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

28 mars 2019

VMware Cloud Director 9.7

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

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

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

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

Table des matières

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

Le *Guide d'installation, de configuration et de mise à niveau de vCloud Director* fournit des informations sur l'installation et la mise à niveau du logiciel VMware vCloud Director® for Service Providers, et la configuration pour qu'il fonctionne avec VMware vSphere®, VMware NSX® for vSphere® et VMware NSX-T™ Data Center.

Public cible

Le *Guide d'installation, de configuration et de mise à niveau de vCloud Director* est destiné à toute personne qui souhaite installer ou mettre à niveau le logiciel vCloud Director. Les informations contenues dans ce manuel ont été rédigées à l'attention d'administrateurs système ayant une expérience des systèmes d'exploitation Linux, Windows, des réseaux IP et de vSphere.

Informations mises à jour

Ce *Guide d'installation, de configuration et de mise à niveau de vCloud Director* est mis à jour à chaque nouvelle version du produit ou lorsque cela s'avère nécessaire.

Ce tableau affiche l'historique des mises à jour du *Guide d'installation, de configuration et de mise à niveau de vCloud Director*.

Révision	Description
11 juin 2019	■ Ajout de la rubrique Renouveler les certificats du dispositif vCloud Director. ■ Ajout du chapitre Chapitre 9 Utilisation de la suite d'outils Replication Manager dans une configuration de cluster haute disponibilité.
10 mai 2019	■ Ajout du chapitre #unique_5. ■ Ajout de la section Utilisation de fichiers journaux pour dépanner les mises à jour et les correctifs de vCloud Director. ■ Ajout de la rubrique Échec de la vérification des mises à jour vCloud Director. ■ Ajout de la section Échec de l'installation de la dernière mise à jour de vCloud Director.
5 avril 2019	■ Ajout du chapitre Chapitre 12 Migration vers le dispositif vCloud Director. ■ Ajout de la section Restauration d'un environnement de dispositif vCloud Director avec une configuration de base de données haute disponibilité. ■ Mise à jour de la rubrique Déploiements du dispositif et configuration de la haute disponibilité de la base de données pour améliorer les graphiques et l'étape 2 dans les workflows. ■ Mise à jour de la rubrique Examiner les fichiers journaux dans le dispositif vCloud Director pour ajouter des informations sur le fichier contenant les paramètres OVF du déploiement.
28 mars 2019	Version initiale.

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

1

Vous créez un groupe de serveurs vCloud Director en installant le logiciel vCloud Director sur un ou plusieurs serveurs Linux, ou en déployant une ou plusieurs instances du dispositif vCloud Director. Pendant le processus d'installation, vous effectuez la configuration initiale de vCloud Director, ce qui inclut l'établissement de connexions réseau et de la base de données.

Le logiciel vCloud Director de Linux requiert une base de données externe, tandis que le dispositif vCloud Director utilise une base de données PostgreSQL intégrée.

Après avoir créé le groupe de serveurs vCloud Director, l'installation de vCloud Director s'intègre avec vos ressources vSphere. Pour les ressources de réseau, vCloud Director peut utiliser NSX Data Center for vSphere, NSX-T Data Center ou les deux.

Lorsque vous mettez à niveau une installation existante de vCloud Director, vous mettez à jour le logiciel vCloud Director et le schéma de la base de données, en laissant les relations existantes entre les serveurs, la base de données et vSphere en place.

Lorsque vous migrez une installation vCloud Director existante sur Linux vers le dispositif vCloud Director, vous mettez à jour le logiciel vCloud Director et migrez la base de données vers la base de données intégrée dans le dispositif.

Ce chapitre contient les rubriques suivantes :

Architecture de vCloud Director

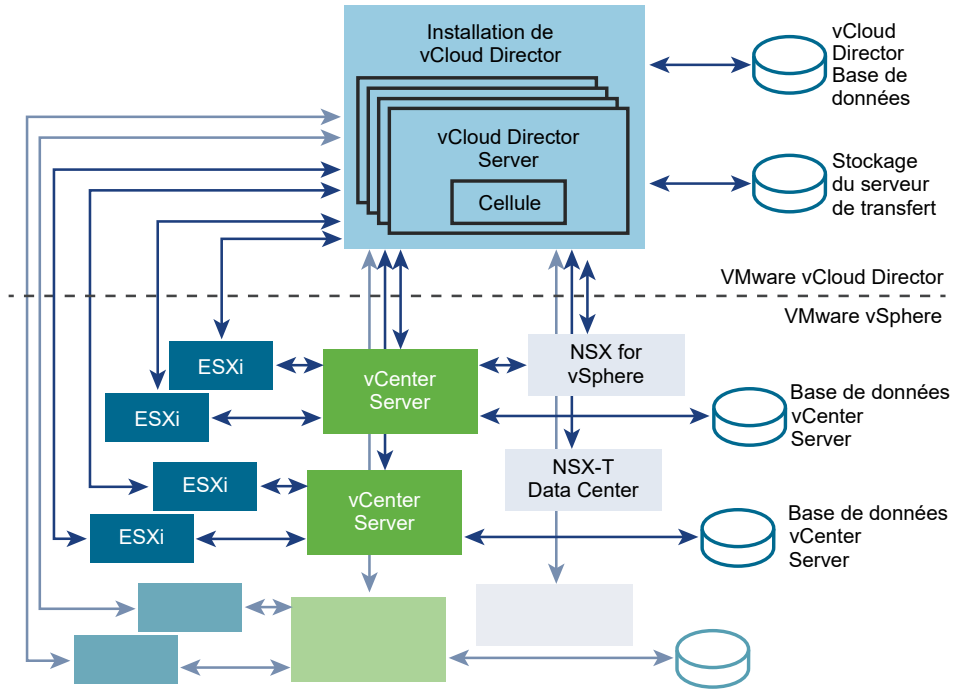
Un groupe de serveurs vCloud Director est composé d'un ou de plusieurs serveurs vCloud Director installés sur Linux ou de déploiements du dispositif vCloud Director. Chaque serveur du groupe exécute un ensemble de services appelé cellule vCloud Director. Toutes les cellules partagent une base de données vCloud Director unique et un stockage de serveur de transfert, et vous connectent aux ressources vSphere et au réseau.

Important Les installations mixtes de vCloud Director sur Linux et les déploiements de dispositifs vCloud Director dans un groupe de serveurs unique ne sont pas pris en charge.

Pour garantir la haute disponibilité de vCloud Director, vous devez installer au moins deux cellules vCloud Director dans un groupe de serveurs. Lorsque vous utilisez un équilibrage de charge de tiers, vous pouvez garantir un basculement automatique sans interruption de service.

Vous pouvez connecter une installation vCloud Director à plusieurs systèmes VMware vCenter Server® et aux hôtes VMware ESXi™ qu'ils gèrent. Pour les services réseau, vCloud Director peut utiliser NSX Data Center for vSphere associé avec vCenter Server ou vous pouvez enregistrer NSX-T Data Center avec vCloud Director. NSX Data Center for vSphere et NSX-T Data Center mixtes sont également pris en charge.

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



Un groupe de serveurs vCloud Director installé sur Linux utilise une base de données externe.

Un groupe de serveurs vCloud Director qui se compose de déploiements de dispositifs utilise la base de données intégrée dans le premier membre du groupe de serveurs. Vous pouvez configurer une haute disponibilité de base de données vCloud Director en déployant deux instances du dispositif en tant que cellules en veille dans le même groupe de serveurs. Reportez-vous à Déploiements du dispositif et configuration de la haute disponibilité de la base de données.

Figure 1-2. Dispositifs vCloud Director comprenant un cluster haute disponibilité de base de données intégrée

Le processus d'installation et de configuration de vCloud Director crée les cellules, les connecte à la base de données partagée et au stockage de serveur de transfert, puis crée le compte d'**administrateur système**. Ensuite, l'**administrateur système** établit des connexions au système vCenter Server, aux hôtes ESXi et aux instances de NSX Manager. Pour plus d'informations sur l'ajout de ressources vSphere et de réseau, reportez-vous à la *Guide de l'administrateur de vCloud Director*.

Planification de la configuration

vSphere fournit des 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 votre Cloud a 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 une cellule vCloud Director à chaque système vCenter Server devant être accessible dans votre Cloud.
- Assurez-vous que tous les serveurs Linux vCloud Director cibles sont conformes à la configuration minimale requise en termes de mémoire et de stockage détaillée dans *Notes de mise à jour de vCloud Director*.
- Si vous prévoyez d'installer vCloud Director sur Linux, configurez la base de données vCloud Director comme décrit dans Préparation de la base de données de vCloud Director.

Configuration matérielle et logicielle requise pour installer vCloud Director

2

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

Compatibilité avec d'autres produits VMware

Pour obtenir les informations les plus récentes sur la compatibilité entre vCloud Director et d'autres produits VMware, reportez-vous à *Matrices d'interopérabilité des produits VMware* à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Configuration requise pour vSphere

Les instances vCenter Server et les hôtes ESXi à utiliser avec vCloud Director doivent avoir une configuration requise spécifique.

- Les réseaux vCenter Server que vous prévoyez d'utiliser en tant que réseaux externes ou pools de réseaux vCloud Director doivent être disponibles pour tous les hôtes de tout cluster devant être utilisés par vCloud Director. Si vous rendez ces réseaux disponibles pour tous les hôtes d'un centre de données, il vous sera plus facile d'ajouter de nouvelles instances vCenter Server à vCloud Director.
- Des vSphere Distributed Switches sont requis pour les réseaux isolés et les pools de réseaux soutenus par NSX Data Center for vSphere.
- Les clusters vCenter Server utilisés avec vCloud Director doivent spécifier le niveau d'automatisation vSphere DRS **Entièrement automatisé**. Storage DRS, s'il est activé, peut être configuré avec n'importe quel niveau d'automatisation.
- Les instances vCenter Server doivent approuver leurs hôtes. Tous les hôtes dans tous les clusters gérés par vCloud Director doivent être configurés pour nécessiter des certificats d'hôte vérifiés. Vous devez en particulier déterminer, comparer et sélectionner des empreintes correspondantes pour tous les hôtes. Consultez la section Configurer les paramètres SSL dans la documentation *vCenter Server et gestion des hôtes*.

Configuration requise de licence vSphere

vCloud Director Service Provider Bundle inclut les licences vSphere nécessaires.

Plates-formes, bases de données et navigateurs pris en charge

Reportez-vous aux *Notes de mise à jour de vCloud Director 9.7* pour obtenir des informations sur les plates-formes de serveurs, les navigateurs, les serveurs LDAP et les bases de données pris en charge par cette version de vCloud Director.

Configuration requise de l'espace disque, de la mémoire et du CPU

La configuration physique requise, telle que l'espace disque, la mémoire et le CPU pour les cellules vCloud Director est répertoriée dans les *Notes de mise à jour de vCloud Director 9.7*.

Stockage partagé

NFS ou autre volume de stockage partagé pour le service de transfert vCloud Director. Le volume de stockage doit être extensible et accessible à tous les serveurs du groupe de serveurs.

Ce chapitre contient les rubriques suivantes :

Configuration réseau requise pour vCloud Director

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

Le réseau qui connecte les serveurs vCloud Director, le serveur de base de données, les systèmes vCenter Server et les composants NSX, doit respecter plusieurs conditions requises :

Adresses IP

Chaque serveur vCloud Director doit prendre en charge deux points de terminaison SSL distincts. Un point de terminaison est destiné au service HTTP. L'autre point de terminaison est destiné au service de proxy de console. Ces points de terminaison peuvent être des adresses IP distinctes ou une adresse IP unique avec deux ports distincts. Vous pouvez utiliser des alias IP ou plusieurs interfaces réseau pour créer ces adresses. N'utilisez pas la commande Linux `ip addr add` pour créer la seconde adresse.

Le dispositif vCloud Director utilise son adresse IP `eth0` avec le port personnalisé 8443 pour le service de proxy de console.

Adresse du proxy de la console

L'adresse IP configurée en tant que point de terminaison 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.

Pour une installation avec une adresse IP unique, vous pouvez personnaliser l'adresse proxy de console à partir de la console Web vCloud Director. Par exemple, pour le dispositif vCloud Director, vous devez personnaliser l'adresse proxy de console sur *vcloud.example.com*:8443.

Service d'heure réseau

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

Fuseaux horaire des serveurs

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

Résolution du nom d'hôte

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

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

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

```
nslookup 192.168.1.1
```

La recherche DNS inversée de l'adresse IP `eth0` est requise pour le dispositif. La commande suivante doit réussir dans votre environnement:

```
host –W 15 –R 1 –T <eth0–IP–address>
```

Configuration requise pour la sécurité réseau

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

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

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

  Tableau 2-1. Ports qui doivent autoriser les paquets entrants provenant des hôtes vCloud Director

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

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

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

Port	Protocole	Commentaires
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	Mappeur de port NFS utilisé par le service de transfert
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	Connexions vCenter, NSX Manager et ESXi utilisant le port standard. Si vous avez choisi un port différent pour ces services, désactivez la connexion au port 443 et activez la connexion vers ce port.
514	UDP	Facultatif. Active l'utilisation de syslog.
902	TCP	Connexions vCenter et ESXi.
903	TCP	Connexions vCenter et ESXi.

