vCloud Director Guide d'installation et de mise à niveau

vCloud Director 5.1

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-000749-00

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 visé

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.

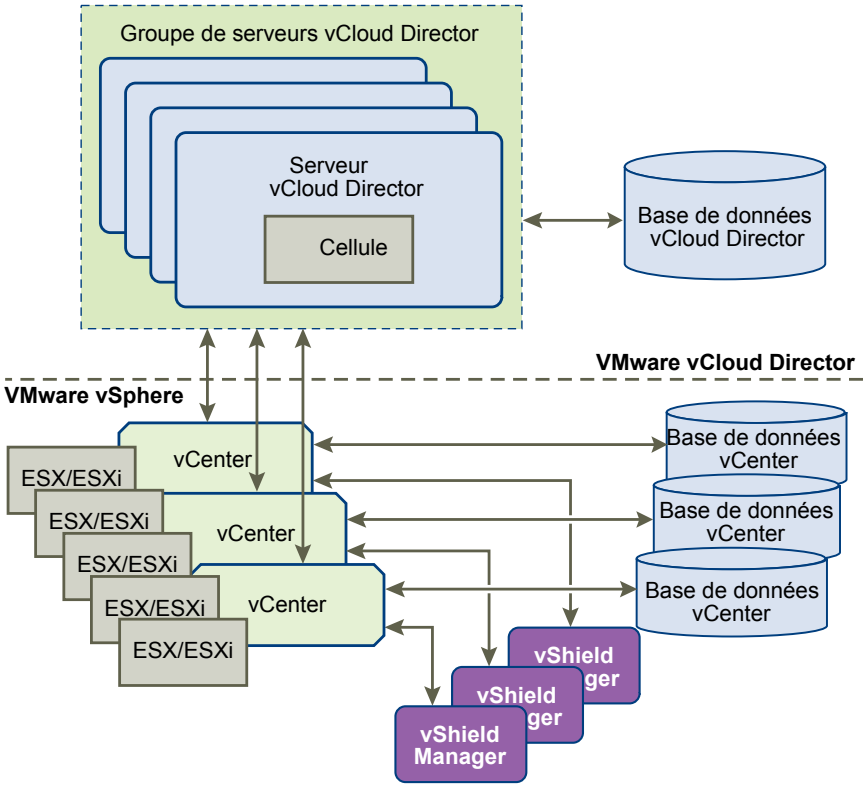
Ce chapitre aborde les rubriques suivantes :

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 serveurs vCenter et d'hôtes ESX/ESXi. Les seveurs vShield Manager fournissent les services réseau à vCenter et vCloud Director.

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 dans le groupe se connecte à plusieurs serveurs vCenter, aux hôtes ESX/ESXi qu'elle gère et aux serveurs vShield Manager qui ont été configurés pour prendre en charge les serveurs vCenter.

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



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 serveur vCenter, à vShield Manager et aux hôtes ESX/ESXi. Un administrateur système peut alors utiliser la console Web vCloud Director pour connecter à tout moment des serveurs vCenter, des serveurs vShield Manager et des serveurs ESX/ESXi supplémentaires 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) pour chaque serveur vCenter devant être accessible dans votre Cloud.
- Assurez-vous que tous les serveurs vCloud Director sont conformes à la configuration requise en termes de mémoire, CPU et 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 il est indiqué dans « Installation et configuration d'une base de données vCloud Director », page 14.

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 pouvoir accéder à un serveur vCenter, un serveur vShield Manager et à un ou plusieurs hôtes ESX/ESXi.

Versions de vCenter Server, ESX/ESXi et vShield Manager prises en charge

Les informations actuelles sur les versions de vCenter Server, ESX/ESXi et vShield Manager prises en charge sont disponibles dans les *Matrices d'interopérabilité des produits VMware* à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Configuration vSphere requise

Les serveurs vCenter et les hôtes ESX/ESXi que vous prévoyez d'utiliser avec vCloud Director doivent répondre à des conditions de configuration spécifiques.

- Les réseaux vCenter que vous prévoyez d'utiliser en tant que réseaux vCloud Director externes ou pools de réseaux doivent être disponibles à tous les hôtes de tout cluster devant être utilisés par vCloud Director. Si vous rendez ces réseaux disponibles à tous les hôtes d'un centre de données, il vous sera plus facile d'ajouter de nouveaux serveurs vCenter à vCloud Director par la suite.
- Les vSphere Distributed Switches doivent être utilisés pour l'isolement entre hôtes et l'allocation de pools de réseaux.
- Les clusters vCenter utilisés avec vCloud Director doivent être configurés pour utiliser le service automatisé DRS. Ce service requiert que le stockage partagé soit connecté à tous les hôtes d'un cluster DRS.
- Les serveurs vCenter doivent avoir confiance en leurs hôtes ESX/ESXi. 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
Red Hat Enterprise Linux 5 (64 bits), Update 4
Red Hat Enterprise Linux 5 (64 bits), Update 5
Red Hat Enterprise Linux 5 (64 bits), Update 6
Red Hat Enterprise Linux 5 (64 bits), Update 8

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

Système d'exploitation
Red Hat Enterprise Linux 6 (64 bits), Update 1
Red Hat Enterprise Linux 6 (64 bits), Update 2

Espace disque requis Chaque serveur vCloud Director requiert environ 950 Mo d'espace disque libre destiné aux fichiers d'installation et aux journaux.

Mémoire requise Chaque serveur vCloud Director doit comporter au moins 1 Go de mémoire (2 Go recommandés).

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	

Bases de données vCloud Director prises en charge

vCloud Director prend en charge les bases de données Oracle et Microsoft SQL Server. Les dernières informations sur les bases de données prises en charge sont disponibles dans les *Matrices d'interopérabilité des produits VMware* à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Pour plus d'informations sur les configurations de serveur de base de données, consultez « Installation et configuration d'une base de données vCloud Director », page 14.

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.

Navigateurs qui prennent en charge vCloud Director

La console Web vCloud Director est compatible avec de nombreuses versions des navigateurs Web Firefox et 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.

