour les installations de serveur suivantes.

Remarque Après avoir exécuté le script de configuration pour configurer le premier membre du groupe de serveurs, vous devez utiliser l'option `-r` et indiquer le chemin du fichier de réponses afin de configurer les autres membres du groupe. Reportez-vous à « Protection et réutilisation du fichier de réponses », page 35.

Prérequis

- Vérifiez qu'une base de données du type pris en charge est accessible depuis le serveur vCloud Director. Reportez-vous à « Installation et configuration d'une base de données vCloud Director », page 15 et « Configuration matérielle et logicielle requise pour installer vCloud Director », page 9.
- Vous devez disposer des informations suivantes :
  - Emplacement et mot de passe du fichier keystore qui inclut les certificats SSL de ce serveur. Reportez-vous à « Création et importation d'un certificat SSL signé », page 19. Le script de configuration ne s'exécute pas avec une identité disposant de privilèges, par conséquent le fichier keystore et le répertoire dans lequel il est stocké doivent être lisibles par n'importe quel utilisateur.
  - Mot de passe de chaque certificat SSL.
  - Nom d'hôte ou adresse IP du serveur de base de données.

- Nom de la base de données et port de connexion.
- Informations de connexion à la base de données (nom d'utilisateur et mot de passe). Cet utilisateur doit être doté de privilèges de base de données spécifiques. Reportez-vous à « Installation et configuration d'une base de données vCloud Director », page 15.

Procédure

1 Indiquez les adresses IP à utiliser par les services HTTP et de proxy de la console s'exécutant sur cet hôte.

Chaque membre d'un groupe de serveurs requiert deux adresses IP afin qu'il puisse prendre en charge deux connexions SSL différentes : une pour le service HTTP et une autre pour le service de proxy de la console. Pour commencer le processus de configuration, choisissez l'une des adresses IP détectées par le script devant être utilisée par chaque service.

```
Please indicate which IP address available on this machine should be used for the HTTP
service and which IP address should be used for the remote console proxy. The HTTP service
IP address is used for accessing the user interface and the REST API. The remote console
proxy IP address is used for all remote console (VMRC) connections and traffic. Please enter
your choice for the HTTP service IP address: 1: 10.17.118.158 2: 10.17.118.159 Choice
[default=1]:2
Please enter your choice for the remote console proxy IP address 1: 10.17.118.158 Choice
[default=1]:
```

2 Indiquez le chemin d'accès complet au fichier keystore Java.

```
Please enter the path to the Java keystore containing your SSL certificates and private
keys:/opt/keystore/certificates.ks
```

3 Tapez les mots de passe associés au keystore et au certificat.

```
Please enter the password for the keystore: Please enter the private key password for the
'http' SSL certificate: Please enter the private key password for the 'consoleproxy' SSL
certificate:
```

4 Configurez les options de traitement des messages d'audit.

Les services de chaque cellule vCloud Director consignent des messages d'audit dans la base de données vCloud Director qui sont conservés pendant 90 jours. Pour conserver les messages d'audit au-delà de cette période, vous pouvez configurer les services vCloud Director pour qu'ils envoient les messages d'audit à l'utilitaire `syslog` en plus de la base de données vCloud Director.

Option	Action
Pour consigner les messages d'audit à la fois dans `syslog` et dans la base de données vCloud Director.	Tapez le nom d'hôte ou l'adresse IP de `syslog`.
Pour consigner les messages d'audit uniquement dans la base de données vCloud Director	Appuyez sur Entrée.

```
If you would like to enable remote audit logging to a syslog host please enter the hostname
or IP address of the syslog server. Audit logs are stored by vCloud Director for 90 days.
Exporting logs via syslog will enable you to preserve them for as long as necessary. Syslog
host name or IP address [press Enter to skip]:10.150.10.10
```

5 Indiquez le port sur lequel le processus `syslog` doit surveiller le serveur spécifié.

Le port par défaut est 514.

```
What UDP port is the remote syslog server listening on? The standard syslog port is 514.
[default=514]: Using default value "514" for syslog port.
```

6 Indiquez le type de base de données ou appuyez sur Entrée pour accepter la valeur par défaut.

```
The following database types are supported: 1. Oracle 2. Microsoft SQL Server Enter the
database type [default=1]: Using default value "1" for database type.
```

7 Indiquez les informations de connexion à la base de données.

Les informations requises par le script dépendent du type de base de données que vous choisissez. L'exemple suivant présente les invites associées à la base de données Oracle. Les invites des autres types de bases de données sont similaires.

a Tapez le nom d'hôte ou l'adresse IP du serveur de base de données.

```
Enter the host (or IP address) for the database:10.150.10.78
```

b Indiquez le port de la base de données ou appuyez sur Entrée pour accepter la valeur par défaut.

```
Enter the database port [default=1521]: Using default value "1521" for port.
```

c Tapez le nom du service de la base de données.

```
Enter the database service name [default=oracle]:orcl.example.com
```

Si vous appuyez sur Entrée, le script de configuration utilise une valeur par défaut susceptible de ne pas être adaptée à certaines installations. Pour plus d'informations sur la recherche du nom du service de base de données d'une base de données Oracle, consultez « Configuration d'une base de données Oracle », page 16.

d Tapez le nom d'utilisateur et le mot de passe associés à la base de données.

```
Enter the database username:vcloud
Enter the database password:
```

Le script valide les informations que vous avez fournies, puis exécute trois autres étapes.

1 Il initialise la base de données et connecte le serveur à celle-ci.

2 Il propose de lancer les services vCloud Director résidant sur cet hôte.

3 Il affiche l'URL vous permettant de vous connecter à l'assistant de configuration après le démarrage du service vCloud Director.

Ce fragment montre une fin type du script.

```
Connecting to the database: jdbc:oracle:thin:vcloud/vcloud@10.150.10.78:1521/vcloud
...........
Database configuration complete. Once the vCloud Director server has been started you will be
able to access the first-time setup wizard at this URL: http://vcloud.example.com Would you like
to start the vCloud Director service now? If you choose not to start it now, you can manually
start it at any time using this command: service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment). The service was started; it may
be several minutes before it is ready for use. Please check the logs for complete details.
vCloud Director configuration is now complete. Exiting...
```

Suivant

Remarque Les informations relatives à la connexion à la base de données ainsi que d'autres réponses réutilisables que vous avez fournies lors de la configuration sont conservées dans un fichier qui se trouve dans le répertoire `/opt/vmware/vcloud-director/etc/responses.properties` sur ce serveur. Ce fichier contient des informations importantes que vous devez réutiliser lorsque vous ajoutez des serveurs à un groupe de serveurs. Conservez ce fichier dans un endroit sûr et faites en sorte qu'il soit disponible uniquement lorsque cela est nécessaire.

Pour ajouter des serveurs à ce groupe, consultez « Installer le logiciel vCloud Director sur un membre supplémentaire d'un groupe de serveurs », page 36.

Une fois que les services vCloud Director s'exécutent sur tous les serveurs, vous pouvez ouvrir l'assistant de configuration à partir de l'URL qui s'affiche lorsque le script se termine. Reportez-vous à Chapitre 4, « Configuration de vCloud Director », page 55.

Protection et réutilisation du fichier de réponses

Les informations de connexion au réseau et à la base de données que vous fournissez lorsque vous configurez le premier serveur vCloud Director sont sauvegardées dans un fichier de réponses. Ce fichier contient des informations importantes que vous devez réutiliser lorsque vous ajoutez des serveurs à un groupe de serveurs. Conservez ce fichier dans un endroit sûr et faites en sorte qu'il soit disponible uniquement lorsque cela est nécessaire.

Le fichier de réponses est créé sur le premier serveur pour lequel vous configurez les connexions au réseau et à la base de données. Il est stocké à `/opt/vmware/vcloud-director/etc/responses.properties`. Lorsque vous ajoutez des serveurs au groupe, vous devez utiliser une copie du fichier de réponses pour fournir les paramètres de configuration qui seront utilisés par tous les serveurs.

Procédure

1 Protégez le fichier de réponses.

   Enregistrez une copie du fichier dans un endroit sûr. Limitez l'accès au fichier et assurez-vous qu'il est sauvegardé dans un endroit sûr. Lorsque vous sauvegardez le fichier, évitez de le transférer sous forme de texte clair sur un réseau public.

2 Réutilisez le fichier de réponses.

   a Copiez le fichier à un emplacement accessible au serveur que vous êtes prêt à configurer.

   Remarque Vous devez installer le logiciel vCloud Director sur un serveur avant de pouvoir réutiliser le fichier de réponses pour le configurer. Tous les répertoires du chemin d'accès vers le fichier de réponses doivent être lisibles par l'utilisateur `vcloud.vcloud`, comme illustré dans cet exemple.

   ```
   [root@cell1 /tmp]# ls -l responses.properties
   -rw------- 1 vcloud vcloud 418 Jun 8 13:42 responses.properties
   ```

   Le programme d'installation crée cet utilisateur et ce groupe.

   b Exécutez le script de configuration, en utilisant l'option `-r` et en spécifiant le chemin d'accès au fichier de réponses.

   Connectez-vous comme utilisateur racine, ouvrez une console, un shell ou une fenêtre de terminal et saisissez :

   ```
   [root@cell1 /tmp]# /opt/vmware/vcloud-director/bin/configure -r /path-to-response-file
   ```

Suivant

Une fois que vous avez configuré les serveurs supplémentaires, supprimez la copie du fichier de réponses que vous avez utilisé pour cela.

Installer le logiciel vCloud Director sur un membre supplémentaire d'un groupe de serveurs

Vous pouvez ajouter des serveurs à un groupe de serveurs vCloud Director à tout moment. Du fait que tous les serveurs d'un groupe de serveurs doivent être configurés avec les mêmes informations de connexion à la base de données, vous devez utiliser le fichier de réponses créé lorsque vous avez configuré le premier membre du groupe afin de fournir ces informations lors de la configuration des autres membres.

Prérequis

- Vérifiez que vous pouvez accéder au fichier de réponses créé lorsque vous avez installé et configuré le premier membre de ce groupe de serveurs. Reportez-vous à « Protection et réutilisation du fichier de réponses », page 35.
- Vérifiez que la base de données vCloud Director est accessible depuis le serveur.
- Vérifiez que les certificats SSL que vous avez créés pour le serveur sont installés dans un emplacement accessible au programme d'installation. Reportez-vous à « Création et importation d'un certificat SSL signé », page 19. Le script de configuration ne s'exécute pas avec une identité disposant de privilèges, par conséquent le fichier keystore et le chemin dans lequel il est stocké doivent être lisibles par n'importe quel utilisateur. L'utilisation du même chemin de keystore (par exemple, `/tmp/certificates.ks`) sur tous les membres d'un groupe de serveurs simplifie l'installation.
- Vous devez disposer des informations suivantes :
  - Mot de passe du fichier de keystore qui contient les certificats SSL du serveur.
  - Mot de passe de chaque certificat SSL.

Procédure

1. Connectez-vous au serveur cible en tant qu'utilisateur root.
2. Téléchargez le fichier d'installation sur le serveur cible.

   Si vous avez acheté le logiciel sur un CD ou un autre support, copiez le fichier d'installation à un emplacement auquel tous les serveurs cibles peuvent accéder.
3. Assurez-vous que le fichier d'installation est exécutable.

   Le fichier d'installation nécessite une autorisation d'exécution. Pour vous assurer que cette autorisation est appliquée au fichier d'installation, ouvrez une console, un shell ou une fenêtre de terminal et exécutez la commande Linux suivante, où *fichier-installation* est le chemin d'accès complet au fichier d'installation de vCloud Director.