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

Port	Protocole	Commentaires
920	TCP, UDP	NFS rpc.statd utilisé par le service de transfert.
1433	TCP	Port de base de données Microsoft SQL Server par défaut.
5672	TCP, UDP	Facultatif. Messages AMQP des extensions de tâche.
61611	TCP	AMQP
61616	TCP	AMQP

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

Avant l'installation de vCloud Director ou le déploiement du dispositif vCloud Director

3

Avant d'installer vCloud Director sur un serveur Linux ou de déployer le dispositif vCloud Director, vous devez préparer votre environnement.

Ce chapitre contient les rubriques suivantes :

- Préparation de la base de données de vCloud Director
- Préparation du stockage du serveur de transfert
- Téléchargement et installation de la clé publique VMware
- Installer et configurer NSX Data Center for vSphere pour vCloud Director
- Installer et configurer NSX-T Data Center pour vCloud Director

Préparation de la base de données de vCloud Director

Les cellules de vCloud Director utilisent une base de données pour stocker les informations partagées. Avant d'installer vCloud Director sous Linux, vous devez installer et configurer une base de données vCloud Director externe. Le dispositif vCloud Director utilise une base de données PostgreSQL intégrée.

Pour plus d'informations sur les bases de données vCloud Director prises en charge, consultez les Matrices d'interopérabilité des produits VMware.

Quel que soit le logiciel de base de données que vous décidez d'utiliser, vous devez créer un schéma de la base de données séparé et dédié qui sera utilisé par vCloud Director. vCloud Director ne peut pas partager un schéma de la base de données avec un autre produit VMware.

Important vCloud Director prend uniquement en charge les connexions SSL à une base de données PostgreSQL. Vous pouvez activer SSL sur la base de données PostgreSQL lors d'une configuration sans surveillance des connexions au réseau et à la base de données ou après avoir créé le groupe de serveurs vCloud Director. Reportez-vous à Référence de configuration sans surveillance et Effectuer des configurations supplémentaires sur la base de données PostgreSQL externe.

Configurer une base de données PostgreSQL externe pour vCloud Director sous Linux

Les bases de données PostgreSQL doivent répondre à des exigences de configuration spécifiques pour les utiliser avec vCloud Director. Avant d'installer vCloud Directorsur Linux, vous devez installer et configurer une instance de base de données et créer le compte d'utilisateur de base de données vCloud Director.

Note Seul vCloud Director sous Linux utilise une base de données externe. Le dispositif vCloud Director utilise la base de données PostgreSQL intégrée.

Conditions préalables

Vous devez bien maîtriser les commandes, l'exécution des scripts et les opérations de PostgreSQL.

Procédure

1. Configurez le serveur de base de données.

   Un serveur de base de données avec 16 Go de mémoire, 100 Go de stockage et 4 CPU est approprié pour les groupes de serveurs vCloud Director classiques.

2. Installez une distribution prise en charge de PostgreSQL sur le serveur de base de données.

   - La valeur `SERVER_ENCODING` de la base de données doit être `UTF-8`. Cette valeur est établie lorsque vous installez la base de données et correspond toujours au codage utilisé par le système d'exploitation du serveur de base de données.
   - Utilisez la commande PostgreSQL `initdb` pour définir la valeur de `LC_COLLATE` et `LC_CTYPE` sur `en_US.UTF-8`. Par exemple :

     ```
     initdb --locale=en_US.UTF-8
     ```

3. Créez l'utilisateur de la base de données.

   La commande suivante crée l'utilisateur `vcloud`.

   ```
   create user vcloud;
   ```

4. Créez l'instance de base de données et attribuez-lui un propriétaire.

   Utilisez une commande semblable à celle-ci pour spécifier un utilisateur de base de données nommé `vcloud` en tant que propriétaire de la base de données.

   ```
   create database vcloud owner vcloud;
   ```

5 Attribuez un mot de passe de base de données au compte du propriétaire de la base de données.

   La commande suivante attribue le mot de passe `vcloudpass` au propriétaire de la base de données `vcloud`.

```
alter user vcloud password 'vcloudpass';
```

6 Autorisez le propriétaire de la base de données à se connecter à la base de données.

   La commande suivante attribue l'option `login` au propriétaire de la base de données `vcloud`.

```
alter role vcloud with login;
```

Étape suivante

Après avoir créé le groupe de serveurs vCloud Director, vous pouvez configurer la base de données PostgreSQL pour exiger des connexions SSL à partir des cellules vCloud Director et ajuster certains paramètres de base de données pour des performances optimales. Reportez-vous à Effectuer des configurations supplémentaires sur la base de données PostgreSQL externe.

Configurer une base de données Microsoft SQL Server externe pour vCloud Director pour Linux

Les bases de données SQL Server doivent répondre à des exigences de configuration spécifiques en vue de les utiliser avec vCloud Director. Avant d'installer vCloud Directorsur Linux, vous devez installer et configurer une instance de base de données et créer le compte d'utilisateur de base de données 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.

Note Seul vCloud Director sous Linux utilise une base de données externe. Le dispositif vCloud Director utilise la base de données PostgreSQL intégrée.

Conditions préalables

- 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.
- Consultez l'article de la base de connaissances VMware https://kb.vmware.com/kb/2148767 pour plus d'informations sur l'utilisation des groupes de disponibilité AlwaysOn de Microsoft SQL Server avec la base de données 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 groupes de serveurs 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
```

Préparation du stockage du serveur de transfert

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

Important Le dispositif vCloud Director prend en charge uniquement le type de stockage partagé NFS. Le processus de déploiement du dispositif implique le montage du stockage du serveur de transfert partagé NFS.

Lorsque NFS est utilisé pour le stockage du serveur de transfert, vous devez configurer chaque cellule vCloud Director dans le groupe de serveurs vCloud Director pour monter et utiliser le stockage du serveur de transfert basé sur NFS. Vous avez besoin d'autorisations d'utilisateur et de groupe spécifiques pour configurer chaque cellule pour monter l'emplacement basé sur NFS et l'utiliser comme stockage de serveur de transfert.

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

- Au cours des transferts, les envois et téléchargements occupent ce stockage. Lorsque le transfert est terminé, les envois et téléchargements sont supprimés du stockage. Les transferts qui ne progressent pas pendant 60 minutes sont marqués comme étant expirés et sont effacés du système. Étant donné que les images transférées peuvent être volumineuses, il est conseillé d'allouer au moins plusieurs centaines de giga-octets à ce type d'opération.
- Les éléments de catalogues qui sont publiés en externe et pour lesquels la mise en cache du contenu publié est activée, occupent ce stockage. Les éléments de catalogues qui sont publiés en externe, mais qui ne permettent pas la mise en cache, n'occupent pas ce stockage. Si vous activez des organisations dans votre cloud pour créer des catalogues qui sont publiés en externe, vous pouvez en déduire que des centaines, voire des milliers d'éléments de catalogue nécessitent un espace sur ce volume. La taille de chaque élément du catalogue est de la taille d'une machine virtuelle dans un format OVF compressé.

Note Le volume du stockage du serveur de transfert doit avoir une capacité pour permettre une future expansion.

Comment vCloud Director utilise les autorisations du système de fichiers sur l'emplacement de stockage du serveur de transfert

Pour toutes les cellules vCloud Director dans le groupe de serveurs vCloud Director :

- Dans les opérations de cloud standard telles que le téléchargement d'éléments dans le catalogue, le démon de la cellule vCloud Director écrit les fichiers dans le stockage du serveur de transfert et les lit dans ce stockage à l'aide de l'utilisateur **vcloud** du groupe **vcloud**. L'utilisateur **vcloud** écrit les fichiers avec `umask 0077`. Lorsque le programme d'installation de vCloud Director exécute et installe le logiciel vCloud Director sur un membre du groupe de serveurs, il crée également l'utilisateur **vcloud** et le groupe **vcloud**.
- Le script `vmware-vcd-support` du collecteur de données du journal vCloud Director peut collecter les journaux de toutes vos cellules vCloud Director en une seule opération et regrouper les journaux dans le fichier `tar.gz`. Lorsque vous exécutez le script, il écrit le fichier `tar.gz` qui en résulte dans un répertoire de l'emplacement de stockage du serveur de transfert en utilisant l'ID d'utilisateur de l'utilisateur qui appelle le script. Par défaut, le seul utilisateur autorisé à exécuter le script est l'utilisateur **racine**.
- L'utilisateur **racine** sur la cellule exécute le script qui écrit le fichier `tar.gz` dans le répertoire `vmware-vcd-support` de l'emplacement de stockage du serveur de transfert. Si vous souhaitez utiliser les options à cellules multiples pour collecter les journaux de toutes les cellules à la fois, l'utilisateur **racine** doit disposer d'une autorisation de lecture pour récupérer le bundle de journaux de diagnostics `tar.gz`.

Exigences pour la configuration du serveur NFS

Il existe des exigences spécifiques pour la configuration du serveur NFS, afin que vCloud Director puisse écrire des fichiers dans un emplacement de stockage de serveur de transfert NFS et y lire des fichiers. En raison de ces exigences, l'utilisateur **vcloud** peut effectuer les opérations de cloud standard et l'utilisateur **racine** peut effectuer une collecte de journaux à plusieurs cellules.

- La liste d'exportation pour le serveur NFS doit permettre à chaque membre du serveur de votre groupe de serveurs vCloud Director d'accéder en lecture-écriture à l'emplacement partagé qui est identifié dans la liste d'exportation. Cette capacité permet à l'utilisateur **vcloud** d'écrire des fichiers dans l'emplacement partagé et d'y lire ces mêmes fichiers.
- Le serveur NFS doit autoriser l'accès en lecture et en écriture à l'emplacement partagé par le compte système **racine** sur chaque serveur de votre groupe de serveurs vCloud Director. Cette capacité permet de collecter les journaux de toutes les cellules à la fois dans un seul bundle à l'aide du script `vmware-vcd-support` avec ses options à cellules multiples. Vous pouvez répondre à ces exigences en utilisant `no_root_squash` dans la configuration d'exportation NFS pour cet emplacement partagé.

Par exemple, si le serveur NFS dispose de l'adresse IP 192.168.120.7 et d'un répertoire nommé vCDspace comme espace de transfert pour le groupe de serveurs vCloud Director avec l'emplacement `/nfs/vCDspace`, vous devez vous assurer que sa propriété et ses autorisations sont **root:root** et **750** pour pouvoir exporter ce répertoire. La méthode pour autoriser l'accès en lecture-écriture à l'emplacement partagé pour deux cellules nommées vcd-cell1-IP et vcd-cell2-IP est la méthode `no_root_squash`. Vous devez ajouter une ligne au fichier `/etc/exports`.