Navigateurs pris en charge sur les plates-formes Microsoft Windows

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

Plate-forme	Internet Explorer 7.*x*	Internet Explorer 8.*x*	Internet Explorer 9.*x*	Firefox 12.*x*, 13.*x*
Windows XP Pro 32 bits	OUI	OUI	Non	OUI
Windows XP Pro 64 bits	OUI	OUI	Non	OUI
Windows Server 2003 Enterprise Edition (32 bits)	OUI	OUI	Non	OUI
Windows Server 2003 Enterprise Edition (64 bits)	OUI	OUI	Non	OUI
Windows Server 2008	OUI	OUI	OUI	OUI
Windows Server 2008 R2	Non	OUI	OUI	OUI
Windows Vista (32 bits)	OUI	OUI	OUI	OUI
Windows Vista (64 bits)	OUI	OUI	OUI	OUI
Windows 7 (32 bits)	Non	OUI	OUI	OUI
Windows 7 (64 bits)	Non	OUI	OUI	OUI

Navigateurs pris en charge sur les plates-formes Linux

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

Plate-forme	Firefox 11.*x*
Red Hat Enterprise Linux 5 (32 bits), Update 6	OUI
Red Hat Enterprise Linux 6 (32 bits)	OUI
Red Hat Enterprise Linux 6 (64 bits)	OUI
SLES 11 (32 bits)	OUI
Ubuntu 10.10 (32 bits)	OUI
Ubuntu 10.10 (64 bits)	OUI

Versions prises en charge d'Adobe Flash Player

La console Web vCloud Director requiert Adobe Flash Player version 10.2 ou ultérieure. 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 versions prises en charge sont SSL 3.0 et TLS 1.0. 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 de la configuration réseau requise

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 auquel les serveurs vCloud Director, le serveur de base de données, les serveurs vCenter et les serveurs vShield Manager sont connectés, doit respecter plusieurs conditions de configuration :

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 les serveurs de bases de données, doivent être configurés dans le même fuseau horaire.

Résolution des noms d'hôtes
Tous les noms d'hôtes que vous spécifiez lors de l'installation et la configuration de vCloud Director et de vShield Manager doivent pouvoir être résolus à l'aide de DNS en utilisant pour cela la résolution (ainsi que la résolution inverse) du nom de domaine complet (FQDN) ou du nom d'hôte non qualifié. Par exemple, pour un hôte nommé `mycloud.example.com`, les deux commandes suivantes doivent s'exécuter avec succès sur un hôte vCloud Director :

```
nslookup mycloud
nslookup mycloud.example.com
```

En outre, si l'adresse IP de l'hôte `mycloud.example.com` est 192.168.1.1, la commande suivante doit retourner `mycloud.example.com`:

```
nslookup 192.168.1.1
```

Stockage du serveur de transfert

Pour mettre en place un stockage temporaire destiné aux téléchargements, tous les serveurs dans un cluster vCloud Director doivent pouvoir accéder à un système de fichiers en réseau ou à un volume de stockage partagé. L'utilisateur racine doit pouvoir accéder en écriture à ce volume. Chaque hôte doit monter ce volume à `$VCLOUD_HOME/data/transfer`, en général `/opt/vmware/vcloud-director/data/transfer`. Les téléchargements peuvent occuper ce stockage quelques heures ou une journée entière. Étant donné que les images transférées peuvent être volumineuses, allouez au moins plusieurs centaines de giga-octets pour ce volume.

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 et ESX
514	UDP	Facultatif. Permet d'utiliser syslog
902	TCP	Connexions vCenter et ESX
903	TCP	Connexions vCenter et ESX
920	TCP, UDP	rpc.statd NFS utilisé par le service de transfert

Tableau 1-7. Ports qui doivent autoriser les paquets sortants provenant des hôtes vCloud Director (suite)

Port	Protocole	Commentaires
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 pour les extensions de tâche
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- Ne connectez pas les ordinateurs hôtes physiques aux réseaux physiques qui constituent des liaisons montantes pour les commutateurs distribués vNetwork qui soutiennent les pools de réseaux vCloud Director.
- 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, puis créez le compte d'utilisateur de la 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 les commandes suivantes pour créer des données (CLOUD_DATA) et un espaces de tables d'index (CLOUD_INDX) distincts :

```
Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1000M
autoextend on;

Create Tablespace CLOUD_INDX datafile '$ORACLE_HOME/oradata/cloud_indx01.dbf' size 500M
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 connaître le nom du service de la base de données, ouvrez le fichier `$ORACLE_HOME/network/admin/tsnames.ora` sur le serveur de la base de données et recherchez une entrée similaire à celle-ci :

```
(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 nécessite 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 que vous envisagez d'utiliser dans un cluster vCloud Director requiert deux certificats SSL, un pour chacune de ses adresses IP.

Remarque Tous les répertoires dans le chemin d'accès vers les certificats SSL doivent être lisibles par l'utilisateur `vcloud.vcloud`. Cet utilisateur est créé par le programme d'installation de vCloud Director.

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.

4 Créez les certificats.

   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. Une longueur de clé de 2 048 bits fournit un niveau de sécurité 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 requiert deux certificats SSL : un pour chacune de ses adresses IP résidant dans un fichier keystore Java. Vous devez créer deux certificats SSL pour chaque serveur que vous prévoyez d'utiliser dans votre groupe de serveurs vCloud Director. 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.

Pour créer et importer des certificats autosignés, consultez « Création d'un certificat SSL autosigné », page 20.

Prérequis

- Générez une liste de noms de domaines complets et de leurs adresses IP associées sur ce serveur, ainsi qu'un choix de services pour chaque adresse IP. Consultez « Création de certificats SSL », page 17.
- Vérifiez que vous avez accès à un ordinateur sur lequel un environnement d'exécution Java version 6 est installé, de sorte à 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 6. 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.

Procédure

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

   Cette commande permet de créer un certificat non approuvé dans un fichier keystore nommé `certificates.ks`.

   ```
   keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias http
   ```

   Le certificat est valide pendant 90 jours.

2 Répondez aux questions de `keytool`.

   Lorsque `keytool` vous demande vos nom et prénom, tapez le nom de domaine complet associé à l'adresse IP destinée au service HTTP.

3 Répondez au reste des questions en indiquant des informations appropriées à votre organisation et votre emplacement, comme le montre l'exemple suivant.

```
What is your first and last name? [Unknown]:mycloud.example.com
What is the name of your organizational unit? [Unknown]:Engineering
What is the name of your organization? [Unknown]:Example Corporation
What is the name of your City or Locality? [Unknown]:Palo Alto
What is the name of your State or Province? [Unknown]:California
What is the two-letter country code for this unit? [Unknown]:US
Is CN=mycloud.example.com, OU=Engineering, O="Example Corporation", L="Palo Alto",
ST=California, C=US correct?[no]:yes
Enter key password for <http> (RETURN if same as keystore password):
```

4 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
```

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

La commande suivante ajoute un certificat non approuvé au fichier keystore créé dans Étape 1.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -
alias consoleproxy
```

Le certificat est valide pendant 90 jours.