   ```
   [root@cell1 /tmp]# chmod u+x installation-file
   ```
4. Copiez le fichier de réponses à un emplacement accessible à ce serveur.

   Tous les répertoires du chemin d'accès vers le fichier de réponses doivent être lisibles par n'importe quel utilisateur.
5. Dans une console, un shell ou une fenêtre de terminal, exécutez le fichier d'installation en utilisant l'option `-r` et en spécifiant le chemin d'accès du fichier de réponses.

   Pour exécuter le fichier d'installation, tapez son nom de chemin complet, par exemple :

   ```
   [root@cell1 /tmp]# ./installation-file -r /path-to-response-file
   ```

Le fichier comprend un script d'installation et un package RPM intégré.

Remarque Vous ne pouvez pas exécuter le fichier d'installation à partir d'un répertoire dont le chemin d'accès comporte des espaces.

Le programme d'installation affiche un avertissement au format suivant si vous n'avez pas installé la clé publique VMware sur le serveur cible.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

Lorsque le programme d'installation s'exécute avec l'option `-r`, il effectue les opérations suivantes.

a Il vérifie que l'hôte est conforme à toutes les exigences.

b Il vérifie la signature numérique dans le fichier d'installation.

c Il crée l'utilisateur et le groupe `vcloud`.

d Il décompresse le package RPM vCloud Director.

e Il installe le logiciel.

f Il copie le fichier de réponses à un emplacement lisible par vcloud.vcloud.

g Il exécute le script de configuration en utilisant le fichier de réponses comme entrée.

Lorsque le script de configuration s'exécute, il recherche les certificats dans le chemin enregistré dans le fichier de réponses (par exemple `/tmp/certificates.ks`), puis vous invite à indiquer les mots de passe de keystore et de certificat. Si le script de configuration ne trouve pas de certificats valides dans le chemin d'accès enregistré dans le fichier de réponses, il vous invite à indiquer le chemin d'accès aux certificats.

6 (Facultatif) Répétez cette procédure pour ajouter d'autres serveurs à ce groupe de serveurs.

Suivant

Si votre cloud doit prendre en charge la personnalisation des invités pour certains systèmes d'exploitation Microsoft plus anciens, installez les fichiers Sysprep sur tous les membres du groupe de serveurs. Reportez-vous à « Installer les fichiers Microsoft Sysprep sur les serveurs », page 37.

Une fois que le script de configuration a terminé et que les services vCloud Director sont exécutés sur tous les serveurs, vous pouvez ouvrir l'assistant de configuration à l'aide de l'URL qui apparaît alors. Reportez-vous à Chapitre 4, « Configuration de vCloud Director », page 55.

Installer les fichiers Microsoft Sysprep sur les serveurs

Pour pouvoir vCloud Director exécuter une personnalisation client sur les machines virtuelles disposant de certains anciens systèmes d'exploitation client Windows, vous devez installer les fichiers Microsoft Sysprep appropriés sur chaque membre du groupe de serveurs.

Les fichiers Sysprep sont nécessaires uniquement pour certains anciens systèmes d'exploitation Microsoft. Si votre cloud n'a pas besoin de prendre en charge la personnalisation client de ces systèmes d'exploitation, il n'est pas nécessaire d'installer les fichiers Sysprep.

Pour installer les fichiers binaires Sysprep, vous les copiez vers un emplacement donné sur le serveur. Vous devez copier les fichiers vers chaque membre du groupe de serveurs.

Prérequis

Vérifiez que vous avez accès aux fichiers binaires Sysprep 32 bits et 64 bits pour Windows 2003 et Windows XP.

Procédure

1 Connectez-vous au serveur cible en tant qu'utilisateur root.

2 Accédez au répertoire `$VCLOUD_HOME/guestcustomization/default/windows`.

```
[root@cell1 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

3 Créez le répertoire `sysprep`.

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep
```

4 Pour chaque système d'exploitation client qui nécessite les fichiers binaires Sysprep, créez le sous-répertoire `$VCLOUD_HOME/guestcustomization/default/windows/sysprep`.

Les noms de sous-répertoire sont spécifiques à un système d'exploitation client.

Tableau 2-1. Affectations de sous-répertoires pour les fichiers Sysprep

Systèmes d'exploitation clients	Sous-répertoire à créer sous $VCLOUD_HOME/guestcustomization/default/windows/sysprep.
Windows 2003 (32 bits)	svr2003
Windows 2003 (64 bits)	svr2003-64
Windows XP (32 bits)	xp
Windows XP (64 bits)	xp-64

Par exemple, pour créer un sous-répertoire pour y placer les fichiers binaires Sysprep de Windows XP, utilisez la commande Linux suivante.

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep/xp
```

5 Copiez les fichiers binaires Sysprep vers l'emplacement approprié sur chaque serveur vCloud Director du groupe de serveurs.

6 Vérifiez que les fichiers Sysprep peuvent être lus par l'utilisateur `vcloud.vcloud`.

Utilisez la commande `chown` à cet effet.

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLOUD_HOME/guestcustomization
```

Une fois les fichiers Sysprep copiés vers tous les membres du groupe de serveurs, vous pouvez exécuter des opérations de personnalisation client sur les machines virtuelles de votre cloud. Il est inutile de redémarrer vCloud Director après la copie des fichiers Sysprep.

Démarrage ou arrêt des services vCloud Director

Une fois que vous avez effectué l'installation et la configuration des connexions à la base de données sur un serveur, vous pouvez démarrer les services vCloud Director sur ce serveur ou les arrêter s'ils sont exécutés.

Le script de configuration vous invite à démarrer les services vCloud Director. Vous pouvez laisser le script démarrer automatiquement ces services ou vous pouvez les démarrer vous-même ultérieurement. Pour effectuer et initialiser l'installation, ces services doivent être exécutés.

Les services vCloud Director démarrent à chaque fois que vous redémarrez un serveur.

IMPORTANT Si vous arrêtez les services vCloud Director pour mettre à niveau le logiciel vCloud Director, vous devez utiliser l'outil de gestion des cellules pour mettre en veille la cellule avant d'arrêter les services. Reportez-vous à « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 44.

Procédure

1 Connectez-vous au serveur cible en tant qu'utilisateur root.

2 Démarrez ou arrêtez les services.

Option	Action
Démarrer les services	Ouvrez une console, un shell ou une fenêtre de terminal et exécutez la commande suivante. `service vmware-vcd start`
Arrêter les services lorsque la cellule est en cours d'utilisation	Utilisez l'outil de gestion des cellules.
Arrêter les services lorsque la cellule n'est pas en cours d'utilisation	Ouvrez une console, un shell ou une fenêtre de terminal et exécutez la commande suivante. `service vmware-vcd stop`

Désinstallation du logiciel vCloud Director

Utilisez la commande Linux `rpm` pour désinstaller le logiciel vCloud Director d'un serveur individuel.

Procédure

1 Connectez-vous au serveur cible en tant qu'utilisateur root.

2 Démontez le stockage du service de transfert, en général monté à `/opt/vmware/vcloud-director/data/transfer`.

3 Ouvrez une console, un shell ou une fenêtre de terminal et exécutez la commande `rpm`.

```
rpm -e vmware-vcloud-director
```

Mise à niveau de vCloud Director 3

Pour mettre à niveau vCloud Director vers une nouvelle version, installez la nouvelle version sur chaque serveur du groupe de serveurs vCloud Director, mettez la base de données vCloud Director à niveau, puis redémarrez les services vCloud Director. Vous devez également mettre à niveau les composants vSphere qui prennent en charge vCloud Director, y compris chacun des dispositifs vShield Manager ou NSX Manager associés à chaque système vCenter Server dans le groupe de serveurs vCloud Director.

Après avoir mis à niveau un serveur vCloud Director, vous devez également mettre à niveau sa base de données vCloud Director. La base de données détient des informations relatives à l'état d'exécution du serveur, notamment l'état de toutes les tâches vCloud Director qu'il exécute. Pour vous assurer qu'il ne reste aucune information de tâche non valide dans la base de données après la mise à niveau, vous devez vérifier qu'aucune tâche n'est active sur le serveur avant de commencer la mise à niveau.

IMPORTANT La procédure de mise à niveau implique la mise à niveau de vCloud Director, de chaque système vCenter Server associé (ainsi que de son dispositif vShield Manager ou NSX Manager) et de tous les hôtes. Vous devez empêcher les utilisateurs d'accéder à vCloud Director jusqu'à ce que la mise à niveau du dispositif vShield Manager ou NSX Manager associé soit complète.

La mise à niveau préserve les éléments suivants :

- les fichiers de propriétés locaux et globaux sont copiés vers la nouvelle installation ;
- les fichiers sysprep Microsoft utilisés pour la personnalisation des invités sont copiés vers la nouvelle installation ;

Si vous utilisez un équilibreur de charge pour distribuer les demandes des clients aux membres du groupe de serveurs vCloud Director, vous pouvez mettre à niveau un sous-ensemble du groupe de serveurs en maintenant les services existants disponibles sur les autres. Si ce n'est pas le cas, prévoyez un temps suffisant de mise hors service de vCloud Director pour mettre à niveau la base de données et au moins un serveur. Vous devez également mettre à niveau des systèmes vCenter Server enregistrés s'ils n'exécutent pas une version compatible du logiciel vCenter. La mise à niveau des systèmes vCenter Server et des hôtes ESXi peut subir des temps morts supplémentaires vCloud Director, car les machines virtuelles sont inaccessibles lorsque leurs hôtes ou leurs systèmes vCenter Server sont mis à niveau.

Les certificats SSL doivent inclure une extension Autre nom de l'objet X.509

À partir de cette version, les certificats SSL utilisés par vCloud Director doivent inclure à la fois un nom unique X.500 une extension Autre nom de l'objet X.509. Dans les versions précédentes, la valeur Autre nom de l'objet n'était pas vérifiée lors de l'établissement d'une liaison SSL. Dans cette version, si vos certificats existants n'incluent pas une extension Autre nom de l'objet X.509, l'établissement de la liaison SSL échoue et les clients ne peuvent pas se connecter à vCloud Director.

Les certificats SSL incluant une extension Autre nom de l'objet X.509 sont compatibles avec toutes les versions antérieures de vCloud Director. Il est conseillé de créer de nouveaux certificats et de les installer dans votre version de vCloud Director existante avant de démarrer la mise à niveau. De cette manière, vous pouvez vous assurer du bon fonctionnement de la connexion SSL avec ces nouveaux certificats avant de commencer la mise à niveau.

« Création de certificats SSL », page 18 présente des informations détaillées sur la création et l'importation de certificats signés et auto-signés. « Génération de certificats SSL auto-signés », page 65 et « Remplacement des certificats SSL », page 64 expliquent comment utiliser l'outil `cell-management-tool` pour créer de nouveaux certificats et remplacer les anciens.