```
192.168.120.7/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
vCD_Cell2_IP_Address(rw,sync,no_subtree_check)
```

Il ne doit y avoir aucun espace entre chaque adresse IP de cellule et sa parenthèse immédiatement à gauche dans la ligne d'exportation. Si le serveur NFS redémarre alors que les cellules écrivent des données dans l'emplacement partagé, l'utilisation de l'option `sync` dans la configuration d'exportation empêche l'endommagement des données dans l'emplacement partagé. L'utilisation de l'option `no_subtree_check` dans la configuration d'exportation améliore la fiabilité lorsqu'un sous-répertoire d'un système de fichiers est exporté.

Chaque serveur du groupe de serveurs vCloud Director doit être autorisé à monter le partage NFS en inspectant la liste d'exportation pour l'exportation NFS. Vous exportez le montage en exécutant `exportfs -a` pour exporter de nouveau tous les partages NFS. Les démons NFS `rpcinfo -p localhost` ou `service nfs status` doivent être en cours d'exécution sur le serveur.

Éléments à prendre en compte lors de la planification de la mise à niveau de votre installation vCloud Director vers une version ultérieure

Lors de la mise à niveau d'un groupe de serveurs vCloud Director, vous exécutez le fichier d'installation de la version mise à niveau pour mettre à niveau tous les membres du groupe de serveurs vCloud Director. Pour des raisons de commodité, certaines organisations choisissent de télécharger le fichier d'installation pour la mise à niveau vers l'emplacement de stockage du serveur de transfert et de l'exécuter à partir de là, car toutes les cellules ont accès à cet emplacement. Comme l'utilisateur **racine** doit être utilisé pour exécuter le fichier d'installation de mise à niveau, si vous souhaitez utiliser l'emplacement de stockage du serveur de transfert pour exécuter une mise à niveau, vous devez vous assurer que l'utilisateur **racine** peut exécuter le fichier d'installation de mise à niveau lorsque vous effectuez la mise à niveau. Si vous ne pouvez pas exécuter la mise à niveau en tant qu'utilisateur **racine** , le fichier doit être copié dans un autre emplacement où il peut être exécuté en tant qu'utilisateur **racine**. Par exemple, un autre répertoire à l'extérieur du montage NFS.

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.

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

Procédure

1. Créez un répertoire pour stocker les clés publiques VMware.
2. Utilisez un navigateur Web pour télécharger toutes les clés publiques de l'offre publique VMware depuis le répertoire http://packages.vmware.com/tools/keys.
3. Enregistrez les fichiers des clés dans le répertoire que vous avez créé.
4. Pour chaque clé que vous téléchargez, exécutez la commande suivante pour l'importer.

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

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

key_name est le nom de fichier d'une clé.

Installer et configurer NSX Data Center for vSphere pour vCloud Director

Si vous planifiez l'installation de vCloud Director pour utiliser les ressources réseau de NSX Data Center for vSphere, vous devez installer et configurer NSX Data Center for vSphere et associer une instance NSX Manager unique à chaque instance de vCenter Server que vous prévoyez d'inclure dans votre installation vCloud Director.

NSX Manager est inclus dans le téléchargement de NSX Data Center for vSphere. Pour obtenir les informations les plus récentes sur la compatibilité entre vCloud Director et d'autres produits VMware, reportez-vous à *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 conditions de réseau requises, consultez Configuration réseau requise pour vCloud Director.

Important Cette procédure ne s'applique que dans le cas d'une nouvelle installation de vCloud Director. Si vous mettez à niveau une installation de vCloud Director existante, consultez Chapitre 11 Mise à niveau de vCloud Director et application de correctifs au dispositif vCloud Director.

Conditions préalables

Vérifiez que chacun de vos systèmes vCenter Server respecte les conditions préalables pour l'installation de NSX Manager.

Procédure

1. Effectuez la tâche d'installation pour le dispositif virtuel NSX Manager.

   Reportez-vous au *Guide d'installation de NSX*.

2. Connectez-vous au dispositif virtuel de NSX Manager que vous avez installé et confirmez les paramètres spécifiés lors de l'installation.

3. Associez le dispositif virtuel de NSX Manager que vous avez installé au système vCenter Server que vous envisagez d'ajouter à vCloud Director dans votre installation de vCloud Director.

4. Configurez le support VXLAN dans les instances NSX Manager associées.

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

5 (Facultatif) Si vous souhaitez que les passerelles Edge du système fournissent un routage distribué, configurez un cluster de NSX Controller.

Reportez-vous au *Guide d'administration de NSX*.

Installer et configurer NSX-T Data Center pour vCloud Director

Si vous planifiez l'installation de vCloud Director pour utiliser les ressources réseau de NSX-T Data Center, vous devez installer et configurer NSX-T Data Center avec au moins une instance de NSX-T Manager.

NSX-T Manager est inclus dans le téléchargement de NSX-T Data Center. Pour obtenir les informations les plus récentes sur la compatibilité entre vCloud Director et d'autres produits VMware, reportez-vous à *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 conditions de réseau requises, consultez Configuration réseau requise pour vCloud Director.

Important Cette procédure ne s'applique que dans le cas d'une nouvelle installation de vCloud Director. Si vous mettez à niveau une installation de vCloud Director existante, consultez Chapitre 11 Mise à niveau de vCloud Director et application de correctifs au dispositif vCloud Director.

Conditions préalables

Vous devez être familiarisé avec NSX-T Data Center.

Procédure

1 Installez le dispositif virtuel NSX-T Manager.

Reportez-vous au *Guide d'installation de NSX-T*.

2 Préparez les hôtes ESXi que vous souhaitez utiliser avec NSX-T Data Center.

Reportez-vous au *Guide d'installation de NSX-T*.

3 Créez des nœuds de transport et des zones de transport pour votre configuration requise de cloud.

Reportez-vous au *Guide d'installation de NSX-T*.

4 Configurez les clusters et les nœuds Edge.

Reportez-vous au *Guide d'installation de NSX-T*.

5 Configurez les routeurs de niveau 0 et de niveau 1.

Reportez-vous au *Guide d'administration de NSX-T*.

6 Configurez un ou plusieurs VLAN ou commutateurs logiques de superposition que vous souhaitez importer dans votre installation vCloud Director.

Reportez-vous au *Guide d'administration de NSX-T*.

Étape suivante

Après avoir installé vCloud Director, vous pouvez enregistrer l'instance de NSX-T Manager dans votre cloud. Pour plus d'informations sur l'enregistrement d'une instance de NSX-T Manager, consultez le *Guide de programmation de vCloud API pour fournisseurs de services*.

Création et gestion de certificats SSL pour vCloud Director sous Linux

4

vCloud Director utilise SSL pour sécuriser les communications entre les clients et les serveurs. Chaque serveur vCloud Director doit prendre en charge deux points de terminaison SSL différents : un pour les communications HTTPS et un pour les communications de proxy de la console.

Ces points de terminaison peuvent être des adresses IP distinctes ou une adresse IP unique disposant de ports distincts. Chaque point de terminaison requiert son propre certificat SSL. Vous pouvez utiliser le même certificat pour les deux points de terminaison, par exemple, en utilisant un certificat de caractère générique.

Ce chapitre contient les rubriques suivantes :

Avant de créer des certificats SSL pour vCloud Director sur Linux

Lorsque vous installez vCloud Director pour Linux, vous devez créer deux certificats pour chaque membre du groupe de serveurs et importer les certificats dans des keystores hôtes.

Note Vous devez créer les certificats pour les membres du groupe de serveurs uniquement après l'installation de vCloud Director sous Linux. Le dispositif vCloud Director crée des certificats SSL auto-signés lors de son premier démarrage.

Procédure

1. Connectez-vous au serveur vCloud Director en tant qu'utilisateur **racine**.
2. Répertoriez les adresses IP pour le serveur.

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

3 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
```

4 Notez chaque adresse IP et le nom de domaine complet qui lui est associé. Si vous n'utilisez pas une adresse IP unique pour les deux services, choisissez l'adresse IP du service HTTPS et l'adresse IP du service de proxy de la console.

   Vous devez fournir les noms de domaine complets pour créer les certificats et les adresses IP pour configurer les connexions au réseau et à la base de données. Notez les autres noms de domaine complets pouvant atteindre l'adresse IP, car vous devrez les fournir si vous souhaitez que le certificat inclue un nom de remplacement du sujet.

Étape suivante

Créez les certificats pour les deux points de terminaison. Vous pouvez utiliser des certificats signés par une autorité de certification de confiance ou des certificats auto-signés.

Note Les certificats signés par une autorité de certification offrent le niveau de confiance le plus élevé.

- Pour plus d'informations sur la création et l'importation de certificats SSL signés par une autorité de certification, consultez Créer un keystore de certificats SSL signés par une autorité de certification pour vCloud Director sous Linux.
- Pour plus d'informations sur la création de certificats SSL auto-signés, reportez-vous à la section Créer des certificats SSL auto-signés pour vCloud Director sous Linux.
- Pour plus d'informations sur l'importation de votre propre clé privée et de fichiers de certificats signés par une autorité de certification, consultez Créer un keystore de certificats SSL signé par une autorité de certification avec des clés privées importées pour vCloud Director sous Linux.

Créer des certificats SSL auto-signés pour vCloud Director sous Linux

Les certificats auto-signés 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 dans un fichier de keystore JCEKS, l'un pour le service HTTPS et l'autre pour le service de proxy de la console.

Vous pouvez utiliser `cell-management-tool` pour créer les certificats SSL auto-signés. L'utilitaire `cell-management-tool` est installé sur la cellule avant l'exécution de l'agent de configuration et après l'exécution du fichier d'installation. Reportez-vous à la section Installez vCloud Director sur le premier membre d'un groupe de serveurs.

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

Procédure

1. Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation du serveur vCloud Director en tant que **racine**.
2. Exécutez la commande pour créer une paire de clés publique et privée pour le service HTTPS et pour le service de proxy de la console.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w passwd
   ```

   La commande crée ou met à jour un keystore dans `certificates.ks` ayant le mot de passe `passwd`. L'outil `cell-management-tool` crée les certificats à l'aide des valeurs par défaut de la commande. Selon la configuration DNS de votre environnement, le nom commun de l'émetteur est défini sur l'adresse IP ou le nom de domaine complet de chaque service. Le certificat utilise la clé 2 048 bits par défaut et expire un an après sa création.

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

Étape suivante

Notez le nom du chemin du magasin d'accès au keystore. Vous avez besoin du nom de chemin d'accès au keystore lorsque vous exécutez le script de configuration pour créer les connexions réseau et de base de données pour la cellule vCloud Director. Reportez-vous à Configuration des connexions au réseau et à la base de données.

Créer un keystore de certificats SSL signés par une autorité de certification pour vCloud Director sous Linux

La création et l'importation de certificats signés par une autorité de certification offrent le niveau de confiance le plus élevé pour les communications SSL et vous aident à sécuriser les connexions de votre infrastructure cloud.

Chaque serveur vCloud Director nécessite deux certificats SSL pour sécuriser les communications entre les clients et les serveurs. Chaque serveur vCloud Director doit prendre en charge deux points de terminaison SSL différents : un pour les communications HTTPS et un pour les communications de proxy de la console.

Ces points de terminaison peuvent être des adresses IP distinctes ou une adresse IP unique disposant de deux ports distincts. Chaque point de terminaison requiert son propre certificat SSL. Vous pouvez utiliser le même certificat pour les deux points de terminaison, par exemple, en utilisant un certificat de caractère générique.

Les certificats pour ces deux points de terminaison doivent inclure un nom distinct X.500 et une extension de nom alternatif d'objet X.509.

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

Vous pouvez utiliser `cell-management-tool` pour créer les certificats SSL auto-signés. L'utilitaire `cell-management-tool` est installé sur la cellule avant l'exécution de l'agent de configuration et après l'exécution du fichier d'installation. Reportez-vous à la section Installez vCloud Director sur le premier membre d'un groupe de serveurs.

Si vous disposez déjà de votre propre clé privée et de fichiers de certificats signés par une autorité de certification, suivez la procédure décrite dans Créer un keystore de certificats SSL signé par une autorité de certification avec des clés privées importées pour vCloud Director sous Linux.

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

Conditions préalables

- Vérifiez que vous avez accès à un ordinateur sur lequel un environnement d'exécution Java version 8 ou version ultérieure est installé, afin de pouvoir importer les certificats 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. L'utilisation de certificats créés avec `keytool` provenant de toute autre source n'est pas prise en charge par vCloud Director. Les exemples de ligne de commande suivants supposent que `keytool` réside dans le chemin d'accès de l'utilisateur.
- Familiarisez-vous avec la commande `keytool`.
- Pour plus d'informations sur les options disponibles pour la commande `generate-certs`, consultez Génération de certificats auto-signés pour les points de terminaison HTTPS et de proxy de console.

- Pour plus d'informations sur les options disponibles pour la commande `certificates`, reportez-vous à la section Remplacement de certificats pour les points de terminaison HTTP et de proxy de console.

Procédure

1. Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation du serveur vCloud Director en tant qu'utilisateur **racine**.
2. Exécutez la commande pour créer une paire de clés publique et privée pour le service HTTPS et pour le service de proxy de la console.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w keystore_password
   ```

   La commande crée ou met à jour un keystore dans `certificates.ks` avec le mot de passe spécifié. Les certificats sont créés à l'aide des valeurs par défaut de la commande. Selon la configuration DNS de votre environnement, le nom commun de l'émetteur est défini sur l'adresse IP ou le nom de domaine complet de chaque service. Le certificat utilise la clé 2 048 bits par défaut et expire un an après sa création.

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

3. Créez une demande de signature de certificat pour le service HTTPS et pour le service de proxy de la console.

   Important Si vous utilisez des adresses IP distinctes pour le service HTTPS et pour le service de proxy de la console, ajustez les noms d'hôte et les adresses IP dans les commandes suivantes.

   a. Créez une demande de signature de certificat dans le fichier `http.csr`.

      ```
      keytool -keystore certificates.ks -storetype JCEKS -storepass keystore_password -certreq -alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
      ```

   b. Créez une demande de signature de certificat dans le fichier `consoleproxy.csr`.

      ```
      keytool -keystore certificates.ks -storetype JCEKS -storepass keystore_password -certreq -alias consoleproxy -file consoleproxy.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
      ```

4. 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.

   Vous obtenez les certificats signés par une autorité de certification.

5 Importez les certificats signés dans le keystore JCEKS.

a Importez le certificat racine de l'autorité de certification à partir du fichier `root.cer` dans le fichier keystore `certificates.ks`.

```
keytool –import –storetype JCEKS –storepass keystore_password –keystore certificates.ks –
alias root –file root_certificate_file
```

b Si vous recevez des certificats intermédiaires, importez-les du fichier `intermediate.cer` dans le fichier keystore `certificates.ks`.

```
keytool –import –storetype JCEKS –storepass keystore_password –keystore certificates.ks –
alias intermediate –file intermediate_certificate_file
```

c Importez le certificat du service HTTPS.

```
keytool –import –storetype JCEKS –storepass keystore_password –keystore certificates.ks –
alias http –file http_certificate_file
```

d Importez le certificat du service de proxy de la console.

```
keytool –import –storetype JCEKS –storepass keystore_password –keystore certificates.ks –
alias consoleproxy –file console_proxy_certificate_file
```

Les commandes remplacent le fichier `certificates.ks` par les versions signées par une autorité de certification récemment acquises.

6 Pour vérifier si les certificats sont importés vers le keystore JCEKS, exécutez la commande pour répertorier le contenu du fichier keystore.

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

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

Étape suivante

- Si vous n'avez pas encore configuré votre instance de vCloud Director, exécutez le script `configure` pour importer le keystore des certificats dans vCloud Director. Reportez-vous à Configuration des connexions au réseau et à la base de données.