6 Lorsque `keytool` vous demande vos nom et prénom, tapez le nom de domaine complet associé à l'adresse IP destinée au service de proxy de la console.

7 Répondez au reste des questions en indiquant des informations appropriées à votre organisation et votre emplacement, comme le montre l'exemple suivant Étape 3.

8 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
```

9 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.

10 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
```

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

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

12 Répétez la procédure de l'étape Étape 1 à l'étape Étape 11 sur chacun des serveurs vCloud Director restants.

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. Consultez « Configuration des connexions au réseau et à la base de données », page 28.

Remarque Le script de configuration de vCloud Director ne pouvant pas s'exécuter sous une identité dotée de privilèges, le fichier keystore et le répertoire dans lequel il réside doivent être accessibles en lecture par n'importe quel utilisateur.

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 requiert deux certificats SSL : un pour chacune de ses adresses IP résidant dans un fichier keystore Java. Vous devez créer deux certificats SSL pour chaque serveur que vous prévoyez d'utiliser dans votre groupe de serveurs vCloud Director. 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.

Pour créer et importer des certificats signés, consultez « Création et importation d'un certificat SSL signé », page 18.

Prérequis

- Générez une liste de noms de domaines complets et de leurs adresses IP associées sur ce serveur, ainsi qu'un choix de services pour chaque adresse IP. Consultez « Création de certificats SSL », page 17.
- Vérifiez que vous avez accès à un ordinateur sur lequel un environnement d'exécution Java version 6 est installé, de sorte à 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 6. 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.

Procédure

1 Créez un certificat non approuvé pour le service HTTP.

Cette commande permet de créer un certificat non approuvé dans un fichier keystore nommé `certificates.ks`.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass motdepasse –genkey –keyalg RSA
–alias http
```

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

La commande suivante ajoute un certificat non approuvé au fichier keystore créé dans Étape 1.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass passwd –genkey –keyalg RSA –
alias consoleproxy
```

Le certificat est valide pendant 90 jours.

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

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

4 Répétez la procédure de l'étape Étape 1 à l'étape Étape 3 sur chacun des serveurs vCloud Director restants.

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. Consultez « Configuration des connexions au réseau et à la base de données », page 28.

Remarque Le script de configuration de vCloud Director ne pouvant pas s'exécuter sous une identité dotée de privilèges, le fichier keystore et le répertoire dans lequel il réside doivent être accessibles en lecture par n'importe quel utilisateur.

Installation et configuration de vShield Manager

vCloud Director dépend de vShield Manager pour fournir les services réseau au Cloud. Installez et configurez vShield Manager avant de commencer l'installation de vCloud Director.

Vous devez associer chaque serveur vCenter que vous ajoutez à vCloud Director à une instance unique de vShield Manager. Pour plus d'informations sur la configuration réseau requise et les versions prises en charge de vShield Manager, consultez « Configuration matérielle et logicielle requise pour installer vCloud Director », page 9.

Important Cette procédure s'applique uniquement aux nouvelles installations de vCloud Director. Si vous mettez à niveau une installation existante de vCloud Director, vous pouvez également mettre à niveau l'installation de vShield Manager qui y est associée, si vous le souhaitez. Une nouvelle version de vShield Manager ne peut pas fonctionner avec une version existante de vCloud Director. Consultez « Mise à niveau de vShield Manager », page 49.

Procédure

1 Utilisez vSphere Client pour vous connecter à vCenter Server.

2 Sélectionnez **[Fichier] > [Déployer le modèle OVF]** .

3 Accédez à l'emplacement de `vShield Manager.ovf` et suivez les invites pour déployer le fichier OVF.

4 Une fois le fichier OVF déployé, démarrez la machine virtuelle vShield Manager et ouvrez la console.

5 Ouvrez une session sur la console avec le nom d'utilisateur **`admin`** et le mot de passe **`default`**.

6 À l'invite `manager`, tapez **`enable`**.

7 À l'invite `Password`, tapez **`default`** pour activer le mode de configuration.

Une fois le mode de configuration activé, la chaîne d'invite devient `manager#`.

8 À l'invite `manager#`, tapez **`setup`** pour commencer la procédure de configuration.

9 Entrez l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour la machine virtuelle vShield Manager.

Vous avez besoin de ces informations pour joindre un serveur vCenter à Cloud Director.

10 Tapez **`exit`** pour fermer la session.

11 Fermez la console, mais n'arrêtez pas la machine virtuelle.

Il n'est pas nécessaire de synchroniser vShield Manager avec vCenter ou d'enregistrer vShield Manager en tant que plug-in vSphere Client lorsque vous utilisez vShield Manager avec vCloud Director.

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 comporte 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.

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 Obtenez et importez les clés publiques VMware.

   a Créez un répertoire pour stocker les clés publiques VMware.

   b Utilisez un navigateur Web pour télécharger toutes les clés publiques VMware depuis le répertoire http://packages.vmware.com/tools/keys.

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

   d 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.

2 (Facultatif) Utilisez l'outil Linux `rpm` pour vérifier la signature numérique du fichier téléchargé.

   ```
   # rpm --checksig installation-file
   ```

   Après avoir vérifié la signature numérique du fichier, vous pouvez utiliser celui-ci pour installer ou mettre à niveau vCloud Director sur n'importe quel serveur, sans devoir installer la clé publique sur ce serveur. Le programme d'installation vous avertit si aucune clé n'est installée. Vous pouvez ignorer l'avertissement si vous avez déjà vérifié la signature du fichier.

Création d'un groupe de serveurs vCloud Director 2

Un groupe de serveurs vCloud Director est constitué d'un ou de plusieurs serveurs vCloud Director. Chaque serveur dans le groupe exécute un ensemble de services appelé cellule vCloud Director. Pour créer un groupe de serveurs, vous devez installer le logiciel vCloud Director sur chaque serveur, configurer les connexions de ce dernier au réseau et à la base de données et démarrer ses services vCloud Director.