Mise à niveau d'un groupe de serveurs vCloud Director

1. Désactivez l'accès des utilisateurs à vCloud Director. Vous pouvez également afficher un message de maintenance lorsque la mise à niveau est en cours. Reportez-vous à « Affichage du message de maintenance lors d'une mise à niveau », page 43.
2. Utilisez l'outil de gestion des cellules pour mettre en veille toutes les cellules du groupe de serveur et arrêter les services vCloud Director sur chaque serveur. Reportez-vous à « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 44.
3. Mettez à niveau le logiciel vCloud Director sur tous les membres du groupe de serveurs. Reportez-vous à « Mise à niveau du logiciel vCloud Director sur un membre d'un groupe de serveurs », page 45. Vous pouvez mettre à niveau les serveurs de manière individuelle ou en parallèle. Dans tous les cas, vous ne devez pas redémarrer les services vCloud Director sur aucun des membres mis à niveau du groupe tant que vous n'avez pas mis la base de données vCloud Director à niveau.
4. Mettez la base de données vCloud Director à niveau. Reportez-vous à « Mise à niveau de la base de données vCloud Director », page 48.
5. Redémarrez vCloud Director sur les serveurs mis à niveau. Reportez-vous à « Démarrage ou arrêt des services vCloud Director », page 38.
6. Mettez à niveau chaque dispositif vShield Manager ou NSX Manager associé. Toutes les installations de dispositifs vShield Manager ou NSX Manager enregistrées sur ce groupe de serveurs doivent être mises à niveau vers une version du logiciel vShield Manager ou NSX Manager compatible avec la version de vCloud Director installée par la mise à niveau. Si le programme de mise à niveau détecte une version incompatible de vShield Manager ou NSX Manager, la mise à niveau n'est pas autorisée. Vous devez effectuer la mise à niveau vers la dernière version de vShield Manager ou NSX Manager, comme indiqué dans« Plates-formes prises en charge », page 9, pour utiliser les fonctions de mise en réseau introduites dans cette version de vCloud Director. Reportez-vous à « Mettre à niveau le dispositif vShield Manager ou NSX Manager qui est associé à un système vCenter Server connecté », page 50.
7. Activez l'accès des utilisateurs à vCloud Director.
8. Mettez à niveau tous les hôtes et systèmes vCenter Server associés. Reportez-vous à « Mettre à niveau les systèmes vCenter Server, les hôtes et les dispositifs vShield Edge », page 51. Tous les systèmes vCenter Server enregistrés dans ce groupe de serveurs doivent être mis à niveau vers une version du logiciel vCenter Server compatible avec la version de vCloud Director installée par la mise à niveau. Des systèmes vCenter Server incompatibles deviennent inaccessibles à vCloud Director une fois la mise à niveau terminée. Reportez-vous à « Plates-formes prises en charge », page 9.

Utilisation d'un équilibreur de charge pour réduire la durée de mise hors service des services

Si vous utilisez un équilibreur de charge ou un autre outil capable de forcer la redirection des demandes vers des serveurs spécifiques, vous pouvez mettre à niveau un sous-ensemble du groupe du serveurs tout en maintenant les services existants disponibles sur le sous-ensemble restant. Cette approche permet de réduire la durée d'inactivité du service vCloud Director au temps nécessaire à la mise à niveau de la base de

données vCloud Director. Les utilisateurs peuvent subir des baisses de performances pendant la mise à niveau, mais les tâches en cours continuent d'être exécutées tant qu'un sous-ensemble du groupe de serveurs est opérationnel. Les sessions de console peuvent être interrompues, mais vous pouvez les redémarrer.

1 Utilisez l'équilibreur de charge pour rediriger les demandes vCloud Director vers un sous-ensemble de serveurs du groupe. Suivez les procédures recommandées dans la documentation fournie avec votre équilibreur de charge.

2 Utilisez l'outil de gestion des cellules pour mettre en veille toutes les cellules ne traitant plus de demandes et arrêtez les services vCloud Director sur ces serveurs.

Remarque Les sessions de console acheminées via le proxy de console d'un serveur sont interrompues lorsque le serveur s'arrête. Les clients peuvent actualiser la fenêtre de console pour la reprise.

Reportez-vous à « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 44.

3 Mettez à niveau le logiciel vCloud Director sur tous les membres du groupe de serveurs sur lesquels vous avez arrêté vCloud Director, mais ne redémarrez pas les services. Reportez-vous à « Mise à niveau du logiciel vCloud Director sur un membre d'un groupe de serveurs », page 45.

4 Utilisez l'outil de gestion des cellules pour mettre en veille toutes les cellules ne traitant plus de demandes et arrêtez les services vCloud Director sur ces serveurs.

5 Mettez la base de données vCloud Director à niveau. Reportez-vous à « Mise à niveau de la base de données vCloud Director », page 48.

6 Redémarrez vCloud Director sur les serveurs mis à niveau. Reportez-vous à « Démarrage ou arrêt des services vCloud Director », page 38.

7 Mettez à niveau chaque dispositif vShield Manager ou NSX Manager associé. Reportez-vous à « Mettre à niveau le dispositif vShield Manager ou NSX Manager qui est associé à un système vCenter Server connecté », page 50.

8 Mettez à niveau tous les hôtes et les systèmes vCenter Server associés. Reportez-vous à « Mettre à niveau les systèmes vCenter Server, les hôtes et les dispositifs vShield Edge », page 51.

9 Redirigez les demandes vCloud Director vers les serveurs mis à niveau à l'aide de l'équilibreur de charge.

10 Mettez à niveau le logiciel vCloud Director sur les serveurs restants du groupe, puis redémarrez vCloud Director sur ces serveurs une fois la mise à niveau terminée. Reportez-vous à « Mise à niveau du logiciel vCloud Director sur un membre d'un groupe de serveurs », page 45.

Affichage du message de maintenance lors d'une mise à niveau

Si vous anticipez un processus de mise à niveau assez long et que vous voulez que le système affiche un message de maintenance lorsque la mise à niveau est en cours, vérifiez qu'au moins une cellule reste accessible lorsque les autres sont mises à niveau. Exécutez la commande `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` sur cette cellule pour activer le message de maintenance de la cellule.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
```

Lorsque vous êtes prêt à remettre en service une cellule mise à niveau, exécutez la commande suivante sur la cellule pour désactiver le message de maintenance.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# service vmware-vcd restart
```

Ce chapitre aborde les rubriques suivantes :

Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur

Avant de mettre à niveau un serveur vCloud Director, utilisez l'outil de gestion des cellules pour mettre en veille et arrêter les services vCloud Director s'exécutant sur la cellule de ce serveur.

vCloud Director crée un objet de tâche chargé d'assurer le suivi et la gestion de chaque opération asynchrone qu'un utilisateur demande. Les informations sur les tâches en cours et récemment terminées sont conservées dans la base de données vCloud Director. Étant donné qu'une mise à niveau de la base de données invalide toutes les informations sur les tâches, vous devez vérifier qu'aucune tâche n'est en cours exécution lorsque vous lancez le processus de mise à niveau.

L'outil de gestion des cellules permet de suspendre le planificateur des tâches pour empêcher le démarrage de nouvelles tâches et de vérifier l'état des tâches actives. Vous pouvez attendre que les tâches se terminent ou ouvrir une session sur vCloud Director en tant qu'administrateur système et annuler les tâches. Reportez-vous à Chapitre 5, « Référence de l'outil de gestion des cellules », page 59. Lorsque plus aucune tâche ne s'exécute, arrêtez les services vCloud Director à l'aide de l'outil de gestion des cellules.

Prérequis

- Vérifiez que vous possédez les informations d'identification de superutilisateur sur le serveur cible.
- Vérifiez que vous possédez des informations de connexion d'administrateur système vCloud Director.
- Si cette cellule sera accessible aux clients vCloud Director lors de sa mise à niveau, utilisez la commande `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` pour activer le message de maintenance de cellule.

  ```
  [root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
  ```

  Cette commande provoque la réponse de la cellule à toutes les demandes avec un message de maintenance. Si vous utilisez un équilibreur de charge ou un outil similaire pour rendre la cellulle inaccessible lors de la mise à niveau, il est inutile d'activer le message de maintenance de cellule.

Procédure

1 Connectez-vous au serveur cible en tant qu'utilisateur root.

2 Utilisez-le pour arrêter en douceur la cellule.

a Affichez l'état actuel des tâches.

La commande `cell-management-tool` suivante fournit les informations d'identification d'administrateur système et indique le nombre de tâches en cours.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3 Is Active = true
```

b Arrêtez le planificateur des tâches pour mettre en veille la cellule.

Utilisez une commande `cell-management-tool` dont le format est le suivant.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --quiesce true
```

Cette commande empêche le démarrage de nouvelles tâches. Les tâches existantes continuent à s'exécuter jusqu'à leur terme ou sont annulées. Pour annuler une tâche, utilisez la console Web de vCloud Director ou l'API REST.

c Lorsque la valeur `Job count` indique `0` et que la valeur `Is Active` indique `false`, vous pouvez arrêter la cellule en toute sécurité.

Utilisez une commande `cell-management-tool` dont le format est le suivant.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --shutdown
```

Remarque Vous pouvez fournir le mot de passe de l'administrateur système vCloud Director dans la ligne de commande `cell-management-tool`, mais il est préférable de l'omettre pour des raisons de sécurité. Dans ce cas, `cell-management-tool` demande le mot de passe qui ne s'affiche pas lorsque vous le tapez.

Les sessions de console acheminées via le proxy de console d'un serveur sont interrompues lorsque le serveur s'arrête. Si d'autres membres du groupe de serveurs sont toujours actifs, les clients peuvent actualiser la fenêtre de console à récupérer.

Suivant

Lorsque l'outil de gestion de cellule arrête les services vCloud Director sur ce serveur, vous pouvez mettre à niveau le logiciel vCloud Director du serveur ou exécuter une autre opération de maintenance que nécessite le serveur.

Mise à niveau du logiciel vCloud Director sur un membre d'un groupe de serveurs

Le programme d'installation de vCloud Director vérifie que le serveur cible répond à toutes les conditions de mise à niveau requises et met à niveau le logiciel vCloud Director sur le serveur.

Le logiciel vCloud Director est distribué en tant que fichier exécutable Linux nommé `vmware-vcloud-director-5.6.0-`*nnnnnn*`.bin`, où *nnnnnn* représente un numéro de build. Une fois que la mise à niveau est installée sur un membre d'un groupe de serveurs, vous devez exécuter un outil qui met à niveau la base de données vCloud Director que le groupe utilise avant de redémarrer les services vCloud Director sur le serveur mis à niveau.

Prérequis

- Vérifiez que vous possédez les informations d'identification de superutilisateur sur le serveur cible.

- Pour que le programme d'installation vérifie la signature numérique du fichier d'installation, téléchargez et installez la clé publique VMware sur le serveur cible. Si vous avez déjà vérifié la signature numérique du fichier d'installation, il n'est pas nécessaire de la revérifier pendant l'installation. Reportez-vous à « Téléchargement et installation de la clé publique VMware », page 27.
- Créez de nouveaux certificats SSL pour le serveur cible. Reportez-vous à « Les certificats SSL doivent inclure une extension Autre nom de l'objet X.509 », page 41.
- Utilisez l'outil de gestion des cellules pour mettre en veille et arrêter les services vCloud Director sur la cellule du serveur.
- Vérifiez que vous disposez d'une clé de licence valide pour utiliser la version du logiciel vCloud Director vers laquelle vous effectuez la mise à niveau.

Procédure

1 Connectez-vous au serveur cible en tant qu'utilisateur root.

2 Téléchargez le fichier d'installation sur le serveur cible.

Si vous avez acheté le logiciel sur un CD ou un autre support, copiez le fichier d'installation à un emplacement auquel tous les serveurs cibles peuvent accéder.

3 Vérifiez que la somme de contrôle du téléchargement correspond à celle publiée sur la page de téléchargement.

Les valeurs des sommes de contrôle MD5 and SHA1 sont publiées sur la page de téléchargement. Utilisez l'outil approprié pour vérifier que la somme de contrôle du fichier d'installation téléchargé correspond à celle indiquée sur la page de téléchargement. Une commande Linux de la forme suivante permet d'afficher la somme de contrôle du fichier *installation-file*.