  Note 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 avez besoin du nom du chemin d'accès au keystore lorsque vous exécuterez le script de configuration.

- Si vous avez déjà installé et configuré votre instance de vCloud Director, utilisez la commande `certificates` de l'outil de gestion des cellules pour importer le keystore des certificats. Reportez-vous à la section Remplacement des certificats pour les points de terminaison HTTP et de proxy de console.

Créer un keystore de certificats SSL signé par une autorité de certification avec des clés privées importées pour vCloud Director sous Linux

Si vous disposez de votre propre clé privée et de fichiers de certificats signés par une autorité de certification, vous devez créer des fichiers keystore dans lesquels importer les certificats et les clés privées pour le service HTTPS et le service de proxy de la console avant d'importer les keystores dans votre environnement vCloud Director.

Conditions préalables

- Reportez-vous à la section Avant de créer des certificats SSL pour vCloud Director sur Linux.
- Vérifiez que vous avez accès à un ordinateur sur lequel un environnement d'exécution Java version 8 ou version ultérieure est installé, afin de pouvoir importer les certificats 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. L'utilisation de certificats créés avec `keytool` provenant de toute autre source n'est pas prise en charge par vCloud Director. Les exemples de ligne de commande suivants supposent que `keytool` réside dans le chemin d'accès de l'utilisateur.
- Familiarisez-vous avec la commande `keytool`.
- Téléchargez et installez OpenSSL.
- Pour plus d'informations sur les options disponibles pour la commande `certificates`, reportez-vous à la section Remplacement de certificats pour les points de terminaison HTTP et de proxy de console.

Procédure

1. Si vous disposez de certificats intermédiaires, exécutez la commande pour combiner le certificat racine signé par une autorité de certification avec les certificats intermédiaires et créer une chaîne de certificats.

   ```
   cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
   ```

2 Utilisez OpenSSL pour créer des fichiers keystore PKCS12 intermédiaires pour les services HTTPS et le service de proxy de la console avec la clé privée, la chaîne de certificats et l'alias respectif, et spécifiez un mot de passe pour chaque fichier keystore.

   a Créez le fichier keystore pour le service HTTPS.

   ```
   openssl pkcs12 –export –in http.crt –inkey http.key –CAfile chain.crt –name http –passout pass:keystore_password –out http.pfx –chain
   ```

   b Créez le fichier keystore pour le service de proxy de la console.

   ```
   openssl pkcs12 –export –in consoleproxy.crt –inkey consoleproxy.key –CAfile chain.crt –name consoleproxy –passout pass:keystore_password –out consoleproxy.pfx -chain
   ```

3 Utilisez `keytool` pour importer les keystores PKCS12 dans le keystore JCEKS.

   a Exécutez la commande pour importer le keystore PKCS12 du service HTTPS.

   ```
   keytool –importkeystore –deststorepass keystore_password –destkeystore certificates.ks –deststoretype JCEKS –srckeystore http.pfx –srcstoretype PKCS12 –srcstorepass keystore_password
   ```

   b Exécutez la commande pour importer le keystore PKCS12 pour le service de proxy de console.

   ```
   keytool –importkeystore –deststorepass keystore_password –destkeystore certificates.ks –deststoretype JCEKS –srckeystore consoleproxy.pfx –srcstoretype PKCS12 –srcstorepass keystore_password
   ```

4 Pour vérifier si les certificats sont importés vers le keystore JCEKS, exécutez la commande pour répertorier le contenu du fichier keystore.

   ```
   keytool –storetype JCEKS –storepass keystore_password –keystore certificates.ks -list
   ```

5 Reprenez cette procédure pour toutes les cellules de vCloud Director dans votre environnement.

Étape suivante

- Si vous n'avez pas encore configuré votre instance de vCloud Director, exécutez le script `configure` pour importer le keystore des certificats dans vCloud Director. Reportez-vous à Configuration des connexions au réseau et à la base de données.

  Note 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 le fichier keystore sur ce serveur. Vous avez besoin du nom du chemin d'accès au keystore lorsque vous exécuterez le script de configuration.

- Si vous avez déjà installé et configuré votre instance de vCloud Director, utilisez la commande `certificates` de l'outil de gestion des cellules pour importer le keystore des certificats. Reportez-vous à la section Remplacement des certificats pour les points de terminaison HTTP et de proxy de console.

Installer vCloud Director sous Linux

5

Vous pouvez créer un groupe de serveurs vCloud Director en installant le logiciel vCloud Director pour un ou plusieurs serveurs Linux. Cette installation et cette configuration sur le premier membre du groupe créent un fichier de réponses que vous utilisez pour configurer les autres membres du groupe.

Cette procédure est uniquement destinée à de nouvelles installations. Si vous mettez à niveau une installation de vCloud Director existante, consultez Chapitre 11 Mise à niveau de vCloud Director et application de correctifs au dispositif vCloud Director.

Important Les installations mixtes de vCloud Director sur Linux et les déploiements de dispositifs vCloud Director dans un groupe de serveurs unique ne sont pas pris en charge.

Conditions préalables

- Vérifiez que les serveurs cible pour votre groupe de serveurs respectent les Chapitre 2 Configuration matérielle et logicielle requise pour installer vCloud Director.
- Vérifiez que vous avez créé un certificat SSL pour chaque point de terminaison des serveurs cible pour votre groupe de serveurs. Tous les répertoires du chemin d'accès vers les certificats SSL doivent être lisibles par n'importe quel utilisateur. L'utilisation d'un même chemin de keystore sur tous les membres d'un groupe de serveurs simplifie l'installation (par exemple, `/tmp/certificates.ks`). Reportez-vous à Avant de créer des certificats SSL pour vCloud Director sur Linux.
- Vérifiez que vous avez préparé un volume NFS ou un autre volume de stockage partagé accessible à tous les serveurs cible pour votre groupe de serveurs vCloud Director. Reportez-vous à Préparation du stockage du serveur de transfert.
- Vérifiez que vous avez créé une base de données vCloud Director et que tous les serveurs du groupe peuvent y accéder. Reportez-vous à Préparation de la base de données de vCloud Director. Vérifiez que le service de base de données démarre lorsque vous redémarrez le serveur de base de données.
- Vérifiez que tous les serveurs vCloud Director, le serveur de base de données, tous les systèmes vCenter Server et les instances NSX Manager associées peuvent résoudre chaque nom d'hôte dans l'environnement comme décrit dans Configuration réseau requise pour vCloud Director.

- 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 Configuration réseau requise pour vCloud Director.
- 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.
- Ouvrez les ports de pare-feu comme il est indiqué dans Configuration requise pour la sécurité réseau. Le port 443 doit être ouvert entre vCloud Director et les systèmes vCenter Server.

Procédure

1 Installez vCloud Director sur le premier membre d'un groupe de serveurs

Après avoir préparé votre environnement et vérifié les conditions préalables, vous pouvez commencer à créer le groupe de serveurs vCloud Director en exécutant le programme d'installation vCloud Director sur le premier serveur Linux cible.

2 Configuration des connexions au réseau et à la base de données

Après avoir installé vCloud Director sur le premier membre du groupe de serveurs, vous devez exécuter le script de configuration qui crée les connexions au réseau et à la base de données pour cette cellule. Le script crée un fichier de réponses que vous devez utiliser lors de la configuration de membres supplémentaires du groupe de serveurs.

3 Installez vCloud Director sur un membre supplémentaire d'un groupe de serveurs

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

4 Configurer vCloud Director

Après avoir installé et configuré tous les serveurs dans le groupe de serveurs vCloud Director, vous devez configurer votre installation vCloud Director. Le programme d'installation vCloud Director initialise la base de données vCloud Director avec une clé de licence, un compte d'administrateur système et des informations connexes.

Étape suivante

Vous pouvez commencer l'ajout de ressources à votre installation vCloud Director. Pour démarrer avec vCloud Director, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.

Installez vCloud Director sur le premier membre d'un groupe de serveurs

Après avoir préparé votre environnement et vérifié les conditions préalables, vous pouvez commencer à créer le groupe de serveurs vCloud Director en exécutant le programme d'installation vCloud Director sur le premier serveur Linux cible.

vCloud Director pour Linux est distribué en tant que fichier exécutable signé numériquement portant un nom sous la forme `vmware-vcloud-director-distribution-`*v.v.v*`-`*nnnnnn*`.bin`, où *v.v.v* représente la version du produit et *nnnnnn* le numéro de build. Par exemple : `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. L'exécution de cet exécutable installe ou met à niveau vCloud Director.

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.

Conditions préalables

- 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, il n'est pas nécessaire de la revérifier pendant l'installation. Reportez-vous à Téléchargement et installation de la clé publique VMware.

Procédure

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

   Si vous avez acheté le logiciel sur un support, copiez le fichier d'installation vers un emplacement accessible au serveur cible.
3. Vérifiez que la somme de contrôle du téléchargement correspond au total de contrôle publié sur la page de téléchargement.

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

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

   La commande renvoie la somme de contrôle du fichier d'installation qui doit correspondre à la somme de contrôle MD5 à partir de la page de téléchargement.
4. Assurez-vous que le fichier d'installation est exécutable.

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

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

5 Exécutez le fichier d'installation.

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

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

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

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

Si vous n'avez pas installé la clé publique VMware sur le serveur cible, le programme d'installation affiche un avertissement au format suivant :

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

Le programme d'installation effectue les actions suivantes.

a Il vérifie que l'hôte est conforme à toute la configuration requise.

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

c Crée l'utilisateur et le groupe `vcloud`.

d Il décompresse le module RPM vCloud Director.

e Il installe le logiciel.

Lorsque l'installation se termine, le programme d'installation vous invite à exécuter le script de configuration, qui configure les connexions réseau et à la base de données.

6 Sélectionnez si vous voulez exécuter le script de configuration.

a Pour exécuter le script de configuration en mode interactif, entrez **y** et appuyez sur Entrée.

b Pour exécuter le script de configuration ultérieurement en mode interactif ou sans surveillance, entrez **n** et appuyez sur Entrée.

Configuration des connexions au réseau et à la base de données

Après avoir installé vCloud Director sur le premier membre du groupe de serveurs, vous devez exécuter le script de configuration qui crée les connexions au réseau et à la base de données pour cette cellule. Le script crée un fichier de réponses que vous devez utiliser lors de la configuration de membres supplémentaires du groupe de serveurs.

Tous les membres du groupe de serveurs vCloud Director partagent la connexion à la base de données et d'autres détails de la configuration. Lorsque vous exécutez le script de configuration sur le premier membre du groupe de serveurs vCloud Director, le script crée un fichier de réponses qui conserve les informations de connexion à la base de données pour une utilisation au cours des installations de serveurs à venir.

Vous pouvez exécuter le script de configuration en mode interactif ou en mode sans surveillance. Pour une configuration interactive, vous exécutez la commande sans options et le script vous demande les informations d'installation requises. Pour une configuration sans surveillance, vous fournissez les informations de configuration en utilisant les options de commande.

Si vous souhaitez utiliser une adresse IP unique avec deux ports distincts pour le service HTTP et le service de proxy de la console, vous devez exécuter le script de configuration en mode sans surveillance.

Note L'outil de gestion des cellules inclut des sous-commandes que vous pouvez utiliser pour modifier le réseau et les détails de la connexion à la base de données que vous avez configurés initialement. Les modifications que vous apportez en utilisant ces sous-commandes sont écrites dans le fichier de configuration globale et dans le fichier de réponses. Pour plus d'informations sur l'utilisation de l'outil de gestion des cellules, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.

Conditions préalables

- Pour une configuration interactive, consultez Référence de configuration interactive.
- Pour une configuration sans surveillance, consultez Référence de configuration sans surveillance.
- Pour une configuration sans surveillance, vérifiez que la valeur de la variable d'environnement `VCLOUD_HOME` est définie sur le chemin d'accès complet du répertoire dans lequel vCloud Director est installé. Cette valeur est généralement `/opt/vmware/vcloud-director`.

Procédure

1. Connectez-vous au serveur vCloud Director en tant qu'utilisateur racine.
2. Exécutez la commande `configure` :
   - Pour le mode interactif, exécutez la commande et fournissez les informations requises par les invites.

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

   - Pour le mode sans surveillance, exécutez la commande avec les options et les arguments appropriés.

     ```
     /opt/vmware/vcloud-director/bin/configure options –unattended
     ```

   Le script valide les informations, puis :

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

   b. Affiche l'URL à laquelle vous pouvez vous connecter à l'assistant **Configuration de VMware vCloud Director** après le démarrage du service vCloud Director.

   c. Il propose de démarrer la cellule vCloud Director.

3 (Facultatif) Notez l'URL de l'assistant **Configuration de VMware vCloud Director** et entrez **y** pour démarrer le service vCloud Director.

Vous pouvez décider de démarrer le service ultérieurement en exécutant la commande `service vmware-vcd start`.

Résultats

Les informations relatives à la connexion à la base de données ainsi que d'autres informations réutilisables que vous avez fournies lors de la configuration sont conservées dans le fichier de réponses 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.

Étape suivante

Enregistrez une copie du fichier de réponses dans un emplacement sécurisé. 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.

Si vous prévoyez d'ajouter des serveurs au groupe de serveurs, montez le stockage de transfert partagé à l'adresse `/opt/vmware/vcloud-director/data/transfer`.