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 35

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

1. Vérifiez qu'un serveur vCenter pris en charge fonctionne et qu'il est configuré correctement pour fonctionner avec vCloud Director. Pour plus d'informations sur les versions prises en charge et la configuration requise, consultez « Versions de vCenter Server, ESX/ESXi et vShield Manager prises en charge », page 9.
2. Vérifiez qu'un serveur vShield Manager pris en charge fonctionne et qu'il est configuré correctement pour fonctionner avec vCloud Director. Pour plus d'informations sur les versions prises en charge, consultez « Versions de vCenter Server, ESX/ESXi et vShield Manager prises en charge », page 9. Pour plus de détails sur l'installation et la configuration, consultez « Installation et configuration de vShield Manager », page 21.
3. Vérifiez que vous disposez d'au moins une plate-forme de serveur vCloud Director en cours de fonctionnement et configurée avec une quantité de mémoire appropriée et un espace de stockage suffisant. 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 9.
   - Chaque membre d'un groupe de serveurs nécessite deux adresses IP : une pour une connexion SSL destinée au service HTTP et l'autre pour le service de proxy de la console.
   - Chaque serveur doit disposer d'un certificat SSL pour chaque adresse IP. Tous les répertoires dans le chemin d'accès vers les certificats SSL doivent être lisibles par l'utilisateur `vcloud.vcloud`. Cet utilisateur est créé par le programme d'installation de vCloud Director. Consultez « Création de certificats SSL », page 17.
   - Pour le service de transfert, chaque serveur doit monter un système de fichiers en réseau ou un autre volume de stockage partagé à `$VCLOUD_HOME/data/transfer`, en général `/opt/vmware/vcloud-director/data/transfer`. L'utilisateur racine doit pouvoir accéder en écriture à ce volume.

- Chaque serveur doit avoir accès à un package de déploiement Microsoft Sysprep. Consultez « Création d'un package de déploiement Microsoft Sysprep », page 33.

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. Consultez « Installation et configuration d'une base de données vCloud Director », page 14.
   - 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 et les serveurs vCenter et vShield Manager peuvent résoudre mutuellement leurs noms comme il est indiqué dans « Résumé de la configuration réseau requise », page 12.

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 de la configuration réseau requise », page 12.

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 13. Le port 443 doit être ouvert entre vCloud Director et les serveurs vCenter.

Ce chapitre aborde les rubriques suivantes :

Installation et configuration 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 requises de la plate-forme et installe le logiciel vCloud Director sur celui-ci.

Le logiciel vCloud Director est distribué en tant que fichier exécutable Linux signé numériquement nommé `vmware-vcloud-director-5.1.0-`*nnnnnn*`.bin`, où *nnnnnn* représente un numéro de build. 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.

Prérequis

- Vérifiez que le serveur cible et que le réseau auquel il est connecté remplissent les conditions spécifiées dans « Résumé de la configuration réseau requise », page 12. Le serveur cible ne doit pas comporter un utilisateur ou un groupe existant nommé `vcloud`.
- Vérifiez que vous possédez les informations d'identification de superutilisateur sur le serveur cible.
- Si vous envisagez de créer un groupe de serveurs vCloud Director comprenant plusieurs serveurs, vérifiez que le serveur cible monte le stockage partagé du service de transfert à `$VCLOUD_HOME/data/transfer`.

- Si vous souhaitez 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, vous n'avez pas besoin de la revérifier au cours de l'installation. Reportez-vous à la rubrique « Téléchargement et installation de la clé publique VMware », page 23

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 et 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 au format suivant valide la somme de contrôle du *fichier d'installation* avec la *valeur de la somme de contrôle* MD5 copiée depuis la page de téléchargement.

```
md5sum –c checksum–value installation–file
```

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.

```
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 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.

Le programme d'installation vérifie que l'hôte répond à toutes les conditions requises, il vérifie la signature numérique du fichier d'installation et déballe le package RPM vCloud Director, puis il installe le logiciel. 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
```

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.

6 Choisissez quand exécuter le script de configuration.

Option	Description
Exécuter le script de configuration maintenant	Tapez **y** et appuyez sur Entrée.
Exécuter le script de configuration plus tard	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 28.

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. 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.

Prérequis

- Vérifiez qu'une base de données du type pris en charge est accessible depuis le serveur vCloud Director. Consultez « Installation et configuration d'une base de données vCloud Director », page 14 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. Consultez « Création et importation d'un certificat SSL signé », page 18. Le script de configuration ne pouvant pas s'exécuter sous une identité dotée de privilèges, le fichier keystore et le répertoire dans lequel il réside doivent être accessibles en lecture 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. Consultez « Installation et configuration d'une base de données vCloud Director », page 14.

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 de prendre en charge deux connexions SSL distinctes : une pour le service HTTP et l'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 14.

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 un groupe, consultez « Installation du logiciel vCloud Director sur des serveurs supplémentaires », page 32.

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. Consultez 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.

   Copiez le fichier à un emplacement auquel les serveurs que vous envisagez de configurer peuvent accéder. Le propriétaire du fichier doit être **`vcloud.vcloud`**. Le propriétaire du fichier doit y avoir accès en lecture et écriture comme le montre cet exemple. Si ce n'est pas le cas, le script de configuration ne pourra pas l'utiliser.

```
% ls -l responses.properties
-rw------- 1 vcloud vcloud 418 Jun 8 13:42
responses.properties
```

Suivant

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

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 la rubrique « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 37

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`

Installation du logiciel vCloud Director sur des serveurs supplémentaires

Vous pouvez ajouter des serveurs à un groupe de serveurs vCloud Director à tout moment. Tous les serveurs dans un groupe de serveurs doivent être configurés avec les mêmes détails de connexion à la base de données. Pour vous assurer que cette information est satisfaite, utilisez le fichier de réponses créé lors de l'installation du premier serveur pour fournir ces informations lorsque vous installez des serveurs supplémentaires.

Prérequis

Une copie du fichier de réponses créée lors de l'installation du premier serveur doit être accessible à tous les serveurs que vous ajoutez au groupe. Consultez « Protection et réutilisation du fichier de réponses », page 31.

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.

```
chmod u+x installation-file
```

4 Exécutez le fichier d'installation et fournissez le chemin d'accès au fichier de réponses.

Spécifiez l'option `-r` sur la ligne de commande d'installation et fournissez le chemin d'accès complet au fichier de réponses en tant qu'argument de cette option.

```
fichier-installation -r chemin d'accès-au-fichier-de-réponse
```

5 (Facultatif) Répétez cette procédure pour chaque serveur supplémentaire que vous ajoutez à cette installation.

Le programme d'installation demande les informations de connexion au réseau et configure les connexions au réseau et à la base de données à partir des réponses du fichier de réponses.

Suivant

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. Consultez Chapitre 4, « Configuration de vCloud Director », page 55.

Création d'un package de déploiement Microsoft Sysprep

Avant que vCloud Director puisse effectuer une personnalisation du client sur des machines virtuelles avec certains systèmes d'exploitation clients Windows, vous devez créer un package de déploiement Microsoft Sysprep sur chaque cellule de Cloud dans votre installation.