```
[root@cell1 /tmp]# md5sum installation-file
checksum-value installation-file
```

Comparez la valeur *checksum-value* générée par cette commande avec la somme de contrôle MD5 copiée depuis la page de téléchargement.

4 Assurez-vous que le fichier d'installation est exécutable.

Le fichier d'installation nécessite une autorisation d'exécution. Pour vous assurer que cette autorisation est appliquée au fichier d'installation, ouvrez une console, un shell ou une fenêtre de terminal et exécutez la commande Linux suivante, où *fichier-installation* est le chemin d'accès complet au fichier d'installation de vCloud Director.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

5 Utilisez l'outil de gestion des cellules pour mettre en veille et arrêter les services vCloud Director sur le serveur.

Reportez-vous à « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 44.

6 Dans une console, un shell ou une fenêtre de terminal, exécutez le fichier d'installation.

Pour exécuter le fichier d'installation, tapez son chemin d'accès complet, par exemple `./fichier-installation`. Le fichier comprend un script d'installation et un package RPM intégré.

Remarque Vous ne pouvez pas exécuter le fichier d'installation à partir d'un répertoire dont le chemin d'accès comporte des espaces.

Si le programme d'installation détecte une version de vCloud Director installée sur ce serveur qui est égale ou ultérieure à la version du logiciel dans le fichier d'installation, il affiche alors un message d'erreur et se ferme. Si ce n'est pas le cas, il vous invite à confirmer que vous êtes prêt à mettre à niveau ce serveur.

```
Checking architecture...done
Checking for a supported Linux distribution...done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
An older version of VMware vCloud Director has been detected
```

7 Répondez à l'invite de mise à niveau.

Option	Action
Continuer la mise à niveau.	Tapez **y**.
Quittez le shell sans apporter de modifications à la base de données actuelle.	Tapez **n**.

Après avoir confirmé que vous êtes prêt à mettre à niveau le serveur, le programme d'installation vérifie que l'hôte répond à toutes les conditions, déballe le package RPM vCloud Director, arrête les services vCloud Director sur le serveur et met à niveau le logiciel vCloud Director installé.

```
Do you wish to proceed with the upgrade? (y/n)? y
Extracting vmware-vcloud-director ......done
Upgrading VMware vCloud Director...
Installing the VMware vCloud Director
Preparing...                ##################################################
vmware-vcloud-director      ##################################################
Migrating settings and files from previous release...done
Migrating in-progress file transfers to /opt/vmware/vcloud-director/data/transfer...done
Uninstalling previous release...done
```

Le programme d'installation affiche un avertissement au format suivant si vous n'avez pas installé la clé publique VMware sur le serveur cible.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

Le programme d'installation affiche un avertissement au format suivant lorsqu'il modifie le fichier `global.properties` existant sur le serveur cible.

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-
director/etc/global.properties.rpmnew
```

La plupart des mises à niveau requièrent ce type de modification et affichent cet avertissement. Si vous avez effectué des modifications au fichier `global.properties` existant, vous pouvez les récupérer à partir de `global.properties.rpmnew`.

8 (Facultatif) Mettez à jour les propriétés de journalisation.

À la suite d'une mise à niveau, de nouvelles propriétés de journalisation sont écrites dans le fichier `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`.

Option	Action
Si vous n'avez pas modifié les propriétés de journalisation existantes	Copiez ce fichier dans `/opt/vmware/vcloud-director/etc/log4j.properties`.
Si vous avez modifié les propriétés de journalisation	Fusionnez le fichier `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` avec le fichier `/opt/vmware/vcloud-director/etc/log4j.properties` existant. En fusionnant ces fichiers vous conservez vos modifications.

Lorsque la mise à niveau du logiciel vCloud Director est terminée, le programme d'installation affiche un message indiquant l'emplacement de stockage des anciens fichiers de configuration, puis il vous rappelle d'exécuter l'outil de mise à niveau de la base de données.

Suivant

- Si vous ne l'avez pas déjà fait, mettez à niveau la base de données vCloud Director que ce serveur utilise.
- Si vous avez déjà mis à niveau la base de données vCloud Director que ce groupe de serveurs utilise, vous pouvez redémarrer le serveur mis à niveau. Reportez-vous à « Démarrage ou arrêt des services vCloud Director », page 38.

Mise à niveau de la base de données vCloud Director

Après avoir mis à niveau un serveur dans le groupe de serveurs vCloud Director, vous devez mettre à niveau la base de données vCloud Director du groupe avant de redémarrer les services vCloud Director sur le serveur.

Tous les serveurs dans un groupe de serveurs vCloud Director partagent la même base de données. Par conséquent, quel que soit le nombre de serveurs que vous mettez à niveau, il n'est nécessaire de mettre à niveau qu'une seule fois la base de données. Une fois la base de données mise à niveau, les serveurs vCloud Director ne peuvent pas s'y connecter tant qu'ils ne sont pas mis à niveau, eux aussi.

Prérequis

IMPORTANT Sauvegardez la base de données existante avant de la mettre à niveau. Suivez pour cela la procédure recommandée par le fournisseur du logiciel de base de données.

Vérifiez que toutes les cellules de vCloud Director sont inactives. Consultez « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 44

Procédure

1 Ouvrez une console, un shell ou une fenêtre de terminal et tapez la commande suivante pour exécuter le script de mise à niveau de la base de données.

```
/opt/vmware/vcloud-director/bin/upgrade
```

IMPORTANT Si le script de mise à niveau de la base de données détecte qu'une version incompatible de vShield Manager ou de NSX Manager est enregistrée dans cette installation de vCloud Director, il affiche un message d'avertissement et annule la mise à niveau.

```
One or more vShield Manager servers registered to this vCloud Director installation are not supported by the version of vCloud Director you are upgrading to. Upgrade canceled, please follow the procedures in the vShield Manager Upgrade Guide to upgrade those unsupported vShield Manager servers.
```

2 Répondez aux invites de mise à niveau de la base de données.

a Confirmez que vous voulez poursuivre la mise à jour de la base de données.

```
Welcome to the vCloud Director upgrade utility This product is intended for use only by service providers under the terms and conditions of the VMware Service Provider Partner (VSPP) Program. If you are a member of the VSPP Program, please locate your license key before proceeding. If you are not a member of this program, do not proceed with this upgrade. Upgrading without a proper key will invalidate your support contract. This utility will apply several updates to the database. Please ensure you have created a backup of your database prior to continuing. Do you wish to upgrade the product now? [Y/N]:
```

Effectuez l'une des opérations suivantes :

Option	Action
Continuer la mise à niveau.	Tapez **y**.
Quittez le shell sans apporter de modifications à la base de données vCloud Director actuelle.	Tapez **n**.

b (Facultatif) Attendez que les cellules deviennent inactives, si nécessaire.

Si l'outil de mise à niveau de la base de données détecte que des cellules sont toujours actives, il demande si vous voulez continuer la mise à niveau ou quitter.

```
Found active cell. Name: "cell-01", IP Address: 10.150.151.190, Identifier: a2eb...
Do you wish to upgrade the database while cells are still active? [Y/N]
```

Si vous voyez ce message, tapez `n` pour quitter et revenir au shell, patientez cinq minutes et redémarrez l'outil de mise à niveau de base de données. Si l'outil de mise à niveau de base de données continue de vous avertir que des cellules sont à présent actives, revenez à la procédure sous « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 44 et vérifiez que toutes les cellules sont à présent inactives.

Une fois que vous avez répondu à toutes les invites, l'outil de mise à niveau de base de données s'exécute et affiche des messages de progression.

```
Executing upgrade task: Start UpdateStatementManager
...[3]
Successfully ran upgrade task
Executing upgrade task: ...
.......... Successfully ran upgrade task
...
```

```
Executing upgrade task: Stop UpdateStatementManager
...[3]
...
Successfully ran upgrade task
```

3 (Facultatif) Recréez les index de base de données et mettez à jour les statistiques de base de données.

Ces procédures peuvent améliorer les performances de la base de données après la mise à niveau.

```
Do you wish to rebuild the database indexes? Cette opération peut prendre quelques minutes.
[Y/N] y
Rebuilding database indexes
...
Do you wish to update the database statistics? Cette opération peut prendre quelques
minutes. [Y/N] y
Updating database statistics
...
```

Une fois la base de données mise à niveau, le script de mise à niveau propose de redémarrer les services vCloud Director sur l'hôte.

```
Would you like to start the vCloud Director service now? If you choose not to start it now, you
can manually start it at any time using this command: service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment).
```

Mettre à niveau le dispositif vShield Manager ou NSX Manager qui est associé à un système vCenter Server connecté

Avant de mettre à niveau un système vCenter Server et les hôtes reliés à vCloud Director, vous devez mettre à niveau le dispositif vShield Manager ou NSX Manager associé à ce système.

Lors de la mise à niveau du dispositif vShield Manager ou NSX Manager, l'accès aux fonctions d'administration est interrompu. Les services réseau, en revanche, continuent de fonctionner.

Prérequis

- Avant de démarrer la mise à niveau, vérifiez qu'au moins une cellule mise à niveau s'exécute dans votre installation de vCloud Director. La cellule écrit des données concernant le dispositif vShield Manager ou NSX Manager mis à niveau dans la base de données vCloud Director.
- Selon que vous mettez à niveau un dispositif vShield Manager ou NSX Manager, vérifiez que vous disposez des élément nécessaires à la mise à niveau de l'un ou de l'autre.

vShield Manager	Gestionnaire NSX
Consultez les informations sur la mise à niveau disponibles dans le Centre de documentation VMware vCloud Networking and Security à l'adresse https://www.vmware.com/support/pubs/vshield_pubs.html.	Consultez les informations sur la mise à niveau disponibles dans le Centre de documentation NSX pour vSphere à l'adresse https://www.vmware.com/support/pubs/nsx_pubs.html.

Procédure

1 Procédez à la mise à niveau de l'installation du dispositif vShield Manager ou NSX Manager associé en suivant la procédure de mise à niveau applicable au produit et à la version vers laquelle vous effectuez la mise à niveau.

AVERTISSEMENT Lorsque vous mettez à niveau vers une nouvelle version de NSX Manager, ne mettez pas à niveau les dispositifs vShield Edge associés existants en les convertissant en dispositifs NSX Edge. vCloud Director ne prend pas en charge les dispositifs NSX Edge. Lorsque vous utilisez un dispositif NSX Manager avec vCloud Director, vCloud Director se sert de celui-ci pour créer des dispositifs vShield Edge.

Option	Action
Mettez à niveau un dispositif vShield Manager associé vers une version plus récente.	Consultez les informations sur la mise à niveau de vShield Manager dans le *Guide d'installation et de mise à niveau de vShield* à l'adresse https://www.vmware.com/support/pubs/vshield_pubs.html. Mettez à niveau uniquement le dispositif vShield Manager, sans mettre à niveau les autres composants vShield Ne mettez pas à niveau les dispositifs vShield Edge associés existants.
Mettez à niveau un dispositif vShield Manager associé en le convertissant en dispositif NSX Manager ou bien mettez à niveau un dispositif NSX Manager associé vers une version plus récente.	Consultez les informations sur la mise à niveau de NSX Manager dans le *Guide d'installation et de mise à niveau de NSX* à l'adresse https://www.vmware.com/support/pubs/nsx_pubs.html. Mettez à niveau uniquement le dispositif vShield Manager ou NSX Manager, sans mettre à niveau les autres composants de vShield ou NSX pour vSphere. Ne mettez pas à niveau les dispositifs vShield Edge associés existants.