Référence de configuration interactive

Lorsque vous exécutez le script `configure` en mode interactif, le script vous invite à fournir les informations suivantes.

Pour accepter la valeur par défaut, appuyez sur Entrée.

Tableau 5-1. Informations requises lors de la configuration d'un réseau interactif et d'une base de données

Informations requises	Description
Adresse IP pour le service HTTP	La valeur est définie par défaut sur la première adresse IP disponible.
Adresse IP pour le service de proxy de la console	La valeur est définie par défaut sur la première adresse IP disponible. **Note** Si vous souhaitez utiliser une adresse IP unique avec deux ports distincts pour le service HTTP et le service de proxy de la console, vous devez exécuter le script de configuration en mode sans surveillance.
Chemin d'accès complet au fichier keystore Java	Par exemple, `/opt/keystore/certificates.ks` .
Mot de passe du keystore	Reportez-vous à Avant de créer des certificats SSL pour vCloud Director sur Linux.
Mot de passe de clé privée pour le certificat SSL HTTP	Reportez-vous à Avant de créer des certificats SSL pour vCloud Director sur Linux.
Mot de passe de clé privée pour le certificat SSL de proxy de la console	Reportez-vous à Avant de créer des certificats SSL pour vCloud Director sur Linux.

Tableau 5-1. Informations requises lors de la configuration d'un réseau interactif et d'une base de données (suite)

Informations requises	Description
Activer la journalisation d'audit à distance à un hôte syslog	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. ■ Pour ignorer, appuyez sur Entrée. ■ Pour activer, entrez le nom d'hôte Syslog ou l'adresse IP.
Si vous avez activé la journalisation d'audit à distance, le port UDP de l'hôte syslog	La valeur est définie par défaut sur 514.
Type de base de données	PostgreSQL ou Microsoft SQL Server. La valeur est définie par défaut sur PostgreSQL.
Nom de l'hôte ou adresse IP du serveur de base de données	Le serveur qui exécute la base de données.
Port de la base de données	Pour PostgreSQL, la valeur est définie par défaut sur 5432. Pour Microsoft SQL Server, la valeur est définie par défaut sur 1433.
Nom de la base de données	La valeur est définie par défaut sur vcloud.
Si votre type de base de données est Microsoft SQL Server, l'instance de base de données	La valeur est définie par défaut sur l'instance par défaut.
Nom d'utilisateur de la base de données	Reportez-vous à Préparation de la base de données de vCloud Director.
Mot de passe de la base de données	Reportez-vous à Préparation de la base de données de vCloud Director.
Indiquez si vous souhaitez participer au programme d'amélioration du produit VMware (CEIP)	Ce produit participe au Programme d'amélioration du produit VMware. Les détails concernant les données collectées via le CEIP et les fins auxquelles elles sont utilisées par VMware sont définis dans le Centre de confiance et assurance à l'adresse http://www.vmware.com/trustvmware/ceip.html. Vous pouvez utiliser l'outil de gestion des cellules pour rejoindre ou quitter le Programme d'amélioration du produit VMware à tout moment. Reportez-vous à la section « Référence de l'outil de gestion de cellules » dans le *Guide de l'administrateur de vCloud Director*. Pour joindre le programme, entrez **y**. Si vous préférez ne pas joindre le programme CEIP de la VMware, entrez **n**.

Référence de configuration sans surveillance

Lorsque vous exécutez le script `configure` en mode sans surveillance, vous fournissez les informations de configuration sur la ligne de commande sous la forme d'options et d'arguments.

Tableau 5-2. Options et arguments de l'utilitaire de configuration

Option	Argument	Description
`--help (-h)`	Aucun	Afficher un résumé des options et des arguments de configuration
`--config-file (-c)`	Chemin d'accès au fichier `global.properties`	Les informations que vous fournissez lorsque vous exécutez l'utilitaire de configuration sont sauvegardées dans ce fichier. Si vous ignorez cette option, l'emplacement par défaut est `/opt/vmware/vcloud-director/etc/global.properties`.
`--console-proxy-ip (-cons)`	Adresse IPv4, avec numéro de port facultatif	Le système utilise cette adresse pour le service de proxy de la console vCloud Director. Par exemple, *10.17.118.159*.
`--console-proxy-port-https`	Entier dans la plage comprise entre 0 et 65535	Numéro de port à utiliser pour le service de proxy de la console vCloud Director.
`--database-ssl`	`true` ou `false`	Si vous utilisez une base de données PostgreSQL, vous pouvez configurer la base de données pour exiger une connexion SSL signée depuis vCloud Director. Ignoré si `--database-type` n'est pas `postgres`. Si vous souhaitez configurer la base de données PostgreSQL pour utiliser un certificat auto-signé ou privé, reportez-vous à la section Effectuer des configurations supplémentaires sur la base de données PostgreSQL externe.
`--database-host (-dbhost)`	Adresse IP ou nom de domaine complet de vCloud Director l'hôte de la base de données	Reportez-vous à Préparation de la base de données de vCloud Director.
`--database-domain (-dbdomain)`	Domaine de l'utilisateur de la base de données SQL Server	Facultatif si `--database-type` est `sqlserver`.
`--database-instance (-dbinstance)`	Instance de la base de données SQL Server	Utilisé si `--database-type` est `sqlserver`.

Tableau 5-2. Options et arguments de l'utilitaire de configuration (suite)

Option	Argument	Description
`--database-name (-dbname)`	Nom de service de la base de données	Reportez-vous à Préparation de la base de données de vCloud Director.
`--database-password (-dbpassword)`	Mot de passe de l'utilisateur de la base de données. Il peut être nul.	Reportez-vous à Préparation de la base de données de vCloud Director.
`--database-port (-dbport)`	Numéro de port utilisé par le service de base de données sur l'hôte de la base de données	Reportez-vous à Préparation de la base de données de vCloud Director.
`--database-type (-dbtype)`	Type de base de données. Peut être : ■ `postgres` ■ `sqlserver`	Reportez-vous à Préparation de la base de données de vCloud Director.
`--database-user (-dbuser)`	Nom d'utilisateur de l'utilisateur de la base de données.	Reportez-vous à Préparation de la base de données de vCloud Director.
`--enable-ceip`	`true` ou `false`	Ce produit participe au Programme d'amélioration du produit VMware. Les détails concernant les données collectées via le CEIP et les fins auxquelles elles sont utilisées par VMware sont définis dans le Centre de confiance et assurance à l'adresse http://www.vmware.com/trustvmware/ceip.html. Vous pouvez utiliser l'outil de gestion des cellules pour rejoindre ou quitter le Programme d'amélioration du produit VMware à tout moment. Reportez-vous à la section « Référence de l'outil de gestion de cellules » dans le *Guide de l'administrateur de vCloud Director*.
`--uuid (-g)`	Aucun	Génère un nouvel identifiant unique pour la cellule
`--primary-ip (-ip)`	Adresse IPv4, avec numéro de port facultatif	Le système utilise cette adresse pour le service d'interface Web de vCloud Director. Par exemple, *10.17.118.159*.

Tableau 5-2. Options et arguments de l'utilitaire de configuration (suite)

Option	Argument	Description
`--primary-port-http`	Entier dans la plage comprise entre 0 et 65535	Numéro de port à utiliser pour les connexions HTTP (non sécurisées) auvCloud Director service d'interface Web
`--primary-port-https`	Entier dans la plage comprise entre 0 et 65535	Numéro de port à utiliser pour les connexions HTTPS (sécurisées) au vCloud Director service d'interface Web
`--keystore (-k)`	Chemin d'accès au keystore Java contenant vos certificats et clés privées SSL	Doit être un nom de chemin d'accès complet. Par exemple, `/opt/keystore/certificates.ks` .
`--syslog-host (-loghost)`	Adresse IP ou nom de domaine complet de l'hôte du serveur syslog	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.
`--syslog-port (-logport)`	Entier dans la plage comprise entre 0 et 65535	Port sur lequel le processus `syslog` surveille le serveur spécifié. Défini par défaut sur 514 s'il n'est pas spécifié.
`--response-file (-r)`	Chemin d'accès au fichier de réponses	Doit être un nom de chemin d'accès complet. Défini par défaut sur `/opt/vmware/vcloud-director/etc/responses.properties` s'il n'est pas spécifié. Toutes les informations que vous fournissez lors de l'exécution de l'utilitaire de configuration sont conservées dans ce fichier. **Important** 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.

Tableau 5-2. Options et arguments de l'utilitaire de configuration (suite)

Option	Argument	Description
`--unattended-installation (-unattended)`	Aucun	Spécifie une installation sans surveillance
`--keystore-password (-w)`	Mot passe du keystore de certificats SSL	Mot de passe du keystore de certificats SSL.

Exemple : Configuration sans surveillance avec deux adresses IP

L'exemple de commande suivant exécute une configuration sans surveillance d'un serveur vCloud Director avec deux adresses IP différentes pour le service HTTP et le service de proxy de la console.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db -dbuser vcloud --enable-ceip true \
-dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10 -unattended
```

Exemple : Configuration sans surveillance avec une adresse IP unique

L'exemple de commande suivant exécute une configuration sans surveillance d'un serveur vCloud Director avec une adresse IP unique à deux ports distincts pour le service HTTP et le service de proxy de la console.

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./configure -ip 10.17.118.159 --primary-port-https 9000 -cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

Protéger et réutiliser le fichier de réponses

Les informations de connexion au réseau et à la base de données que vous configurez dans la première cellule de vCloud Director sont sauvegardées dans un fichier de réponses. Ce fichier contient des informations importantes que vous devez réutiliser lorsque vous ajoutez des serveurs au groupe de serveurs. Vous devez conserver le fichier dans un emplacement sécurisé.

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.

Important L'outil de gestion des cellules inclut des sous-commandes que vous pouvez utiliser pour modifier le réseau et les détails de la connexion à la base de données que vous avez spécifiés initialement. Les modifications que vous apportez à l'aide de ces outils sont écrites dans le fichier de configuration globale et dans le fichier de réponses, vous devez donc vous assurer que le fichier de réponses est en place (dans `/opt/vmware/vcloud-director/etc/responses.properties`) et inscriptible avant d'utiliser les commandes pouvant le modifier.

Procédure

1. Protégez le fichier de réponses.

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

2. Réutilisez le fichier de réponses.

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

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

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

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

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

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

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

Étape suivante

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

Installez vCloud Director sur un membre supplémentaire d'un groupe de serveurs

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

Important Les installations mixtes de vCloud Director sur Linux et les déploiements de dispositifs vCloud Director dans un groupe de serveurs unique ne sont pas pris en charge.

Conditions préalables

- Vérifiez que vous pouvez accéder au fichier de réponses créé lorsque vous avez configuré le premier membre de ce groupe de serveurs. Reportez-vous à Configuration des connexions au réseau et à la base de données.
- Vérifiez que vous avez monté le stockage de transfert partagé sur le premier membre du groupe de serveurs vCloud Director sur `/opt/vmware/vcloud-director/data/transfer`.

Procédure

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

   Si vous avez acheté le logiciel sur un support, copiez le fichier d'installation vers un emplacement accessible au serveur cible.
3. Assurez-vous que le fichier d'installation est exécutable.

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

   ```
   [root@cell1 /tmp]# chmod u+x installation-file
   ```
4. Exécutez le fichier d'installation.

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

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

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

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

Si vous n'avez pas installé la clé publique VMware sur le serveur cible, le programme d'installation affiche un avertissement au format suivant :

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

Le programme d'installation effectue les actions suivantes.

a Il vérifie que l'hôte est conforme à toute la configuration requise.

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

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

d Il décompresse le module RPM vCloud Director.

e Il installe le logiciel.

Lorsque l'installation se termine, le programme d'installation vous invite à exécuter le script de configuration, qui configure les connexions réseau et à la base de données.

5 Entrez **n** et appuyez sur Entrée pour rejeter le script de configuration en cours d'exécution.

Vous exécutez le script de configuration ultérieurement en fournissant le fichier de réponses comme entrée.

6 Montez le stockage de transfert partagé sur `/opt/vmware/vcloud-director/data/transfer`.

Tous les serveurs vCloud Director du groupe de serveurs doivent monter ce volume sur le même point de montage.

7 Copiez le fichier de réponses à un emplacement accessible à ce serveur.

Tous les répertoires du chemin d'accès vers le fichier de réponses doivent être lisibles par n'importe quel utilisateur.

8 Exécutez le script de configuration.

a Exécutez la commande `configure` en fournissant le chemin du fichier de réponses.