Au cours de l'installation, vCloud Director place certains fichiers dans le dossier `sysprep`, sur l'hôte du serveur vCloud Director. Ne remplacez pas ces fichiers lorsque vous créez le package Sysprep.

Prérequis

Accédez aux fichiers binaires Sysprep pour Windows 2000, Windows 2003 (32 et 64 bits) et Windows XP (32 et 64 bits).

Procédure

1 Copiez les fichiers binaires Sysprep pour chaque système d'exploitation à un emplacement pratique sur un hôte de serveur vCloud Director.

Chaque système d'exploitation nécessite son propre dossier.

Remarque Les noms de dossier sont sensibles à la casse.

Systèmes d'exploitation clients	Destination de copie
Windows 2000	*SysprepBinariesDirectory* `/win2000`
Windows 2003 (32 bits)	*SysprepBinariesDirectory* `/win2k3`
Windows 2003 (64 bits)	*SysprepBinariesDirectory* `/win2k3_64`
Windows XP (32 bits)	*SysprepBinariesDirectory* `/winxp`
Windows XP (64 bits)	*SysprepBinariesDirectory* `/winxp_64`

SysprepBinariesDirectory représente un emplacement de votre choix pour copier les binaires.

2 Exécutez la commande `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh` *SysprepBinariesDirectory*.

   Par exemple, `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MySysprepFiles`.

3 Utilisez la commande `service vmware-vcd restart` pour redémarrer la cellule de Cloud.

4 Si vous possédez plusieurs cellules de Cloud, copiez le package et le fichier de propriétés dans toutes les cellules de Cloud.

```
scp /opt/vmware/vcloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/vcloud-director/guestcustomization/windows_deployment_package_sysprep.cab
root@next_cell_IP:/opt/vmware/vcloud-director/guestcustomization
```

5 Redémarrez chaque cellule de Cloud dans laquelle vous copiez les fichiers.

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, dont vShield Manager, vCenter et ESX/ESXi.

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 Le processus de mise à niveau nécessite la mise à niveau de vCloud Director, vShield Manager, vCenter et de ESX/ESXi. Vous devez empêcher les utilisateurs d'accéder à vCloud Director jusqu'à ce que l'étape de mise à niveau de vShield Manager 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 votre Cloud fait appel à un équilibreur de charge, vous pouvez mettre à niveau un sous-ensemble du groupe de serveurs tout en gardant des 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 serveurs vCenter enregistrés s'ils n'exécutent pas une version compatible du logiciel vCenter. La mise à niveau de serveurs vCenter ou d'hôtes ESX/ESXi peut entraîner une interruption de service supplémentaire de vCloud Director, car les machines virtuelles sont inaccessibles lorsque leurs hôtes ou vCenter Server sont en cours de mise à niveau.

Mise à niveau d'un groupe de serveurs vCloud Director

1. Désactivez l'accès des utilisateurs à vCloud Director. Si vous le souhaitez, vous pouvez afficher un message de maintenance pendant la durée de la mise à niveau. Reportez-vous à la rubrique « Affichage du message de maintenance lors d'une mise à niveau », page 37.
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 la rubrique « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 37.

3 Mettez à niveau le logiciel vCloud Director sur tous les membres du groupe de serveurs. Reportez-vous à la rubrique « 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 la rubrique « Mise à niveau de la base de données vCloud Director », page 47.

5 Redémarrez vCloud Director sur les serveurs mis à niveau. Reportez-vous à la rubrique « Démarrage ou arrêt des services vCloud Director », page 32.

6 Mettez à niveau vShield Manager. Toutes les installations vShield Manager enregistrées sur ce groupe de serveurs doivent être mises à niveau vers une version du logiciel vShield Manager compatible avec la version de vCloud Director installée par la mise à niveau. Si le programme de mise à niveau détecte une version de vShield Manager incompatible, la mise à niveau ne sera pas autorisée. La dernière version de vShield Manager répertoriée dans « Versions de vCenter Server, ESX/ESXi et vShield Manager prises en charge », page 9 est requise pour utiliser les nouvelles fonctionnalités de mise en réseau de cette version de vCloud Director. Consultez « Mise à niveau de vShield Manager », page 49

7 Réactivez l'accès des utilisateurs à vCloud Director.

8 Mise à niveau de vCenter et d'hôtes ESX/ESXi. Reportez-vous à la rubrique « Mise à niveau de vCenter, d'hôtes ESX/ESXi et des dispositifs vShield Edge », page 50. Tous les serveurs vCenter enregistrés sur ce groupe de serveur doivent être mis à niveau vers une version du logiciel vCenter compatible avec la version de vCloud Director installée par la mise à niveau. Des serveurs vCenter incompatibles deviennent inaccessibles à vCloud Director une fois la mise à niveau terminée. Reportez-vous à la rubrique « Versions de vCenter Server, ESX/ESXi et vShield Manager prises en charge », page 9.

9 Prenez connaissance des modifications apportées à vos réseaux mis à niveau et reconfigurez les règles de pare-feu si nécessaire. Reportez-vous à la rubrique « Modifications de réseaux mis à niveau », page 51.

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.

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. Reportez-vous à la rubrique « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 37.

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 la rubrique « 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 la rubrique « Mise à niveau de la base de données vCloud Director », page 47.

6 Redémarrez vCloud Director sur les serveurs mis à niveau. Reportez-vous à la rubrique « Démarrage ou arrêt des services vCloud Director », page 32.

7 Mettez à niveau vShield Manager. Reportez-vous à la rubrique « Mise à niveau de vShield Manager », page 49.

8 Mise à niveau de vCenter et d'hôtes ESX/ESXi. Reportez-vous à la rubrique « Mise à niveau de vCenter, d'hôtes ESX/ESXi et des dispositifs vShield Edge », page 50.

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 la rubrique « Mise à niveau du logiciel vCloud Director sur un membre d'un groupe de serveurs », page 45.

11 Prenez connaissance des modifications apportées à vos réseaux mis à niveau et reconfigurez les règles de pare-feu si nécessaire. Reportez-vous à la rubrique « Modifications de réseaux mis à niveau », page 51.