2 Répétez la procédure Étape 1 pour chaque dispositif vShield Manager ou NSX Manager associé aux autres systèmes vCenter Server enregistrés dans votre Cloud.

Une fois la mise à niveau terminée, le dispositif vShield Manager ou NSX Manager mis à niveau notifie à vCloud Director que la version du logiciel a changé. L'envoi de la notification et son traitement par vCloud Director peut prendre quelques minutes.

Suivant

Une fois que vous avez mis à niveau chaque dispositif vShield Manager ou NSX Manager associé, vous devez mettre à niveau l'ensemble des hôtes et des systèmes vCenter Server enregistrés avant d'utiliser vCloud Director pour mettre à niveau les dispositifs vShield Edge associés. Reportez-vous à « Mettre à niveau les systèmes vCenter Server, les hôtes et les dispositifs vShield Edge », page 51.

Mettre à niveau les systèmes vCenter Server, les hôtes et les dispositifs vShield Edge

Une fois que vous avez mis à niveau vCloud Director et le dispositif vShield Manager ou NSX Manager, vous devez mettre à niveau les systèmes vCenter Server et les hôtes reliés à votre Cloud. Une fois l'ensemble des systèmes vCenter Server et des hôtes reliés mis à niveau, vous devez alors utiliser vCloud Director pour mettre à niveau les dispositifs vShield Edge associés, par le biais d'un redéploiement des passerelles Edge Gateway ou d'une réinitialisation des réseaux vApp.

Prérequis

Assurez-vous que chacun des dispositifs vShield Manager ou NSX Manager associés aux systèmes vCenter Server connectés à votre Cloud ont bien été mis à niveau. Reportez-vous à « Mettre à niveau le dispositif vShield Manager ou NSX Manager qui est associé à un système vCenter Server connecté », page 50.

Procédure

1 Mettez à niveau le système vCenter Server relié.

Consultez le *Guide d'installation et de configuration de vSphere*.

2 Vérifiez l'ensemble des URL publiques et des chaînes de certificat de vCloud Director.

Dans l'onglet **Administration** de la console Web de vCloud Director, cliquez sur **Adresses publiques** dans le volet gauche. Entrez des valeurs dans tous les champs.

3 (Facultatif) Si vous avez configuré vCloud Director pour utiliser vCenter Single Sign On, vous devez désinscrire et réinscrire vCloud Director auprès de vCenter Lookup Service.

a Connectez-vous à vCloud Director comme administrateur système en utilisant un compte local ou LDAP. N'utilisez pas vCenter Single Sign On pour cette connexion.

b Désinscrivez vCloud Director de vCenter Lookup Service.

Dans l'onglet **Administration** de la console Web de vCloud Director, cliquez sur **Fédération** dans le volet gauche et cliquez sur **Désinscription**. Vous devez fournir les informations d'identification d'administrateur vCenter appropriées pour mener à bien cette action.

c Inscrivez vCloud Director sur vCenter Lookup Service.

Voir « Configurer vCloud Director pour utiliser vCenter Single Sign On » dans le *Guide de l'administrateur de vCloud Director*

4 Actualisez l'enregistrement du système vCenter Server avec vCloud Director.

a Dans la console Web de vCloud Director, cliquez sur l'onglet **Gérer et surveiller**, puis sur **vCenter** dans le volet de gauche.

b Cliquez avec le bouton droit sur le nom du système vCenter Server et sélectionnez **Actualiser**.

c Cliquez sur **Oui**.

5 Mettez à niveau chaque hôte pris en charge par le système vCenter Server mis à niveau.

Consultez le *Guide d'installation et de configuration de vSphere*. Pour chaque hôte, la mise à niveau requiert les étapes suivantes :

a Sur la console Web vCloud Director, désactivez l'hôte.

Sur la page **Gérer et surveiller**, cliquez sur **Hôtes**, puis cliquez avec le bouton droit sur l'hôte et sélectionnez **Désactiver l'hôte**.

b Utilisez le système vCenter Server pour activer le mode de maintenance sur l'hôte et autoriser toutes les machines virtuelles sur cet hôte à migrer vers un autre hôte.

c Mettez à niveau l'hôte.

Pour disposer de suffisamment d'hôtes mis à niveau afin de prendre en charge les machines virtuelles de votre Cloud, mettez les hôtes à niveau par lots. Ainsi, les mises à niveau de l'agent hôte peuvent s'effectuer à temps pour permettre aux machines virtuelles de retourner sur l'hôte mis à niveau.

d Utilisez le système vCenter Server pour reconnecter l'hôte.

e Mettez à niveau l'agent hôte vCloud Director sur l'hôte.

Reportez-vous à la section « Mettre à niveau un agent hôte ESX/ESXi » dans le *Guide de l'administrateur vCloud Director*.

f Sur la console Web vCloud Director, activez l'hôte.

Sur la page **Gérer et surveiller**, cliquez sur **Hôtes**, puis cliquez avec le bouton droit sur l'hôte et sélectionnez **Activer l'hôte**.

g Utilisez le système vCenter Server pour désactiver le mode de maintenance sur l'hôte.

6 Utilisez votre version de vCloud Director mise à niveau pour mettre à niveau, à leur tour, tous les dispositifs vShield Edge gérés par le dispositif vShield Manager ou NSX Manager associé au système vCenter Server mis à niveau.

AVERTISSEMENT Si le système vCenter Server mis à niveau est associé à un dispositif NSX Manager au lieu de vShield Manager, utilisez uniquement les méthodes décrites dans cette étape afin de mettre à niveau automatiquement les dispositifs vShield Edge à l'aide de vCloud Director. N'utilisez aucune autre méthode de mise à niveau des dispositifs vShield Edge associés par conversion en dispositifs NSX Edge. vCloud Director ne prend pas en charge les dispositifs NSX Edge. Lorsque vous utilisez un dispositif NSX Manager avec vCloud Director, vCloud Director se sert de celui-ci pour créer des dispositifs vShield Edge.

Lorsque vous réinitialisez un réseau protégé par vShield Edge à l'aide de la console Web de vCloud Director ou de l'API REST, le dispositif vShield Edge est automatiquement mis à niveau vers la version appropriée.

- Dans le cas d'une passerelle Edge Gateway, il vous suffit de la redéployer pour mettre à niveau le dispositif vShield Edge qui y est associé.
- Dans le cas des réseaux vApp auxquels les machines virtuelles se connectent (tels que les réseaux vApp routés ou isolés, ou les réseaux de centres de données virtuels d'organisation protégés), il vous suffit de réinitialiser le réseau vApp dans le contexte du vApp pour mettre à niveau le dispositif vShield Edge associé à ce réseau. Pour utiliser la console Web de vCloud Director pour réinitialiser un réseau vApp dans le contexte d'un vApp, accédez à l'onglet **Mise en réseau** du vApp, affichez ses détails de mise en réseau, cliquez avec le bouton droit sur le réseau vApp, puis sélectionnez **Réinitialiser le réseau**.

Pour plus d'informations sur le redéploiement des passerelles Edge Gateway et la réinitialisation des réseaux vApp, consultez l'aide en ligne de la console Web de vCloud Director ou le *Guide de programmation des API vCloud*, selon la méthode que vous souhaitez utiliser.

Suivant

Reprenez cette procédure pour les autres systèmes vCenter Server enregistrés sur votre Cloud.

Configuration de vCloud Director 4

Après avoir configuré tous les serveurs du groupe de serveurs vCloud Director et les avoir connectés à la base de données, vous pouvez initialiser la base de données du groupe de serveurs avec une clé de licence, un compte d'administrateur système et des informations connexes. Au terme de ce processus, terminez le provisionnement initial de votre Cloud à l'aide de la console Web vCloud Director.

Avant d'exécuter la console Web vCloud Director, vous devez exécuter l'assistant de configuration. Celui-ci rassemble des informations dont la console Web a besoin pour démarrer. Une fois l'assistant terminé, la console Web démarre et affiche l'écran d'ouverture de session. La console Web vCloud Director offre un ensemble d'outils de provisionnement et de gestion du Cloud. Elle inclut la fonctionnalité de démarrage rapide qui vous guide tout au long d'étapes, telles que la liaison de vCloud Director à vCenter et la création d'une organisation.

Prérequis

- Terminez l'installation de tous les serveurs vCloud Director et vérifiez que les services vCloud Director ont démarré sur tous les serveurs.
- Vérifiez que vous disposez de l'URL que le script de configuration affiche à la fin de son exécution.

Remarque Pour connaître l'URLde l'assistant de configuration, consultez le nom de domaine complet associé à l'adresse IP que vous avez spécifiée pour le service HTTP lors de l'installation du premier serveur et utilisez-la pour créer une URL de la forme suivante, https://*nom-domaine-complet*, par exemple, https://moncloud.exemple.com. Vous pouvez connecter l'assistant à cette URL.

Terminez l'installation de tous les serveurs vCloud Director et vérifiez que les services vCloud Director ont démarré sur tous les serveurs.

Procédure

1 Ouvrez un navigateur Web et connectez-vous à l'URL que le script de configuration a affichée lorsqu'il s'est terminé.

2 Pour terminer l'installation, laissez-vous guider par les invites.

Ce chapitre aborde les rubriques suivantes :

Lecture du contrat de licence

Avant de configurer un groupe de serveurs vCloud Director, vous devez lire et accepter les conditions générales du contrat de licence de l'utilisateur final.

Procédure

1 Lisez le contrat de licence.

2 Acceptez ou refusez le contrat.

Option	Action
Pour accepter le contrat de licence.	Cliquez sur **Oui, j'accepte les termes du contrat de licence**.
Pour refuser le contrat de licence, cliquez sur	**Non, je n'accepte pas les termes du contrat de licence**.

Si vous refusez le contrat de licence, vous ne pourrez pas procéder à la configuration de vCloud Director.

Saisie de la clé de licence

Chaque cluster vCloud Director requiert une licence pour fonctionner. La licence correspond au numéro de série du produit. Le numéro de série du produit figure dans la base de données vCloud Director.

Le numéro de série du produit vCloud Director est différent de la clé de licence vCenter Server. Pour utiliser un vCloud, vous devez disposer d'un numéro de série du produit vCloud Director et d'une clé de licence vCenter Server. Les deux types de clés de licence sont disponibles sur le portail des licences VMware.

Procédure

1 Procurez-vous un numéro de série du produit vCloud Director sur le portail des licences VMware.

2 Tapez le numéro de série du produit dans la zone de texte **Numéro de série du produit**.

Création du compte de l'administrateur système

Spécifiez le nom d'utilisateur, le mot de passe et les informations de contact pour l'administrateur système vCloud Director.

L'administrateur système vCloud Director bénéficie de privilèges de superutilisateur pour l'ensemble du Cloud. La création du compte d'administrateur système initial s'effectue au cours de la configuration de vCloud Director. Une fois l'installation et la configuration terminées, cet administrateur système peut créer d'autres comptes d'administrateur système selon les besoins.

Procédure

1 Tapez le nom d'utilisateur de l'administrateur système.

2 Tapez le mot de passe de l'administrateur système et confirmez-le.

3 Tapez le nom complet de l'administrateur système.

4 Tapez l'adresse e-mail de l'administrateur système.

Spécification des paramètres système

Vous pouvez spécifier les paramètres système qui régissent les interactions de vCloud Director avec vSphere et vShield Manager ou NSX Manager.

Le processus de configuration crée un dossier dans le système vCenter Server connecté destiné à vCloud Director et spécifie un identifiant d'installation à utiliser lors de la création d'adresses MAC pour des cartes réseaux virtuelles.