```
/opt/vmware/vcloud-director/bin/configure -r /responses.properties
```

Le script copie le fichier de réponses sur un emplacement lisible par `vcloud.vcloud` et exécute le script de configuration en utilisant le fichier de réponses comme entrée.

b Sur les invites, fournissez les adresses IP pour le protocole HTTP et les services proxy de la console.

c Si le script de configuration ne trouve pas les certificats valides dans le chemin d'accès enregistré dans le fichier de réponses, lorsque vous y êtes invité, fournissez le chemin d'accès vers les certificats et les mots de passe.

Le script valide les informations, connecte le serveur à la base de données et propose de démarrer la cellule vCloud Director.

9 (Facultatif) Entrez **y** pour démarrer le service vCloud Director.

Vous pouvez décider de démarrer le service ultérieurement en exécutant la commande `service vmware-vcd start`.

Étape suivante

Répétez cette procédure pour ajouter d'autres serveurs à ce groupe de serveurs.

Une fois que les services vCloud Director s'exécutent sur tous les serveurs, vous devez initialiser la base de données vCloud Director avec une clé de licence, un compte d'administrateur système et les informations associées. Vous pouvez initialiser la base de données de l'une des manières suivantes :

- À l'aide d'un navigateur Web, ouvrez l'assistant de configuration à l'URL affichée à la fin du script de configuration. Reportez-vous à Configurer vCloud Director.
- Utilisez l'outil de gestion de cellules avec la sous-commande `system-setup`. Pour plus d'informations sur l'utilisation de l'outil de gestion des cellules, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.

Configurer vCloud Director

Après avoir installé et configuré tous les serveurs dans le groupe de serveurs vCloud Director, vous devez configurer votre installation vCloud Director. Le programme d'installation vCloud Director initialise la base de données vCloud Director avec une clé de licence, un compte d'administrateur système et des informations connexes.

Avant de lancer la console Web vCloud Director, exécutez l'assistant de la **Configuration de VMware vCloud Director** qui rassemble les informations dont la console Web a besoin pour démarrer.

Comme alternative à l'utilisation de l'assistant de la **Configuration de VMware vCloud Director**, pour configurer l'installation vCloud Director, vous pouvez utiliser la sous-commande `system-setup` de l'outil de gestion des cellules. Pour plus d'informations sur l'outil de gestion des cellules, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.

Conditions préalables

- Vérifiez que les services vCloud Director sont démarrés sur tous les serveurs.
- Procurez-vous un numéro de série du produit vCloud Director sur le portail des licences VMware.

Procédure

Procédure

1 Ouvrez un navigateur Web et accédez à l'URL qui affiche le script de configuration.

Pour détecter l'URL de l'assistant de **Configuration de VMware vCloud Director**, vous pouvez également rechercher 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. Pour vous connecter à l'assistant, accédez à https://*fully-qualified-domain-name*, par exemple, https://mycloud.example.com.

Note Le démarrage de l'assistant peut prendre quelques minutes.

2 Révisez la page d'accueil et cliquez sur **Suivant**.

3 Lisez et acceptez le contrat de licence, puis cliquez sur **Suivant**.

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

4 Entrez votre numéro de série du produit vCloud Director et cliquez sur **Suivant**.

5 Entrez un nom d'utilisateur, un mot de passe et les informations de contact de l'administrateur système vCloud Director, puis cliquez sur **Suivant**.

L'administrateur système vCloud Director bénéficie de privilèges de superutilisateur pour l'ensemble du Cloud. Cet administrateur système peut créer des comptes d'administrateur système supplémentaires.

6 Configurez les paramètres système qui contrôlent comment vCloud Director interagit avec vSphere et NSX Manager et cliquez sur **Suivant**.

a Dans la zone de texte **Nom du système**, entrez un nom pour le dossier vCenter Server à utiliser pour cette installation de vCloud Director.

b Dans la zone de texte **ID d'installation**, définissez l'ID de cette installation de vCloud Director à utiliser lorsque vous créez des adresses MAC pour les cartes réseau virtuelles.

Si vous prévoyez de créer des réseaux étirés dans les installations de vCloud Director sur des déploiements multisites, envisagez de définir un identifiant d'installation unique pour chaque installation de vCloud Director.

7 Sur la page Prêt à se connecter, vérifiez les paramètres et cliquez sur **Terminer**.

Résultats

Lorsque le processus de configuration se termine, vous êtes redirigé vers la page de connexion de la Console Web vCloud Director.

Étape suivante

Connectez-vous à la Console Web vCloud Director avec le nom d'utilisateur et le mot de passe de l'administrateur système et commencez à provisionner votre cloud. Pour plus d'informations sur l'ajout de ressources sur vCloud Director, reportez-vous à la *Guide de l'administrateur de vCloud Director*.

Déploiement du dispositif vCloud Director

6

Vous pouvez créer un groupe de serveurs vCloud Director en déployant une ou plusieurs instances du dispositif vCloud Director. Vous déployez le dispositif vCloud Director à l'aide de vSphere Client (HTML5), de vSphere Web Client (Flex) ou de VMware OVF Tool.

Important Les installations mixtes de vCloud Director sur Linux et les déploiements de dispositifs vCloud Director dans un groupe de serveurs unique ne sont pas pris en charge.

Le dispositif vCloud Director est une machine virtuelle préconfigurée optimisée pour exécuter les services vCloud Director.

Le dispositif est distribué avec un nom sous la forme `VMware vCloud Director-`*v.v.v.v*`-`*nnnnnn*`_OVF10.ova`, où *v.v.v.v* représente la version du produit et *nnnnnn* le numéro de build. Par exemple : `VMware vCloud Director-9.7.0.0-9229800_OVA10.ova`.

Le module du dispositif vCloud Director comporte les logiciels suivants :

- VMware Photon™ OS
- Groupe de services vCloud Director
- PostgreSQL 10

Les tailles de petit dispositif principal et de petit dispositif en veille vCloud Director sont adaptées aux systèmes de laboratoire ou de test. Les tailles de grand dispositif principal et de grand dispositif en veille répondent aux exigences de dimensionnement minimales pour les systèmes de production. En fonction de la charge de travail, vous devrez peut-être ajouter des ressources supplémentaires.

Important L'installation d'un composant tiers sur le dispositif vCloud Director n'est pas prise en charge. Vous pouvez installer uniquement des composants VMware pris en charge en fonction des Matrices d'interopérabilité des produits VMware. Par exemple, vous pouvez installer une version prise en charge d'un agent de surveillance VMware vRealize ®Operations Manager™ ou VMware vRealize ®Log Insight™.

Configuration de la base de données du dispositif

À partir de la version 9.7, le dispositif vCloud Director inclut une base de données PostgreSQL intégrée avec la fonction HA (High Availability). Pour créer un déploiement de dispositif avec un cluster HA de base de données, vous devez déployer une instance du dispositif vCloud Director comme cellule principale et deux instances comme cellules en veille. Vous pouvez déployer des instances supplémentaires du dispositif vCloud Director dans le groupe de serveurs comme cellules d'application vCD, qui exécutent uniquement le groupe de services vCloud Director sans la base de données intégrée. Les cellules d'application vCD se connectent à la base de données dans la cellule principale. Reportez-vous à Déploiements du dispositif et configuration de la haute disponibilité de la base de données.

Par défaut, le dispositif vCloud Director utilise TLS, au lieu du SSL obsolète, pour les connexions de base de données, notamment la réplication. Cette fonctionnalité est active immédiatement après le déploiement, en utilisant un certificat PostgreSQL auto-signé. Pour utiliser un certificat signé d'une autorité de certification, reportez-vous à la section Remplacer un certificat auto-signé de base de données PostgreSQL intégrée et d'interface utilisateur de gestion de dispositifs vCloud Director.

Note Le dispositif vCloud Director ne prend pas en charge les bases de données externes.

Configuration du réseau du dispositif

À partir de la version 9.7, le dispositif vCloud Director est déployé avec deux réseaux, `eth0` et `eth1`, afin que vous puissiez isoler le trafic HTTP du trafic de la base de données. Différents services écoutent l'une des interfaces réseau correspondantes ou les deux.

Service	Port sur `eth0`	Port sur `eth1`
SSH	22	22
HTTP	80	s/o
HTTPS	443	s/o
PostgreSQL	s/o	5432
Interface utilisateur de gestion	5480	5480
Proxy de console	8443	s/o
JMX	8998, 8999	s/o
JMS/ActiveMQ	61616	s/o

Le dispositif vCloud Director prend en charge la personnalisation par l'utilisateur des règles de pare-feu à l'aide de `iptables`. Pour ajouter des règles `iptables` personnalisées, vous pouvez ajouter vos propres données de configuration à la fin du fichier `/etc/systemd/scripts/iptables`.

Ce chapitre contient les rubriques suivantes :

- Déploiements du dispositif et configuration de la haute disponibilité de la base de données

- Conditions préalables au déploiement du dispositif vCloud Director
- Déployer le dispositif vCloud Director à l'aide de vSphere Web Client ou de vSphere Client
- Déploiement du dispositif vCloud Director avec VMware OVF Tool

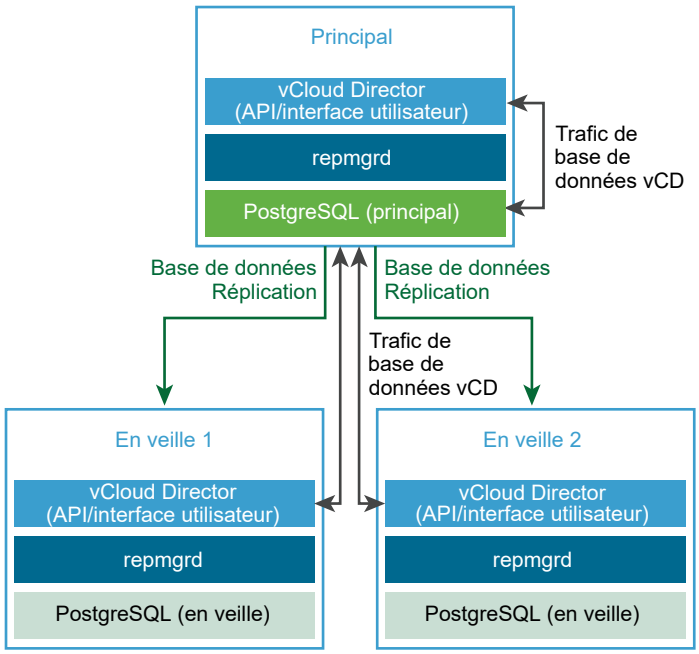
Déploiements du dispositif et configuration de la haute disponibilité de la base de données

Le dispositif vCloud Director inclut une base de données PostgreSQL intégrée. La base de données PostgreSQL intégrée inclut la suite d'outils Replication Manager (repmgr), qui fournit une fonctionnalité de haute disponibilité (HA) à un cluster de serveurs PostgreSQL. Vous pouvez créer un déploiement de dispositif avec un cluster HA de base de données qui fournit des fonctionnalités de basculement à votre base de données vCloud Director.

Vous pouvez déployer le dispositif vCloud Director en tant que cellule principale, cellule en veille ou cellule d'application vCD. Reportez-vous à la section Déployer le dispositif vCloud Director à l'aide de vSphere Web Client ou de vSphere Client, Déploiement du dispositif vCloud Director avec VMware OVF Tool ou Déployer le dispositif vCloud Director avec des certificats génériques signés pour la communication HTTPS et du proxy de la console.

Pour configurer la HA pour votre base de données vCloud Director, lorsque vous créez votre groupe de serveurs, vous pouvez configurer un cluster HA de base de données en déployant une instance principale et deux instances en veille du dispositif vCloud Director.

Figure 6-1. Un cluster HA de base de données du dispositif vCloud Director



Création d'un déploiement de dispositif vCloud Director avec HA de base de données

Pour créer un groupe de serveurs vCloud Director avec une configuration HA de base de données, suivez ce workflow :

1 Déployez le dispositif vCloud Director en tant que cellule principale.

   La cellule principale est le premier membre du groupe de serveurs vCloud Director. La base de données intégrée est configurée en tant que base de données vCloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`.

2 Vérifiez que la cellule principale fonctionne correctement.

   a Pour vérifier la santé du service vCloud Director, connectez-vous avec les informations d'identification de **l'administrateur système** à la console Web vCloud Director à l'adresse `https://`*`primary_eth0_ip_address`*`/cloud`.

   b Pour vérifier la santé de la base de données PostgreSQL, connectez-vous en tant que **racine** à l'interface utilisateur de gestion du dispositif à l'adresse `https://`*`primary_eth1_ip_address`*`:5480`.

      Le nœud principal doit être en cours d'exécution.

3 Déployez deux instances du dispositif vCloud Director en tant que cellules en veille.

   Les bases de données intégrées sont configurées en mode de réplication avec la base de données principale.

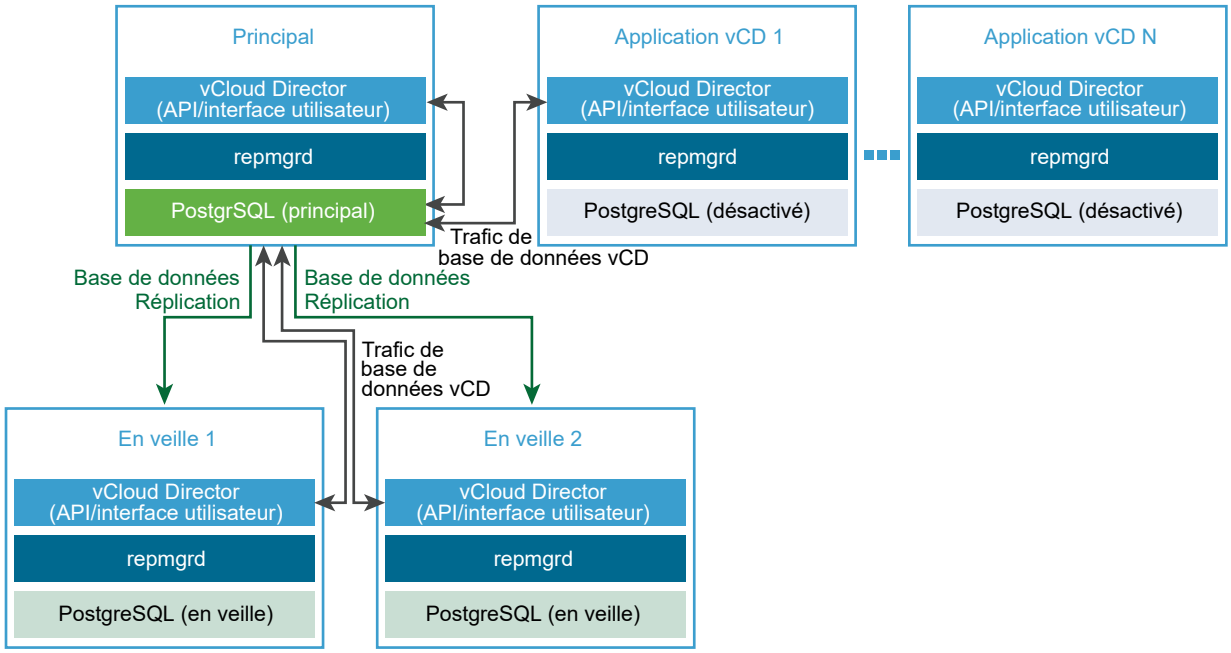
   Note Après le déploiement initial du dispositif en veille, le gestionnaire de réplication commence à synchroniser sa base de données avec la base de données du dispositif principal. Pendant ce temps, la base de données vCloud Director et, par conséquent, l'interface utilisateur vCloud Director sont indisponibles.

4 Vérifiez que toutes les cellules du cluster HA sont en cours d'exécution.

   Reportez-vous à Afficher l'état des cellules dans un cluster haute disponibilité de base de données.

5 (Facultatif) Déployez une ou plusieurs instances du dispositif vCloud Director en tant que cellules d'application vCD.