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
```

Vous pouvez exécuter cette commande sur une cellule avant ou après sa mise à niveau. Lorsque vous êtes prêt à mettre la cellule à niveau ou à remettre une cellule mise à niveau en service, exécutez la commande suivante sur la cellule pour désactiver le message de maintenance.

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

Ce chapitre aborde les rubriques suivantes :

- « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 37
- « Mise à niveau du logiciel vCloud Director sur un membre d'un groupe de serveurs », page 45
- « Mise à niveau de la base de données vCloud Director », page 47
- « Mise à niveau de vShield Manager », page 49
- « Mise à niveau de vCenter, d'hôtes ESX/ESXi et des dispositifs vShield Edge », page 50
- « Modifications de réseaux mis à niveau », page 51

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 la rubrique « Référence de l'outil de gestion des cellules », page 38 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.

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 -p Pa55w0rd 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 -p Pa55w0rd 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 -p Pa55w0rd cell --shutdown
```

Suivant

Une fois que l'outil de gestion des cellules a arrêté les services vCloud Director sur le serveur, vous pouvez procéder à la mise à niveau du logiciel vCloud Director.

Référence de l'outil de gestion des cellules

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
 -p,--password <arg>   administrator password
 -u,--username <arg>   administrator username

Available commands:
 cell - Manipulates the Cell and core components
 dbextract - Exports the data from the given set of tables
 certificates - Reconfigures the SSL certificates for the cell
 generate-certs - Generates self-signed SSL certificates for use with vCD cell
 recover-password - Change a forgotten System Administrator password. Database credentials are
required

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

- Commandes pour la gestion d'une cellule page 39

  Utilisez la commande `cell` de l'outil de gestion des cellules pour suspendre le planificateur des tâches afin d'empêcher le démarrage de nouvelles tâches, pour vérifier l'état des tâches actives et pour arrêter correctement la cellule.

- Commandes pour l'exportation de tables de base de données page 40

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

- Commandes pour le remplacement de certificats SSL page 42

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

- Commandes pour la génération de certificats SSL auto-signés page 43

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

- Restauration du mot de passe de l'administrateur système page 44

  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.

Commandes pour la gestion d'une cellule

Utilisez la commande `cell` de l'outil de gestion des cellules pour suspendre le planificateur des tâches afin d'empêcher le démarrage de nouvelles tâches, pour vérifier l'état des tâches actives et pour arrêter correctement 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.
command	Sous-commande `cell`.

Tableau 3-1. 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.
`--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.

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 -p Pa55w0rd cell --status
Job count = 3
Is Active = true
```

Commandes pour l'exportation de 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 3-2. 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.
`-dataFile`	Chemin d'accès absolu vers un fichier décrivant les données à exporter.	Facultatif. S'il n'est pas fourni, la commande utilise `$VCLOUD_HOME/etc/data_to_export.properties`. Reportez-vous à la rubrique « Spécification de tables et de colonnes à exporter », page 41
`-dumpFile`	Chemin absolu vers un fichier dump.	Toutes les données seront exportées vers ce fichier.
`-exportSettingsFile`	Chemin absolu vers un fichier de propriétés de paramètres d'exportation de données.	Facultatif. S'il n'est pas fourni, la commande utilise `$VCLOUD_HOME/etc/data_export_settings.ini`. Reportez-vous à la rubrique « Limitation et tri des lignes exportées », page 42

Tableau 3-2. Options et arguments de l'outil de gestion des cellules, sous-commande `dbextract` (suite)

Option	Argument	Description
`–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 la rubrique « Spécification d'un fichier de propriétés », page 41
`–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
```

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

password 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.

Ce 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 -dumpFile /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.
```

Commandes pour le remplacement de 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 18.

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

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

Tableau 3-3. 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 `$VCLOUD_HOME/etc/global.properties`.
`--responses` (-r)	Chemin d'accès complet vers le fichier `responses.properties` de la cellule	Réglé par défaut sur `$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 magasin de clés dans `/tmp/new.ks` a le mot de passe `kspw`. Il remplace les certificats existants de la cellule par ceux trouvés dans `/tmp/new.ks`

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

Commandes pour la 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 20.

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 3-4. 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.
`-issuer` (-i)	*name=value* [, *name=value*, ...]	Nom distinct X.509 de l'émetteur du certificat. Réglé par défaut sur `CN=Unknown`. Si vous spécifiez plusieurs paires attribut/valeur, séparez-les par des virgules et placez des guillemets autour de l'argument.

Tableau 3-4. Options et arguments de l'outil de gestion des cellules, sous-commande `generate-certs` (suite)

Option	Argument	Description
`--out` (-o)	*keystore-pathname*	Chemin d'accès complet vers un magasin de clés sur cet hôte.
`--key-size` (-s)	*key-size*	Taille de paire de clés exprimée sous forme de nombre entier de bits. Réglé par défaut sur 1024.
`--keystore-pwd` (-w)	*keystore-password*	Mot de passe du magasin de clés sur cet hôte.
`--expiration` (-x)	*days-until-expiration*	Nombre de jours avant l'expiration des certificats. Réglé par défaut sur 365.

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 le cryptage 1024 bits et expire un an après sa création.

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

Cet exemple crée les nouveaux certificats à l'aide de valeurs personnalisées pour la taille de clé et le nom de l'émetteur. Le nom de l'émetteur est défini sur `CN=Test, L=London, C=GB`. Le certificat utilise le cryptage 2048 bits et expire 90 jours après sa création.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool generate-certs -o /tmp/cell.ks -w kspw
 -i "CN=Test, L=London, C=GB" -s 2048 -x 90
New keystore created and written to /tmp/cell.ks.
```

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 3-5. 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.

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-5.1.0-`*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 toutes les organisations dans le système contenant un réseau d'organisation contiennent également un vDC d'organisation. Comme le processus de mise à niveau convertit des réseaux d'organisation existants en réseaux vDC d'organisation, des organisations contenant des réseaux d'organisation mais aucun vDC d'organisation ne peuvent pas être mises à niveau, et la mise à niveau de la base de données échoue.
- Vérifiez que vous possédez les informations d'identification de superutilisateur sur le serveur cible.
- Si vous souhaitez 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, vous n'avez pas besoin de la revérifier au cours de l'installation. Reportez-vous à la rubrique « Téléchargement et installation de la clé publique VMware », page 23
- Utilisez l'outil de gestion des cellules pour mettre en veille et arrêter les services vCloud Director sur la cellule du serveur.

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 et 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 au format suivant valide la somme de contrôle du *fichier d'installation* avec la *valeur de la somme de contrôle* MD5 copiée depuis la page de téléchargement.

   ```
   md5sum –c checksum-value installation-file
   ```

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.

   ```
   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 la rubrique « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 37.

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.  Would you like
   to upgrade it?  The installer will stop the vmware-vcd service,
   back up any configuration files from the previous release and migrate the
   product configuration as necessary.
   ```

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.

```
Would you like to upgrade now? (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
```

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. Consultez « Démarrage ou arrêt des services vCloud Director », page 32.