Procédure

1 Tapez le nom du dossier vCenter Server de vCloud Director dans le champ **Nom de système**.

2 Dans le champ **Identifiant d'installation**, spécifiez l'identifiant d'installation pour cette installation de vCloud Director.

Si un centre de données comprend plusieurs installations de vCloud Director, vous devez spécifier un identifiant d'installation unique pour chaque installation.

Prêt à se connecter à vCloud Director

Une fois que vous avez fourni toutes les informations requises par l'assistant de configuration, il vous reste à confirmer les paramètres que vous avez définis et à exécuter l'assistant. Lorsque l'assistant a terminé, l'écran de connexion de la console Web vCloud Director apparaît.

La page Prêt à se connecter répertorie tous les paramètres que vous avez fournis à l'assistant. Vérifiez soigneusement les paramètres.

Prérequis

Vérifiez que vous avez accès au système vCenter Server que vous souhaitez utiliser avec votre Cloud ainsi qu'au dispositif vShield Manager ou NSX Manager associé à ce système vCenter Server. La console Web vCloud Director doit pouvoir accéder aux installations de vCenter Server et aux dispositifs vShield Manager ou NSX Manager que vous voulez configurer pour cette installation de vCloud Director. Ces installations doivent être exécutées et configurées pour fonctionner ensemble afin que vous puissiez terminer cette tâche. Pour plus d'informations sur les exigences relatives à la configuration, consultez « Configuration matérielle et logicielle requise pour installer vCloud Director », page 9.

Procédure

- Pour modifier un paramètre, cliquez sur **Précédent** jusqu'à ce que vous reveniez à la page d'origine du paramètre.
- Pour confirmer tous les paramètres et terminer le processus de configuration, cliquez sur **Terminer**.

Lorsque vous cliquez sur **Terminer**, l'assistant applique les paramètres que vous avez spécifiés, puis il démarre la console Web vCloud Director et affiche son écran de connexion.

Suivant

Utilisez cet écran pour vous connecter à la console Web vCloud Director avec le nom d'utilisateur et le mot de passe que vous avez fournis pour le compte de l'administrateur système. Une fois que vous vous êtes connecté, la console affiche un certain nombre d'étapes de démarrage rapide que vous devez effectuer pour utiliser ce Cloud. Une fois que vous avez effectué toutes ces étapes, les Tâches guidées sont activées et le Cloud est prêt à l'emploi.

Référence de l’outil de gestion des cellules 5

L'outil de gestion des cellules est un utilitaire de ligne de commande que vous pouvez utiliser pour gérer une cellule et ses certificats SSL et pour exporter des tables depuis la base de données vCloud Director. Des informations d'identification de superutilisateur ou d'administrateur système sont requises pour certaines opérations.

L’outil de gestion des cellules est installé dans `/opt/vmware/vcloud-director/bin/cell-management-tool`.

Liste des commandes disponibles

Pour lister les commandes disponibles de l'outil de gestion des cellules, utilisez la ligne de commande suivante.

```
cell-management-tool -h
```

Exemple : Aide sur l'utilisation de l’outil de gestion des cellules

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool
-h,--help   print this message

Available commands:
cell - Manipulates the Cell and core components
certificates - Reconfigures the SSL certificates for the cell
ciphers - Reconfigure the list of disallowed SSL ciphers for the cell
configure-metrics - Collects and stores properties necessary for collecting and querying metrics
data
dbextract - Exports the data from the given set of tables
fix-scheduler-data - Scan database for corrupt scheduler data.  Fix scheduler job data if
corrupt.
generate-certs - Generates self-signed SSL certificates for use with vCD cell.
recover-password - Change a forgotten System Administrator password. Database credentials are
required.
fail-tasks - Fail all tasks running on this cell and set a custom failure message.

For command specific help:
 cell-management-tool <commandName> -h
```

- Gestion d’une cellule page 60

  Utilisez la commande `cell` de l'outil de gestion de cellule pour suspendre le planificateur de tâches pour que les nouvelles tâches ne puissent pas être démarrées, pour vérifier l'état des tâches actives, pour contrôler le mode de maintenance de la cellule et pour arrêter proprement la cellule.

- Exportation des tables de base de données page 61

  Utilisez la commande `dbextract` de l'outil de gestion des cellules pour exporter des données depuis la base de données vCloud Director.

- Détection et réparation des données corrompues du planificateur page 64

  Si vous connaissez le nom d'utilisateur et le mot de passe de la base de données vCloud Director, vous pouvez utiliser la commande `fix-scheduler-data` de l'outil de gestion des cellules pour rechercher les données corrompues du planificateur dans la base de données et réparer les données le cas échéant.

- Remplacement des certificats SSL page 64

  Utilisez la commande `certificates` de l'outil de gestion des cellules pour remplacer les certificats SSL des cellules.

- Génération de certificats SSL auto-signés page 65

  Utilisez la commande `generate-certs` de l'outil de gestion des cellules pour générer de nouveaux certificats SSL auto-signés pour la cellule.

- Gestion de la liste des chiffrements SSL autorisés page 67

  Utilisez la commande `ciphers` de l'outil de gestion des cellules pour configurer l'ensemble des suites de chiffrement que la cellule propose d'utiliser lors du processus d'établissement de liaison SSL.

- Configuration de la connexion à la base de données de mesures page 69

  Utilisez la commande `configure-metrics` de l'outil de gestion des cellules pour connecter la cellule à la base de données de mesures en option.

- Restauration du mot de passe de l'administrateur système page 69

  Si vous connaissez le nom d'utilisateur et le mot de passe de la base de données vCloud Director, vous pouvez utiliser la commande `recover-password` de l'outil de gestion des cellules pour restaurer le mot de passe de l'administrateur système vCloud Director.

- Forcer l'exécution des tâches en cours page 70

  Utilisez la commande `fail-tasks` de l'outil de gestion des cellules pour générer la liste des tâches en cours sur une cellule mise en veille dont vous pouvez forcer immédiatement l'exécution avec un état d'échec.

Gestion d'une cellule

Utilisez la commande `cell` de l'outil de gestion de cellule pour suspendre le planificateur de tâches pour que les nouvelles tâches ne puissent pas être démarrées, pour vérifier l'état des tâches actives, pour contrôler le mode de maintenance de la cellule et pour arrêter proprement la cellule.

Pour gérer une cellule, utilisez une ligne de commande au format suivant :

`cell-management-tool -u` *`sysadmin-username`* `-p` *`sysadmin-password`* `cell` *`command`*

sysadmin-username Nom d'utilisateur d'un administrateur système vCloud Director.

sysadmin-password Mot de passe de l'administrateur système vCloud Director.

REMARQUE Vous pouvez fournir le mot de passe de l'administrateur système vCloud Director dans la ligne de commande `cell-management-tool`, mais il est préférable de l'omettre pour des raisons de sécurité. Dans ce cas, `cell-management-tool` demande le mot de passe qui ne s'affiche pas lorsque vous le tapez.

commande Sous-commande `cell`.

Tableau 5-1. Options et arguments de l'outil de gestion des cellules, sous-commande `cell`

Commande	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--maintenance` (`-m`)	`true` ou `false`	Contrôle le mode de maintenance d'une cellule. L'argument `true` place la cellule en mode de maintenance. (Vous devez préalablement mettre au repos la cellule.) L'argument `false` fait sortir la cellule du mode de maintenance.
`--quiesce` (`-q`)	`true` ou `false`	Met en veille l'activité sur la cellule. L'argument `true` suspend le planificateur. L'argument `false` redémarre le planificateur.
`--shutdown` (`-s`)	Aucun	Arrête les services vCloud Director sur le serveur.
`--status` (`-t`)	Aucun	Affiche des informations sur le nombre de tâches exécutées sur la cellule et l'état de la cellule.
`--status-verbose` (`-tt`)	Aucun	Affiche des informations détaillées sur le nombre de tâches exécutées sur la cellule et l'état de la cellule.

Exemple : Obtention de l'état des tâches

La ligne de commande `cell-management-tool` suivante fournit les informations d'identification d'administrateur système et indique le nombre de tâches en cours. Lorsque la valeur `Job count` indique `0` et que la valeur `Is Active` indique `false`, vous pouvez arrêter la cellule en toute sécurité.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3 Is Active = true
```

Exportation des tables de base de données

Utilisez la commande `dbextract` de l'outil de gestion des cellules pour exporter des données depuis la base de données vCloud Director.

Pour exporter des tables de base de données, utilisez une ligne de commande au format suivant :

```
cell-management-tool dbextract options
```

Tableau 5-2. Options et arguments de l'outil de gestion des cellules, sous-commande `dbextract`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`-categories`	Liste séparée par des virgules de catégories de table à exporter.	Facultatif. `NETWORKING` est la seule catégorie prise en charge.

Tableau 5-2. Options et arguments de l'outil de gestion des cellules, sous-commande `dbextract` (suite)

Option	Argument	Description
`-dataFile`	Chemin d'accès absolu vers un fichier décrivant les données à exporter.	Facultatif. S'il n'est pas fourni, la commande utilise `$VCLOUD_HOME/etc/data_to_export.properties`. Reportez-vous à « Spécification de tables et de colonnes à exporter », page 63.
`-dumpFolder`	Un chemin d'accès absolu vers le dossier dans lequel créer le vidage de mémoire. Le dossier doit exister et être accessible par vcloud.vcloud.	Toutes les données seront exportées dans un fichier situé dans ce dossier.
`-exportSettingsFile`	Chemin absolu vers un fichier de propriétés de paramètres d'exportation de données.	Facultatif. S'il n'est pas fourni, la commande utilise `$VCLOUD_HOME/etc/data_export_settings.ini`. Reportez-vous à « Limitation et tri des lignes exportées », page 63.
`-properties`	Chemin absolu vers un fichier de propriétés de connexion de base de données.	Facultatif. S'il n'est pas fourni, la commande utilise les propriétés de connexion de base de données dans `$VCLOUD_HOME/etc/global.properties`. Reportez-vous à « Spécification d'un fichier de propriétés », page 62.
`-tables`	Liste séparée par des virgules de tables.	Facultatif. Exportez toutes les tables pour voir des noms de table individuelle.

Spécification d'un fichier de propriétés

Par défaut, la commande `dbextract` extrait des données depuis la base de données vCloud Director à l'aide des informations de connexion de base de données dans le fichier `$VCLOUD_HOME/etc/global.properties` de la cellule actuelle. Pour extraire des données depuis une base de données vCloud Director différente, spécifiez les propriétés de connexion de base de données dans un fichier et utilisez l'option `-properties` pour fournir le chemin d'accès vers ce fichier sur la ligne de commande. Le fichier de propriétés est un fichier UTF-8 au format suivant.

```
username=username
password=password
servicename=db_service_name
port=db_connection_port
database-ip=db_server_ip_address
db-type=db_type
```

nom d'utilisateur Nom d'utilisateur de la base de données vCloud Director.

mot de passe Mot de passe de la base de données vCloud Director.

db_service_name Nom de service de la base de données. Par exemple, `orcl.example.com`.

db_connection_port Port de base de données.

db_server_ip_address Adresse IP du serveur de base de données.

db_type Type de base de données. Doit être `Oracle` ou `MS_SQL`.

Spécification de tables et de colonnes à exporter

Pour limiter l'ensemble de données exportées, utilisez l'option `–exportSettingsFile` et créez un fichier `data_to_export.properties` spécifiant des tables individuelles et, en option, des colonnes à exporter. Ce fichier est un fichier UTF-8 contenant zéro ligne ou plus au format *TABLE_NAME*:*COLUMN_NAME*.