   Les bases de données intégrées ne sont pas utilisées. La cellule de l'application vCD se connecte à la base de données principale.



Création d'un déploiement de dispositif vCloud Director sans HA de base de données

Pour créer un serveur vCloud Director sans configuration HA de base de données, suivez ce workflow :

1 Déployez le dispositif vCloud Director en tant que cellule principale.

   La cellule principale est le premier membre du groupe de serveurs vCloud Director. La base de données intégrée est configurée en tant que base de données vCloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`.

2 Vérifiez que la cellule principale fonctionne correctement.

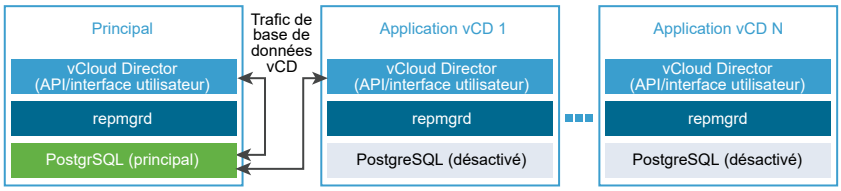
   a Pour vérifier la santé du service vCloud Director, connectez-vous avec les informations d'identification de **l'administrateur système** à la console Web vCloud Director à l'adresse `https://`*`primary_eth0_ip_address`*`/cloud`.

   b Pour vérifier la santé de la base de données PostgreSQL, connectez-vous en tant que **racine** à l'interface utilisateur de gestion du dispositif à l'adresse `https://`*`primary_eth1_ip_address`*`:5480`.

      Le nœud principal doit être en cours d'exécution.

3 (Facultatif) Déployez une ou plusieurs instances du dispositif vCloud Director en tant que cellules d'application vCD.

   La base de données intégrée n'est pas utilisée. La cellule de l'application vCD se connecte à la base de données principale.



Conditions préalables au déploiement du dispositif vCloud Director

Pour garantir un déploiement réussi du dispositif vCloud Director, vous devez effectuer certaines tâches et vérifications préalables avant de démarrer le déploiement.

- Vérifiez que vous avez accès au fichier `.ova` de vCloud Director.
- Avant de déployer le dispositif principal, préparez un stockage de service de transfert partagé NFS. Reportez-vous à Préparation du stockage du serveur de transfert.

  Note Le stockage du service de transfert partagé ne doit contenir aucun fichier `responses.properties` ni répertoire `appliance-nodes`.

- Installer et configurer un broker AMQP RabbitMQ.

Méthodes de déploiement du dispositif vCloud Director

- Déployer le dispositif vCloud Director à l'aide de vSphere Web Client ou de vSphere Client
- Déploiement du dispositif vCloud Director avec VMware OVF Tool
- Déployer le dispositif vCloud Director avec des certificats génériques signés pour la communication HTTPS et du proxy de la console

Déployer le dispositif vCloud Director à l'aide de vSphere Web Client ou de vSphere Client

Vous déployez le dispositif vCloud Director sous la forme d'un modèle OVF en utilisant vSphere Web Client (Flex) ou vSphere Client (HTML5).

Vous devez déployer le premier membre d'un groupe de serveurs vCloud Director en tant que cellule principale. Vous pouvez déployer un membre suivant d'un groupe de serveurs vCloud Director en tant que cellule d'application en veille ou vCD. Reportez-vous à Déploiements du dispositif et configuration de la haute disponibilité de la base de données.

Important Les installations mixtes de vCloud Director sur Linux et les déploiements de dispositifs vCloud Director dans un groupe de serveurs unique ne sont pas pris en charge.

Pour plus d'informations sur le déploiement des modèles OVF dans vSphere, reportez-vous à *Administration d'une machine virtuelle vSphere*.

Comme alternative, vous pouvez déployer le dispositif à l'aide de l'outil VMware OVF Tool. Reportez-vous à Déploiement du dispositif vCloud Director avec VMware OVF Tool.

Note Le déploiement du dispositif vCloud Director dans vCloud Director n'est pas pris en charge.

Conditions préalables

Reportez-vous à Conditions préalables au déploiement du dispositif vCloud Director.

Procédure

1. Démarrer le déploiement du dispositif vCloud Director

   Pour démarrer le déploiement du dispositif, vous ouvrez l'assistant de déploiement dans vSphere Web Client (Flex) ou vSphere Client (HTML5).

2. Personnaliser le dispositif vCloud Director et terminer le déploiement

   Pour configurer les détails de vCloud Director, vous personnalisez le modèle de dispositif.

Étape suivante

- Configurez l'adresse proxy de console publique, car le dispositif vCloud Director utilise sa carte réseau `eth0` avec le port personnalisé 8443 pour le service de proxy de console. Reportez-vous à Personnaliser les points de terminaison publics.
- Pour ajouter des membres au groupe de serveurs vCloud Director, répétez la procédure.
- Pour entrer la clé de licence, connectez-vous à la console Web de vCloud Director.
- Pour remplacer le certificat auto-signé qui est créé lors du premier démarrage du dispositif, vous pouvez Créer un keystore de certificats SSL signés par une autorité de certification pour vCloud Director sous Linux.

Démarrer le déploiement du dispositif vCloud Director

Pour démarrer le déploiement du dispositif, vous ouvrez l'assistant de déploiement dans vSphere Web Client (Flex) ou vSphere Client (HTML5).

Procédure

1. Dans vSphere Web Client ou vSphere Client, cliquez avec le bouton droit sur un objet d'inventaire, puis cliquez sur **Déployer le modèle OVF**.
2. Entrez le chemin d'accès au fichier `.ova` de vCloud Director et cliquez sur **Suivant**.
3. Entrez un nom pour la machine virtuelle et naviguez dans le référentiel vCenter Server pour sélectionner un centre de données ou un dossier sur lequel déployer le dispositif, puis cliquez sur **Suivant**.
4. Sélectionnez un hôte ou un cluster ESXi sur lequel déployer le dispositif, puis cliquez sur **Suivant**.
5. Vérifiez les détails du modèle, puis cliquez sur **Suivant**.

6 Lisez et acceptez le contrat de licence, puis cliquez sur **Suivant**.

7 Sélectionnez le type et la taille de déploiement, puis cliquez sur **Suivant**.

Les tailles de petit dispositif principal et de petit dispositif en veille vCloud Director sont adaptées aux systèmes de laboratoire ou de test. Les tailles de grand dispositif principal et de grand dispositif en veille répondent aux exigences de dimensionnement minimales pour les systèmes de production. En fonction de la charge de travail, vous devrez peut-être ajouter des ressources supplémentaires.

Option	Description
Principal-petit	Déploie le dispositif avec 12 Go de RAM et 2 vCPU en tant que premier membre dans un groupe de serveurs vCloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données vCloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`.
Principal-grand	Déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que premier membre dans un groupe de serveurs vCloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données vCloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`.
En veille-petit	Permet de joindre une petite cellule principale dans un cluster HA de base de données. Déploie le dispositif avec 12 Go de RAM et 2 vCPU en tant que deuxième ou troisième membre dans un groupe de serveurs vCloud Director avec une configuration haute disponibilité de base de données. La base de données intégrée dans une cellule en veille est configurée en mode de réplication avec la base de données principale.
En veille-grand	Permet de joindre une grande cellule principale dans un cluster HA de base de données. Déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que deuxième ou troisième membre dans un groupe de serveurs vCloud Director avec une configuration haute disponibilité de base de données. La base de données intégrée d'un dispositif en veille est configurée en mode de réplication avec la base de données principale.
Cellule d'application vCD	Déploie le dispositif avec 8 Go de RAM et 2 vCPU en tant que membre suivant dans un groupe de serveurs vCloud Director. La base de données intégrée dans une cellule d'application vCD n'est pas utilisée. La cellule de l'application vCD se connecte à la base de données principale.

Important Les cellules principale et en veille dans un groupe de serveurs vCloud Director doivent être de la même taille. Un cluster HA de base de données peut se composer d'une cellule principale de petite taille et deux cellules en veille de petite taille, ou d'une cellule principale de grande taille et deux cellules en veille de grande taille.

Après le déploiement, vous pouvez reconfigurer la taille du dispositif.

8 Sélectionnez le format de disque et la banque de données pour les fichiers de configuration de machine virtuelle et les disques virtuels, puis cliquez sur **Suivant**.

   Les formats statiques améliorent les performances et les formats dynamiques économisent de l'espace de stockage.

9 Dans les menus déroulants des cellules **Réseau de destination**, sélectionnez les réseaux cibles des cartes réseau `eth1` et `eth0` du dispositif.

   La liste de réseaux source peut être dans l'ordre inverse. Vérifiez que vous sélectionnez le réseau de destination approprié pour chaque réseau source.

   Important Les deux réseaux de destination doivent être différents.

10 Dans les menus déroulants **Paramètres d'allocation d'adresses IP**, sélectionnez l'allocation IP **Statique-manuelle** et un protocole **IPv4**.

11 Cliquez sur **Suivant**.

   Vous êtes redirigé vers la page **Personnaliser un modèle** pour configurer les détails vCloud Director.

Personnaliser le dispositif vCloud Director et terminer le déploiement

Pour configurer les détails de vCloud Director, vous personnalisez le modèle de dispositif.

Lorsque vous personnalisez le dispositif vCloud Director, vous configurez les paramètres du dispositif, la base de données et les propriétés du réseau. Vous configurez les paramètres système initiaux uniquement lors du déploiement d'un dispositif principal, qui est le premier membre d'un groupe de serveurs.

Note Seule Étape 3 de cette procédure est facultative. Vous devez effectuer toutes les autres étapes pour personnaliser le dispositif vCloud Director.

Procédure

1 Dans la section **Paramètres du dispositif VCD**, configurez les détails du dispositif.

Paramètre	Description
Serveur NTP	Nom d'hôte ou adresse IP du serveur NTP à utiliser.
Mot de passe racine initial	Le mot de passe racine initial du dispositif. Doit contenir au moins huit caractères, une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial. **Important** Le mot de passe racine initial devient le mot de passe du keystore. Le déploiement du cluster impose que toutes les cellules aient le même mot de passe racine lors du déploiement initial. Une fois le processus de démarrage terminé, vous pouvez modifier le mot de passe racine sur n'importe quelle cellule souhaitée. **Note** L'Assistant de déploiement OVF ne valide pas le mot de passe racine initial par rapport aux critères de mot de passe.

Paramètre	Description
Faire expirer le mot de passe racine lors de la première connexion	Si vous souhaitez continuer à utiliser le mot de passe initial après la première connexion, vous devez vérifier que le mot de passe initial répond aux critères de mot de passe racine. Pour continuer à utiliser le mot de passe racine initial après la première connexion, désélectionnez cette option.
Activer SSH	Désactivé par défaut.
Montage NFS pour l'emplacement de transfert de fichier	Reportez-vous à Préparation du stockage du serveur de transfert.

Note Pour plus d'informations sur la modification de la date, de l'heure ou du fuseau horaire du dispositif, reportez-vous à l'article https://kb.vmware.com/kb/59674.

2 Si vous déployez le premier membre d'un groupe de serveurs, dans la section **Configuration VCD - Requis uniquement pour les dispositifs principaux**, entrez les détails de la base de données, créez le compte de l'**administrateur système** et configurez les paramètres système.

Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`.

Paramètre	Description
Mot de passe de base de données « vcloud » pour l'utilisateur « vcloud »	Le mot de passe de l'utilisateur de la base de données `vcloud`.
Nom d'utilisateur de l'administrateur	Le nom d'utilisateur pour l'**administrateur système**. Réglé par défaut sur `administrator`.
Nom complet de l'administrateur	Le nom complet de l'**administrateur système**. Réglé par défaut sur `vCD Admin`.
Mot de passe de l'utilisateur de l'administrateur	Le mot de passe du compte de l'**administrateur système**.
E-mail de l'administrateur	L'adresse e-mail de l'**administrateur système**.
Nom du système	Le nom du dossier vCenter Server à créer pour cette installation de vCloud Director. Réglé par défaut sur `vcd1`.
ID d'installation	L'ID à utiliser pour cette installation de vCloud Director lorsque vous créez des adresses MAC pour les cartes réseau virtuelles. Réglé par défaut sur `1`. Si vous prévoyez de créer des réseaux étirés dans les installations de vCloud Director sur des déploiements multisites, envisagez de définir un identifiant d'installation unique pour chaque installation de vCloud Director.