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 d'un groupe de serveurs vCloud Director partagent la même base de données, donc quel que soit le nombre de serveurs que vous mettez à niveau, vous ne devez mettre à niveau la base de données qu'une seule fois. Une fois la base de données mise à niveau, les serveurs vCloud Director ne peuvent pas s'y connecter tant qu'ils n'ont pas été, eux aussi, mis à niveau.

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 qu'aucun serveur vCloud Director n'utilise la base de données. Consultez « Utilisation de l'outil de gestion des cellules pour mettre en veille et arrêter un serveur », page 37

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 base de données détecte qu'une version incompatible de vShield Manager est enregistrée dans cette installation de vCloud Director, il affiche ce 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 to vShield Manager version 5.0 or later versions.
```

Reportez-vous à la rubrique « Mise à niveau de vShield Manager », page 49

2 Répondez à l'invite de mise à niveau de la base de données.

```
Welcome to the vCloud Director upgrade utility

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]: y
```

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**.

L'outil de mise à niveau de la base de données s'exécute et affiche des messages de progression.

```
Examining database at URL: jdbc:oracle:thin:@10.26.50.54:1521/orcl
Applying 1 upgrade batches
Executing upgrade batch:
Executing SQL statements from file: cc-tool-uninstall-graceful.sql
.....................................
Executing SQL statements from file: Upgrade.sql []
.....................................
Executing SQL statements from file: Upgrade_Data.sql []
.....................................
Executing SQL statements from file: NewInstall_Indexes.sql []
.....................................
Executing SQL statements from file: Upgrade_UUID.sql []
.....................................
Executing SQL statements from file: NewInstall_Funcs.sql []
```

```
.....................................

Successfully applied upgrade batch:
Running 2 upgrade tasks
Successfully ran upgrade task
Successfully ran upgrade task
Applying 1 upgrade batches
Executing upgrade batch: cleanup
Executing SQL statements from file: NewInstall_Funcs.sql []
.....................................
Executing SQL statements from file: Upgrade_UUID_Clean.sql []
.....................................
Executing SQL statements from file: Upgrade_Clean.sql []
.....................................

Successfully applied upgrade batch: cleanup
Database upgrade complete
++++++++++++++++++++++++++++++++
```

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

Ces étapes sont facultatives et peuvent entraîner de meilleures performances de la base de données après la mise à niveau.

```
Do you wish to rebuild the database indexes? This may take several minutes. [Y/N] y
Rebuilding database indexes

...
Do you wish to update the database statistics? This may take several minutes. [Y/N] y
Updating database statistics
...
```

Une fois la base de données mise à niveau, le script de mise à niveau propose de démarrer des services vCloud Director sur cet 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).
```

Mise à niveau de vShield Manager

Avant de pouvoir effectuer une mise à niveau d'hôtes vCenter et ESX/ESXi enregistrés sur vCloud Director, vous devez mettre à niveau les serveurs vShield Manager joints aux serveurs vCenter.

Avant de mettre à niveau vCenter Server joint à vCloud Director, mettez à niveau le serveur vShield Manager associé à vCenter Server mis à niveau. La mise à niveau de vShield Manager interrompt l'accès aux fonctions administratives de vShield Manager, mais elle n'interrompt pas les services réseau.

Prérequis

Pour que vous puissiez effectuer cette mise à niveau, au moins une cellule dans votre installation de vCloud Director doit être exécutée. La cellule est chargée d'écrire des données sur le serveur vShield Manager mis à niveau dans la base de données de vCloud Director.

Procédure

1 Mettez à niveau vShield Manager.

Suivez la procédure indiquée dans le *Guide de démarrage rapide de vShield*. Une fois la mise à niveau terminée, vShield Manager notifie vCloud Director que sa version a changé. L'envoi de la notification à vCloud Director et son traitement par ce dernier peuvent prendre plusieurs minutes.

2 Une fois la mise à niveau de vShield Manager effectuée, vous devez mettre à niveau tous les vCenter et les hôtes ESX/ESXi avant de mettre à niveau les dispositifs vShield Edge gérés par vShield Manager mis à niveau.

Mise à niveau de vCenter, d'hôtes ESX/ESXi et des dispositifs vShield Edge

Une fois la mise à niveau de vCloud Director et de vShield Manager effectuée, effectuez la mise à niveau des vCenter server et des hôtes ESX/ESXi liés à votre Cloud, puis mettez les dispositifs vShield Edge à niveau sur les vCenter server mis à niveau.

Procédure

1 Mettez à niveau vCenter Server.

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

2 Actualisez l'enregistrement de 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]** .

3 Mettez à niveau chaque hôte ESX/ESXi que vCenter Server mis à niveau prend en charge.

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 vCenter 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 vCenter 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 vCenter pour désactiver le mode maintenance sur l'hôte.

4 Mettez à niveau toutes les dispositifs vShield Edge gérées par vShield Manager sur vCenter Server mis à niveau.

Utilisez l'interface utilisateur de vShield Manager pour gérer cette mise à niveau.

Remarque Si vous utilisez la console Web de vCloud Director ou l'API REST pour réinitialiser un réseau que vShield Edge protège, cette mise à niveau s'effectue automatiquement. Utiliser l'interface utilisateur de vShield Manager pour gérer le dispositif vShield Edge offre un meilleur contrôle administratif sur le processus de mise à niveau et l'interruption de service du réseau qui en résulte.

Modifications de réseaux mis à niveau

Du fait des modifications de l'infrastructure de réseau vCloud Director, les réseaux et les services existants sont parfois modifiés par le processus de mise à niveau. Même si aucune de ces modifications n'affecte les connexions réseau existantes, il peut être nécessaire d'effectuer une reconfiguration après la mise à niveau, pour certains services réseau.

Réseaux d'organisation

Lors de la mise à niveau de vCloud Director vers cette version, les réseaux d'organisation existants sont convertis pour pouvoir utiliser la nouvelle infrastructure de réseau vCloud Director. Vous pourrez constater les modifications suivantes dans vos réseaux d'organisation mis à niveau.