TABLE_NAME Nom d'une table dans la base de données. Pour voir une liste de noms de table, exportez toutes les tables.

COLUMN_NAME Nom d'une colonne dans le *TABLE_NAME* spécifié.

Cet exemple de fichier `data_to_export.properties` exporte des colonnes depuis les tables `ACL` et `ADDRESS_TRANSLATION`.

```
ACL:ORG_MEMBER_ID
ACL:SHARABLE_ID
ACL:SHARABLE_TYPE
ACL:SHARING_ROLE_ID
ADDRESS_TRANSLATION:EXTERNAL_ADDRESS
ADDRESS_TRANSLATION:EXTERNAL_PORTS
ADDRESS_TRANSLATION:ID
ADDRESS_TRANSLATION:INTERNAL_PORTS
ADDRESS_TRANSLATION:NIC_ID
```

La commande s'attend à trouver ce fichier dans `$VCLOUD_HOME/etc/data_to_export.properties`, mais vous pouvez spécifier un autre chemin.

Limitation et tri des lignes exportées

Pour n'importe quelle table, vous pouvez spécifier le nombre de lignes à exporter et comment trier les lignes exportées. Utilisez l'option `–exportSettingsFile` et créez un fichier `data_export_settings.ini` spécifiant des tables individuelles. Ce fichier est un fichier UTF-8 contenant zéro entrée ou plus au format suivant :

```
[TABLE_NAME]
rowlimit=int
orderby=COLUMN_NAME
```

TABLE_NAME Nom d'une table dans la base de données. Pour voir une liste de noms de table, exportez toutes les tables.

COLUMN_NAME Nom d'une colonne dans le *TABLE_NAME* spécifié.

Cet exemple de fichier `data_export_settings.ini` limite les données exportées depuis la table `AUDIT_EVENT` aux 10 000 premières lignes et trie ces lignes en fonction de la valeur dans la colonne `event_time`.

```
[AUDIT_EVENT]
rowlimit=100000
orderby=event_time
```

La commande s'attend à trouver ce fichier dans `$VCLOUD_HOME/etc/data_export_settings.ini`, mais vous pouvez spécifier un autre chemin.

Exemple : Exportation de toutes les tables depuis la base de données vCloud Director actuelle.

Cet exemple exporte toutes les tables de la base de données vCloud Director actuelle vers le fichier `/tmp/dbdump`.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool dbextract -dumpFolder /tmp/dbdump
This utility outputs data from your vCloud Director system that may contain sensitive data. Do
you want to continue and output the data (y/n)?
y
Exporting data now. Please wait for the process to finish Exported 144 of 145 tables.
```

Détection et réparation des données corrompues du planificateur

Si vous connaissez le nom d'utilisateur et le mot de passe de la base de données vCloud Director, vous pouvez utiliser la commande `fix-scheduler-data` de l'outil de gestion des cellules pour rechercher les données corrompues du planificateur dans la base de données et réparer les données le cas échéant.

Pour rechercher les données corrompues du planificateur dans la base de données, utilisez une ligne de commande au format suivant :

```
cell-management-tool fix-scheduler-data options
```

Tableau 5-3. Options et arguments de l'outil de gestion des cellules, sous-commande `fix-scheduler-data`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--dbuser`	Nom d'utilisateur de l'utilisateur de la base de données vCloud Director.	Doit être fourni sur la ligne de commande.
`--dbpassword`	Mot de passe de l'utilisateur de la base de données vCloud Director.	Invité à le fournir s'il n'est pas indiqué.

Remplacement des certificats SSL

Utilisez la commande `certificates` de l'outil de gestion des cellules pour remplacer les certificats SSL des cellules.

La commande `certificates` de l'outil de gestion des cellules automatise le processus de remplacement des certificats existants d'une cellule par des nouveaux, qui sont stockés dans un magasin de clés JCEKS. La commande `certificates` vous aide à remplacer des certificats auto-signés par des certificats signés. Pour créer un magasin de clés JCEKS contenant des certificats signés, consultez « Création et importation d'un certificat SSL signé », page 19.

Pour remplacer les certificats SSL de la cellule, utilisez une commande au format suivant :

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

Tableau 5-4. Options et arguments de l'outil de gestion des cellules, sous-commande `certificates`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--config` (-c)	Chemin d'accès complet vers le fichier `global.properties` de la cellule	Réglé par défaut sur `$VCLOUD_HOME/etc/global.properties`.
`--httpks` (-j)	Aucun	Générer un fichier keystore nommé `certificates` à utiliser par le point de terminaison http.
`--consoleproxyks` (-p)	Aucun	Générer un fichier keystore nommé `proxycertificates` à utiliser par le point de terminaison proxy.
`--responses` (-r)	Chemin d'accès complet vers le fichier `responses.properties` de la cellule	Réglé par défaut sur `$VCLOUD_HOME/etc/responses.properties`.
`--keystore` (-s)	*keystore-pathname*	Chemin d'accès complet vers un magasin de clés JCEKS contenant les certificats signés.
`--keystore-pwd` (-w)	*keystore-password*	Mot de passe du magasin de clés JCEKS référencé par l'option `--keystore`.

Exemple : Remplacement des certificats

Vous pouvez omettre les options `--config` et `--responses` sauf si ces fichiers ont été déplacés vers leurs emplacements par défaut. Dans cet exemple, un keystore dans `/tmp/my-new-certs.ks` a le mot de passe `kspw`. Cet exemple remplace le certificat existant du point de terminaison http de la cellule par celui trouvé dans `/tmp/my-new-certs.ks`

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool certificates -j -s /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks. You will need to restart the
cell for changes to take effect.
```

Remarque Vous devez redémarrer la cellule une fois que vous avez remplacé les certificats.

Génération de certificats SSL auto-signés

Utilisez la commande `generate-certs` de l'outil de gestion des cellules pour générer de nouveaux certificats SSL auto-signés pour la cellule.

La commande `generate-certs` de l'outil de gestion des cellules automatise la procédure indiquée dans « Création d'un certificat SSL autosigné », page 22.

Pour générer de nouveaux certificats SSL auto-signés et les ajouter à un magasin de clés nouveau ou existant, utilisez une ligne de commande au format suivant :

```
cell-management-tool generate-certs options
```

Tableau 5-5. Options et arguments de l'outil de gestion des cellules, sous-commande `generate-certs`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--expiration` (-x)	*days-until-expiration*	Nombre de jours avant l'expiration des certificats. Réglé par défaut sur 365.
`--issuer` (-i)	*name=value* [, *name=value*, ...]	Nom distinct X.509 de l'émetteur du certificat. Réglé par défaut sur `CN=`*`FQDN`*. où *FQDN* est le nom de domaine complet de la cellule ou son adresse IP si aucun nom de domaine complet n'est disponible. Si vous spécifiez plusieurs paires attribut/valeur, séparez-les par des virgules et placez des guillemets autour de l'argument.
`--httpcert` (-j)	Aucun	Générer un certificat pour le point de terminaison http.
`--key-size` (-s)	*key-size*	Taille de paire de clés exprimée sous forme de nombre entier de bits. Réglé par défaut sur 2 048. Notez que les tailles de clés inférieures à 1 024 bits ne sont plus prises en charge par la publication spéciale NIST 800-131A.
`--keystore-pwd` (-w)	*keystore-password*	Mot de passe du magasin de clés sur cet hôte.
`--out` (-o)	*keystore-pathname*	Chemin d'accès complet vers un magasin de clés sur cet hôte.
`--consoleproxycert` (-p)	Aucun	Générer un certificat pour le point de terminaison de proxy de la console.

Remarque Pour conserver la compatibilité avec les versions précédentes de cette sous-commande, le fait d'omettre `-j` et `-p` a le même résultat que le fait d'indiquer `-j` et `-p`.

Exemple : Création de certificats auto-signés

Ces deux exemples supposent l'existence d'un magasin de clés dans `/tmp/cell.ks` avec le mot de passe `kspw`. Ce magasin de clés est créé s'il n'existe pas déjà.

Cet exemple crée les nouveaux certificats à l'aide des valeurs par défaut. Le nom de l'émetteur est défini sur `CN=Unknown`. Le certificat utilise la clé 2 048 bits par défaut et expire un an après sa création.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool generate-certs -j -p -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

Cet exemple créé un nouveau certificat pour le point de terminaison http uniquement. Il détermine également la taille de la clé et le nom de l'émetteur qui sont des valeurs personnalisées. Le nom de l'émetteur est défini sur `CN=Test, L=London, C=GB`. Le nouveau certificat pour la connexion http a une clé de 4 096 bits et expire 90 jours après sa création. Le certificat existant du point de terminaison de proxy de la console demeure inchangé.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]#
./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London, C=GB" -s
4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

Gestion de la liste des chiffrements SSL autorisés

Utilisez la commande `ciphers` de l'outil de gestion des cellules pour configurer l'ensemble des suites de chiffrement que la cellule propose d'utiliser lors du processus d'établissement de liaison SSL.

Lorsqu'un client effectue une connexion SSL sur une cellule vCloud Director, la cellule propose d'utiliser uniquement les chiffrements qui sont configurés sur la liste par défaut des chiffrements autorisés. Plusieurs chiffrements ne font pas partie de cette liste, soit parce qu'ils ne sont pas suffisamment robustes pour sécuriser la connexion, soit parce qu'ils sont connus pour contribuer aux échecs de connexion SSL. Lorsque vous installez ou mettez à niveau vCloud Director, le script d'installation ou de mise à niveau examine les certificats de la cellule. Si l'un des certificats utilise un chiffrement qui ne fait pas partie de la liste des chiffrements autorisés, le script modifie la configuration de la cellule afin d'autoriser l'utilisation de ce chiffrement et affiche un avertissement. Vous pouvez continuer à utiliser les certificats existants malgré leur dépendance vis-à-vis de ces chiffrements ou suivre les étapes pour remplacer les certificats et reconfigurer la liste des chiffrements autorisés :

1. Créez de nouveaux certificats qui n'utilisent aucun des chiffrements rejetés. Vous pouvez utiliser `cell-management-tool ciphers -a` comme indiqué à la section « Exemple : Répertorier tous les chiffrements autorisés », page 68 pour répertorier tous les chiffrements autorisés dans la configuration par défaut.
2. Utilisez la commande `cell-management-tool certificates` pour remplacer les certificats existants de la cellule par les nouveaux.
3. Utilisez la commande `cell-management-tool ciphers` pour reconfigurer la liste des chiffrements autorisés afin d'exclure tous les chiffrements non utilisés par les nouveaux certificats. L'exclusion de ces chiffrements facilite la mise en place d'une connexion SSL sur la cellule, du fait que le nombre de chiffrements offerts lors de l'établissement de liaison est réduit au minimum pratique.

   IMPORTANT Étant donné que la console VMRC requiert l'utilisation de chiffrements AES256-SHA et AES128-SHA, vous ne pouvez pas les rejeter si vos clients vCloud Director utilisent la console VMRC.

Pour gérer la liste des chiffrements SSL autorisés, utilisez une ligne de commande ayant le format suivant :

```
cell-management-tool ciphers options
```

Tableau 5-6. Options et arguments de l'outil de gestion des cellules, sous-commande `ciphers`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--all-allowed` (-a)	Aucun	Répertorier tous les chiffrements autorisés.
`--compatible-reset` (-c)	Aucun	Réinitialiser la liste par défaut des chiffrements autorisés et autoriser les chiffrements utilisés par les certificats de cette cellule.

Tableau 5-6. Options et arguments de l'outil de gestion des cellules, sous-commande `ciphers` (suite)

Option	Argument	Description
`--disallow` (-d)	Liste séparée par des virgules de noms de chiffrement, telle que publiée sur le site http://www.openssl.org/docs/apps/ciphers.html	Rejeter les chiffrements de la liste séparée par des virgules.
`--list` (-l)	Aucun	Répertorier les chiffrements actuellement configurés.
`--reset` (-r)	Aucun	Réinitialiser la liste par défaut des chiffrements autorisés. Si les certificats de cette cellule utilisent des chiffrements rejetés, vous ne pourrez pas établir de connexion SSL à la cellule tant que vous n'aurez pas installé de nouveaux certificats qui contiennent un chiffrement autorisé.

Exemple : Répertorier tous les chiffrements autorisés

Utilisez l'option `--all-allowed` (-a) pour répertorier tous les chiffrements que la cellule est autorisée à offrir lors de l'établissement de liaison SSL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA * TLS_DHE_DSS_WITH_AES_128_CBC_SHA *
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA * TLS_DHE_RSA_WITH_AES_256_CBC_SHA *
TLS_DHE_RSA_WITH_AES_128_CBC_SHA * TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA *
TLS_RSA_WITH_AES_256_CBC_SHA * TLS_RSA_WITH_AES_128_CBC_SHA * TLS_RSA_WITH_3DES_EDE_CBC_SHA *
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA * TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA *
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA * TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA *
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA * TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA *
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA * TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA *
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA * TLS_ECDH_RSA_WITH_AES_256_CBC_SHA *
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA * TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA *
SSL_RSA_WITH_3DES_EDE_CBC_SHA * SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

Exemple : Rejeter deux chiffrements

Utilisez l'option `--disallow` (-d) pour supprimer un ou plusieurs chiffrements de la liste des chiffrements autorisés. Cette option requiert au moins un nom de chiffrement. Vous pouvez fournir plusieurs noms de chiffrement dans une liste séparée par des virgules. Vous pouvez obtenir des noms pour cette liste à partir du résultat de `ciphers -a`. Cet exemple supprime deux chiffrements répertoriés dans l'exemple précédent.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]#
./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

Configuration de la connexion à la base de données de mesures

Utilisez la commande `configure-metrics` de l'outil de gestion des cellules pour connecter la cellule à la base de données de mesures en option.

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. Les données concernant les mesures historiques sont stockées dans une base de données KairosDB dépendant de Cassandra. Reportez-vous à Chapitre 6, « Installer et configurer le logiciel de base de données facultatif pour stocker et récupérer les mesures historiques de performances de machine virtuelle », page 71.

Pour créer une connexion entre KairosDB et un dispositif vCloud Director, utilisez une ligne de commande au format suivant :

```
cell-management-tool configure-metrics options
```

Tableau 5-7. Options et arguments de l'outil de gestion des cellules, sous-commande `configure-metrics`

Commande	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--repository-host`	Nom d'hôte ou adresse IP de l'hôte KairosDB	Si vous avez plusieurs installations de KairosDB, vous devez fournir ici l'adresse de l'équilibrage de charge.
`--repository-port`	Port de KairosDB à utiliser.	Par défaut, KairosDB écoute le port 8080.

Exemple : Configuration d'une connexion à la base de données de mesures

Cet exemple configure le système pour utiliser une instance de KairosDB hébergée à l'adresse IP 10.0.0.1 avec le port par défaut. L'adresse peut être l'adresse d'une machine unique exécutant une seule instance de KairosDB ou l'adresse d'un équilibrage de charge qui répartit les demandes sur plusieurs installations de KairosDB.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]#
./cell-management-tool configure-metrics --repository-host 10.0.0.1 --repository-port 8080
```

Restauration du mot de passe de l'administrateur système

Si vous connaissez le nom d'utilisateur et le mot de passe de la base de données vCloud Director, vous pouvez utiliser la commande `recover-password` de l'outil de gestion des cellules pour restaurer le mot de passe de l'administrateur système vCloud Director.

Avec la commande `recover-password` de l'outil de gestion des cellules, un utilisateur qui connaît le nom d'utilisateur et le mot de passe de la base de données vCloud Director peut restaurer le mot de passe de l'administrateur système vCloud Director.

Pour restaurer le mot de passe de l'administrateur système, utilisez une ligne de commande au format suivant :

```
cell-management-tool recover-password options
```

Tableau 5-8. Options et arguments de l'outil de gestion des cellules, sous-commande `recover-password`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--dbuser`	Nom d'utilisateur de l'utilisateur de la base de données vCloud Director.	Doit être fourni sur la ligne de commande.
`--dbpassword`	Mot de passe de l'utilisateur de la base de données vCloud Director.	Invité à le fournir s'il n'est pas indiqué.

Forcer l'exécution des tâches en cours

Utilisez la commande `fail-tasks` de l'outil de gestion des cellules pour générer la liste des tâches en cours sur une cellule mise en veille dont vous pouvez forcer immédiatement l'exécution avec un état d'échec.

Lorsque vous mettez une cellule en veille avec la commande `cell-management-tool -q`, les tâches en cours d'exécution doivent se terminer proprement en quelques minutes. Si des tâches continuent de s'exécuter sur une cellule mise en veille, le superutilisateur peut forcer l'arrêt de ces tâches avec un état d'échec afin que la maintenance du système puisse commencer.

Pour générer la liste des tâches en cours d'exécution pour lesquelles vous pouvez forcer l'échec, utilisez une ligne de commande au format suivant :

```
cell-management-tool fail-tasks -m "message"
```

Tableau 5-9. Options et arguments de l'outil de gestion des cellules, sous-commande `fail-tasks`

Commande	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--message` (-m)	Texte de message.	Texte de message à placer dans l'état de fin de tâche.

Exemple : Échec des tâches en cours d'exécution sur la cellule

Cet exemple génère la liste des tâches en cours d'exécution sur cette cellule qui peuvent être mises en échec et demande la confirmation de mise en échec forcée pour ces tâches.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system, Organization:
org1 Would you like to fail the tasks listed above?
```

Tapez **y** pour faire échouer la tâche avec un état d'échec d'arrêt administratif. Tapez **n** pour permettre à la tâche de continuer de s'exécuter.

Remarque Si plusieurs tâches sont renvoyées dans la réponse, vous devez décider de faire échouer toutes ces tâches ou de ne prendre aucune mesure. Vous ne pouvez pas décider de faire échouer un sous-ensemble de tâches.

Installer et configurer le logiciel de base de données facultatif pour stocker et récupérer les mesures historiques de performances de machine virtuelle

6

vCloud Director peut collecter des mesures qui fournissent des informations actuelles et historiques sur les performances et la consommation de ressources des machines virtuelles qui se trouvent dans votre Cloud. Les données concernant les mesures historiques sont stockées dans une base de données KairosDB dépendant d'un cluster de Cassandra.

Cassandra et KairosDB sont des bases de données Open Source qui, lorsqu'elles sont déployées ensemble, offrent une solution haute performance et évolutive pour collecter des données de séries chronologiques telles que les mesures de la machine virtuelle. Si vous souhaitez que votre Cloud puisse récupérer les mesures historiques des machines virtuelles, vous devez installer et configurer Cassandra et KairosDB, puis utiliser l'utilitaire `cell-management-tool` pour connecter vCloud Director à KairosDB. La récupération des mesures historiques ne nécessite pas l'utilisation du logiciel de base de données facultatif.

Pour prendre en charge la récupération des mesures historiques, vCloud Director nécessite un cluster Cassandra. Un cluster Cassandra comprend une ou plusieurs machines sur lesquelles vous avez installé Cassandra et qui exécutent le service Cassandra. Pour une installation standard de vCloud Director, vous devez installer au moins trois machines dans le cluster Cassandra. Dans la mesure où la fonction de surveillance des mesures de vCloud Director utilise un facteur de réplication de deux, le fait d'avoir trois machines (les nœuds) dans le cluster Cassandra, permet de s'assurer qu'un nœud est toujours disponible pour gérer une transaction. Vous pouvez utiliser un cluster Cassandra unique pour votre installation de vCloud Director.

Vous devez également disposer d'au moins une instance de KairosDB configurée pour pouvoir utiliser votre cluster Cassandra. Si votre Cloud collecte des mesures historiques provenant de nombreuses machines virtuelles, des instances supplémentaires de KairosDB peuvent s'avérer nécessaires. Vous pouvez installer et configurer KairosDB comme l'un des nœuds Cassandra et pointer l'outil de gestion des cellules vers ce point de terminaison ou installer et configurer KairosDB sur chaque nœud Cassandra, ajouter un équilibrage de charge en face de la configuration, puis pointer l'outil de gestion des cellules vers le point de terminaison de l'équilibrage de charge. Du fait que vCloud Director est censé communiquer avec KairosDB à une adresse IP unique, les installations qui incluent plusieurs instances de KairosDB doivent utiliser un équilibrage de charge pour fournir cette adresse et répartir les demandes de vCloud Director sur ces instances de KairosDB.

Prérequis

- Vérifiez que vCloud Director est installé et qu'il fonctionne avant de configurer le logiciel de base de données facultatif.
- Si vous ne vous êtes pas encore familiarisé avec Cassandra et KairosDB, consultez la documentation disponible à l'adresse http://cassandra.apache.org/ et https://code.google.com/p/kairosdb/.
- Procurez-vous soit Cassandra 1.2.*x*, soit Cassandra 2.0. *x* à partir de http://cassandra.apache.org/download/.
- Procurez-vous KairosDB 0.9.1 à partir de https://code.google.com/p/kairosdb/.

- Terminez l'installation et la configuration du cluster Cassandra que vous prévoyez d'utiliser avec votre installation de vCloud Director, conformément à la configuration suivante :
  - Cassandra 1.2.*x* ou Cassandra 2.0.*x* est installé sur au moins trois machines qui sont connectées au même réseau que celui utilisé par vos cellules vCloud Director.
  - Les machines sont configurées de façon à avoir leur propre stockage physique et non un stockage partagé.
  - Les machines sont configurées en tant que cluster Cassandra.
  - Java Native Access (JNA) version 3.2.7 ou ultérieure est activé pour le cluster Cassandra, afin d'améliorer les performances d'utilisation de la mémoire et d'accès au disque.
- Terminez l'installation et la configuration d'au moins une instance de KairosDB 0.9.1 sur l'un des nœuds Cassandra afin d'utiliser votre cluster Cassandra comme sa base de données. Vous pouvez également installer et configurer KairosDB sur chaque nœud Cassandra si vous ajoutez un équilibrage de charge en face de cette configuration.
- Vérifiez que KairosDB et Cassandra sont configurés correctement. Utilisez un navigateur Web pour accéder à `http://KairosDB-IP:8080/api/v1/metricnames`. Si la page s'ouvre sans erreur, KairosDB et Cassandra sont configurés correctement.
- Vérifiez que vous pouvez exécuter la commande `service` de l'utilitaire `cell-management-tool`. Pour plus de détails concernant la commande `service`, consultez « Démarrage ou arrêt des services vCloud Director », page 38.

Procédure

1 Utilisez l'utilitaire `cell-management-tool` pour configurer une connexion entre vCloud Director et KairosDB.

Utilisez une commande similaire à la suivante, où *KairosDB-IP* est l'adresse IP de la machine sur laquelle vous avez installé KairosDB ou l'adresse IP de l'équilibrage de charge que vous utilisez pour répartir les demandes entre plusieurs instances de KairosDB.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool configure-metrics --repository-host KairosDB-IP
--repository-port 8080
```

2 Redémarrez chaque cellule vCloud Director en utilisant la commande `service` de l'utilitaire `cell-management-tool`.

Index

S

V