- Les réseaux d'organisation acheminés deviennent des réseaux vDC d'organisation acheminés. Ces réseaux sont connectés à une passerelle Edge dans l'un de vos vDC d'organisation. Des services, tels que la traduction d'adresses réseau et les pare-feux ayant été définis dans le réseau de l'organisation sont maintenant définis dans la passerelle Edge. Si votre organisation dispose de plusieurs vDC, les réseaux vDC d'organisation créés lors d'une mise à niveau sont partagés entre tous les vDC de l'organisation.
- Les réseaux d'organisation isolés deviennent des réseaux vDC d'organisation isolés.
- Les réseaux d'organisation directement connectés ne sont pas modifiés.
- Les nouveaux réseaux vDC d'organisation utilisent le pool de réseaux assigné au vDC d'organisation dans lequel le réseau a été créé.
- Les règles NAT des réseaux d'organisation acheminés sont converties en règles NAT de passerelle Edge. L'effet de chaque règle reste le même, même si la règle est exprimée différemment. Consultez le *Guide de l'administrateur de vCloud Director* pour plus d'informations sur les règles NAT. Les règles NAT des réseaux vApp acheminés ne sont pas modifiées.

Passerelles Edge et réseaux vApp

Les services et les règles de pare-feux ont été modifiés pour permettre une plus grande flexibilité de la configuration des passerelles Edge et des réseaux vApp.

Après une mise à niveau, tous les services de pare-feu des passerelles Edge et des réseaux vApp acheminés s'exécutent en mode de compatibilité, ce qui préserve la sémantique opérationnelle de leurs règles de pare-feu. Après la conversion de règles de pare-feu existantes vers le format actuel, il est possible de mettre les réseaux à niveau afin de s'affranchir des restrictions imposées par le mode de compatibilité. Consultez le *Guide de l'administrateur de vCloud Director* pour plus d'informations sur les règles de pare-feu.

Limitations du réseau en mode de compatibilité

Plusieurs limitations s'appliquent lorsque le système est en mode de compatibilité.

- Chaque passerelle Edge prend en charge une liaison montante et une interface interne, ainsi, il n'existe qu'un seul réseau vDC d'organisation acheminé par passerelle Edge.
- Les règles de pare-feu de la version 5.1 ne peuvent pas être créées dans le cadre d'un service de pare-feu.

Pour supprimer ces limitations, consultez « Reconfigurer les passerelles Edge et les réseaux vApp pour permettre un fonctionnement normal », page 52

Reconfigurer les passerelles Edge et les réseaux vApp pour permettre un fonctionnement normal

Après la conversion de règles de pare-feu existantes vers le format actuel, il est possible de reconfigurer vos passerelles Edge et vos réseaux vApp pour permettre un fonctionnement normal et s'affranchir des restrictions imposées par le mode de compatibilité.

Dans de précédentes versions de vCloud Director, les règles de pare-feu spécifiaient la direction des paquets sujets à la règle. A partir de cette version, la direction du paquet est dérivée des adresses IP source et de destination. Dans l'adresse IP **[Source]** ou **[Destination]** d'une règle de pare-feu, vous pouvez désormais utiliser les mots-clés **`internal`** et **`external`** en plus du mot-clé **`any`** ou d'une adresse IP.

Après une mise à niveau, tous les services de pare-feu des passerelles Edge et des réseaux vApp s'exécutent en mode de compatibilité, ce qui préserve la sémantique opérationnelle de leurs règles de pare-feu. Après la conversion de règles de pare-feu existantes vers le format actuel, il est possible de mettre les réseaux à niveau afin de s'affranchir des restrictions imposées par le mode de compatibilité. Consultez le *Guide de l'administrateur de vCloud Director* pour plus d'informations sur les règles de pare-feu.

Procédure

1 Redéployer toutes les passerelles Edge

Cliquez avec le bouton droit sur chaque passerelle Edge et sélectionnez **[Redéployer]** .

2 Redéployer tous les réseaux vApp.

Cliquez avec le bouton droit sur chaque réseau vApp et sélectionnez **[Réinitialiser le réseau]** .

3 Convertissez toutes les règles de pare-feu de la passerelle Edge au format actuel.

Vous pouvez cliquer sur **[Convertir des règles]** sur l'onglet **[Pare-feu]** de la page **[Service de passerelle]** pour convertir automatiquement la règle. Vous pouvez également convertir les règles manuellement.

a Sur l'onglet **[Pare-feu]** de la page **[Services de passerelle]** , sélectionnez la règle et cliquez sur **[Modifier]** .

b Décochez la case **[Faire correspondre une règle sur l'IP traduit]** .

c Lorsque **`any`** est utilisé pour spécifier une adresse IP **[Source]** ou **[Destination]** , utilisez **`internal`** ou **`external`** à la place.

d Si la règle est destinée à fournir une NAT de destination, changez l'adresse IP **[Destination]** d'**`internal`** en **`external`**.

4 Convertissez toutes les règles de pare-feu de réseau vApp au format actuel.

Vous pouvez cliquer sur **[Convertir des règles]** sur l'onglet **[Pare-feu]** de la page **[Configurer des services]** pour convertir automatiquement la règle. Vous pouvez également convertir les règles manuellement.

a Sur l'onglet **[Pare-feu]** de la page **[Configurer des services]** d'un réseau vApp, sélectionnez la règle et cliquez sur **[Modifier]** .

b Décochez la case **[Faire correspondre une règle sur l'IP traduit]** .

c Lorsque **`any`** est utilisé pour spécifier une adresse IP **[Source]** ou **[Destination]** , utilisez **`internal`** ou **`external`** à la place.

d Si la règle est destinée à fournir une NAT de destination, changez l'adresse IP **[Destination]** d'**`internal`** en **`external`**.

5 Reconfigurez toutes les passerelles Edge pour supprimer toutes les contraintes du mode de compatibilité.

   Sur l'onglet **[Général]** de la page Propriétés de la passerelle Edge, sélectionnez **[Activer le support de plusieurs interfaces]** .

6 Reconfigurez tous les réseaux vApp pour supprimer toutes les contraintes du mode de compatibilité.

   a Cliquez sur l'onglet **[Mon Cloud]** , puis sur **[vApp]** dans le volet gauche.

   b Cliquez avec le bouton droit sur un vApp et sélectionnez **[Ouvrir]** .

   c Sous l'onglet **[Mise en réseau]** , sélectionnez **[Afficher les détails de mise en réseau]** .

   d Cliquez avec le bouton droit sur le réseau vApp et sélectionnez **[Configurer des services]** .

   e Dans l'onglet **[Pare-feu]** , sélectionnez **[Faire correspondre les règles uniquement aux adresses d'origine]**

Configuration de vCloud Director 4

Une fois que vous avez configuré tous les serveurs du groupe de serveurs vCloud Director et les avez 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.

Le processus de configuration crée un dossier dans vCenter pour 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 pour 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 à vCenter et vShield Manager. La console Web vCloud Director doit pouvoir accéder aux installations de vCenter et de vShield 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, 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

Connectez-vous 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.

Index