3 (Facultatif) Dans la section **Propriétés de mise en réseau supplémentaires**, entrez les routes statiques des interfaces réseau `eth0` et `eth1`, puis cliquez sur **Suivant**.

Vous devrez éventuellement fournir des routes statiques si vous souhaitez atteindre des hôtes sur un itinéraire de passerelle autre que celui par défaut. Par exemple, l'infrastructure de gestion est accessible uniquement via l'interface `eth1`, alors que la passerelle par défaut se trouve sur `eth0`. Dans la plupart des cas, ce paramètre peut rester vide.

Les routes statiques doivent se trouver dans une liste de routes statiques séparées par des virgules. Une spécification de route doit être composée de l'adresse IP de la passerelle cible et, en option, d'une spécification de réseau CIDR (Classless Inter-Domain Routing). Par exemple, **`172.16.100.253 172.16.100.0/19, 172.16.100.253 192.168.100.0/24`**.

4 Dans la section **Propriétés de mise en réseau**, entrez les détails de réseau pour les cartes réseau `eth0` et `eth1`, puis cliquez sur **Suivant**.

Note Tous les paramètres sont requis.

Paramètre	Description
Passerelle par défaut	L'adresse IP de la passerelle par défaut pour le dispositif.
Nom de domaine	Nom de domaine, par exemple *mondomaine.com*.
Chemin de recherche du domaine	Liste de noms de domaine séparés par des virgules ou des espaces pour le chemin de recherche de domaine du dispositif.
Serveurs de noms de domaine	L'adresse IP du serveur de nom de domaine du dispositif.
Adresse IP du réseau eth0	L'adresse IP de l'interface `eth0`.
Masque réseau eth0	Le masque réseau ou le préfixe de l'interface `eth0`.
Adresse IP du réseau eth1	L'adresse IP de l'interface `eth1`.
Masque réseau eth1	Le masque réseau ou le préfixe de l'interface `eth1`.

5 Sur la plage **Prêt à terminer**, passez en revue les paramètres de configuration du dispositif vCloud Director, puis cliquez sur **Terminer** pour démarrer le déploiement.

Étape suivante

Mettez sous tension la nouvelle machine virtuelle.

Déploiement du dispositif vCloud Director avec VMware OVF Tool

Vous déployez le dispositif vCloud Director sous la forme d'un modèle OVF en utilisant VMware OVF Tool.

Vous devez déployer le premier membre d'un groupe de serveurs vCloud Director en tant que cellule principale. Vous pouvez déployer un membre suivant d'un groupe de serveurs vCloud Director en tant que cellule d'application en veille ou vCD. Reportez-vous à Déploiements du dispositif et configuration de la haute disponibilité de la base de données.

Pour plus d'informations sur l'installation d'OVF Tool, consultez le document *Notes de mise à jour de VMware OVF Tool*.

Pour plus d'informations sur l'utilisation d'OVF Tool, consultez le *Guide de l'utilisateur d'OVF Tool*.

Avant d'exécuter la commande de déploiement, consultez Conditions préalables au déploiement du dispositif vCloud Director.

Après avoir déployé le dispositif, recherchez les messages d'erreur d'avertissement dans le fichier journal de premier démarrage. Reportez-vous à Examiner les fichiers journaux dans le dispositif vCloud Director.

Options et propriétés de commande `ovftool` pour le déploiement du dispositif vCloud Director

Option	Valeur	Description
`--noSSLVerify`	s/o	Ignore la vérification SSL pour les connexions vSphere.
`--acceptAllEulas`	s/o	Accepte tous les contrats de licence d'utilisateur final (CLUF).
`--datastore`	*target_vc_datastore*	Le nom de la banque de données cible sur laquelle stocker les fichiers de configuration de machine virtuelle et les disques virtuels.
`--allowAllExtraConfig`	s/o	Convertit toutes les options de configuration supplémentaires au format VMX.
`--net:"eth0 Network"`	*portgroup_on_vc_for_eth0*	Le réseau de destination pour le réseau `eth0` du dispositif. **Important** Doit être différent du réseau de destination `eth1`.
`--net:"eth1 Network"`	*portgroup_on_vc_for_eth1*	Le réseau de destination pour le réseau `eth1` du dispositif. **Important** Doit être différent du réseau de destination `eth0`.
`--name`	*vm_name_on_vc*	Nom de machine virtuelle du dispositif.
`--diskMode`	`thin` ou `thick`	Le format de disque pour les fichiers de configuration de machine virtuelle et les disques virtuels.
`--prop:"vami.ip0.VMware_vCloud_Director"`	*eth0_ip_address*	L'adresse IP de `eth0`. Utilisée pour l'interface utilisateur et l'accès à l'API. Sur cette adresse, la recherche DNS inversée détermine et définit le nom d'hôte du dispositif.
`--prop:"vami.ip1.VMware_vCloud_Director"`	*eth1_ip_address*	L'adresse IP de `eth1`. Utilisée pour accéder aux services internes, y compris le service de base de données PostreSQL intégrée.
`--prop:"vami.DNS.VMware_vCloud_Director"`	*dns_ip_address*	L'adresse IP du serveur de nom de domaine du dispositif.
`--prop:"vami.domain.VMware_vCloud_Director"`	*domain_name*	Domaine de recherche DNS. S'affiche comme premier élément du chemin de recherche.

Option	Valeur	Description
`--prop:"vami.gateway.VMware_vCloud_Director.eth0"`	*gateway_ip_address*	L'adresse IP de la passerelle par défaut pour le dispositif.
`--prop:"vami.netmask0.VMware_vCloud_Director.eth0"`	*netmask*	Le masque réseau ou le préfixe de l'interface `eth0`.
`--prop:"vami.netmask1.VMware_vCloud_Director.eth1"`	*netmask*	Le masque réseau ou le préfixe de l'interface `eth1`.
`--prop:"vami.searchpath.VMware_vCloud_Director"`	*"list_of_domain_names*	Le chemin de recherche du domaine du dispositif. Liste de noms de domaine séparés par des virgules ou des espaces.
`--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"`	*true* ou *false*	Active ou désactive l'accès SSH **racine** au dispositif.
`--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"`	*true* ou *false*	Détermine s'il convient ou non de continuer d'utiliser le mot de passe initial après la première connexion.
`--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"`	*nfs_ip_address*:*nfs_mount_path*	L'adresse IP et chemin d'exportation du serveur NFS externe. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"`	*"ip_address*	L'adresse IP du serveur horaire.
`--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"`	*vCloud_Director_password*	Le mot de passe racine initial du dispositif. Doit contenir au moins huit caractères, une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial. **Important** Le mot de passe racine initial devient le mot de passe du keystore. Le déploiement du cluster impose que toutes les cellules aient le même mot de passe racine lors du déploiement initial. Une fois le processus de démarrage terminé, vous pouvez modifier le mot de passe racine sur n'importe quelle cellule souhaitée.
`--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"`	*DB_password*	Le mot de passe de la base de données de l'utilisateur **vcloud**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.admin_email.VMware_vCloud_Director"`	*vcd_admin_email_address*	L'adresse e-mail du compte de l'**administrateur système**. Utilisé uniquement pour une cellule principale.

Option	Valeur	Description
`--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director_ora`	*Admin_vcd_name*	Le nom du compte de l'**administrateur système**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director_ora`	*vCD_admin_password*	Le mot de passe du compte de l'**administrateur système**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director_or`	*vcd_admin_username*	Le nom d'utilisateur pour l'**administrateur système**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.inst_id.VMware_vCloud_Director_ora`	*vCD_install_ID*	L'ID d'installation de vCloud Director. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudconf.sys_name.VMware_vCloud_Director_ora`	*vCD_system_name*	Le nom du dossier vCenter Server à créer pour cette installation de vCloud Director.
`--prop:"vcloudnet.routes0.VMware_vCloud_Director_ora`	*ip_address1 cidr, ip_address2, ...*	Facultatif. Routes statiques pour l'interface `eth0`. Il doit s'agir d'une liste de spécifications de route séparées par des virgules. Une spécification de route doit être composée d'un adresse IP de passerelle et, en option, d'une spécification de réseau CIDR (Classless Inter-Domain Routing) (préfixe/bits). Par exemple, **`172.16.100.253 172.16.100/19, 172.16.200.253`**.
`--prop:"vcloudnet.routes1.VMware_vCloud_Director_ora`	*ip_address1 cidr, ip_address2, ...*	Facultatif. Routes statiques pour l'interface `eth1`. Il doit s'agir d'une liste de spécifications de route séparées par des virgules. Une spécification de route doit être composée d'un adresse IP de passerelle et, en option, d'une spécification de réseau CIDR (Classless Inter-Domain Routing) (préfixe/bits). Par exemple, **`172.16.100.253 172.16.100/19, 172.16.200.253`**.

Option	Valeur	Description
`--deploymentOption`	`primary-small`, `primary-large`, `standby-small`, `standby-large` ou `cell`	Le type et la taille du dispositif que vous souhaitez déployer. Les tailles de petit dispositif principal et de petit dispositif en veille sont adaptées aux systèmes de laboratoire ou de test. Les tailles de grand dispositif principal et de grand dispositif en veille répondent aux exigences de dimensionnement minimales pour les systèmes de production. En fonction de la charge de travail, vous devrez peut-être ajouter des ressources supplémentaires. ■ `primary-small` déploie le dispositif avec 12 Go de RAM et 2 vCPU en tant que premier membre dans un groupe de serveurs vCloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données vCloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`. ■ `primary-large` déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que premier membre dans un groupe de serveurs vCloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données vCloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`. ■ `standby-small` déploie le dispositif avec 12 Go de RAM et 2 vCPU en tant que deuxième ou troisième membre dans un groupe de serveurs vCloud Director avec une configuration haute disponibilité de base de données. La base de données intégrée dans une cellule en veille est configurée en mode de réplication avec la base de données principale. ■ `standby-large` déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que deuxième ou troisième membre dans un groupe de serveurs vCloud Director avec une

Option	Valeur	Description
		configuration haute disponibilité de base de données. La base de données intégrée dans une cellule en veille est configurée en mode de réplication avec la base de données principale. ■ `cell` déploie le dispositif avec 8 Go de RAM et 2 vCPU en tant que membre suivant dans un groupe de serveurs vCloud Director. La base de données intégrée dans une cellule d'application vCD n'est pas utilisée. La cellule de l'application vCD se connecte à la base de données principale. **Important** Les cellules principale et en veille dans un groupe de serveurs vCloud Director doivent être de la même taille. Un cluster HA de base de données peut se composer d'une cellule principale de petite taille et deux cellules en veille de petite taille, ou d'une cellule principale de grande taille et deux cellules en veille de grande taille. Après le déploiement, vous pouvez reconfigurer la taille du dispositif.
`--powerOn`	*path_to_ova*	Mettez la machine virtuelle sous tension après le déploiement.

Exemple de commande pour déployer le dispositif vCloud Director principal

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig  \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
```

```
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="XjO52mXAP7n#" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="o@e@vJW26Pnb" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_dataceter_name/host/vc_cluster_name
```

Exemple de commande pour déployer un dispositif vCloud Director en veille

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig  \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_dataceter_name/host/vc_cluster_name
```

Création et gestion des certificats SSL du dispositif vCloud Director 7

Le dispositif vCloud Director utilise SSL pour sécuriser les communications entre les clients et les serveurs. Chaque dispositif vCloud Director doit prendre en charge deux points de terminaison SSL différents : pour les communications HTTPS et les communications de proxy de console.

Ces points de terminaison peuvent être des adresses IP distinctes ou une adresse IP unique avec deux ports distincts. Chaque point de terminaison requiert son propre certificat SSL. Vous pouvez utiliser le même certificat (par exemple, un certificat générique) pour les deux points de terminaison.

Ce chapitre contient les rubriques suivantes :

Déployer le dispositif vCloud Director avec des certificats génériques signés pour la communication HTTPS et du proxy de la console

Vous pouvez déployer le dispositif vCloud Director avec des certificats génériques signés. Vous pouvez utiliser ces certificats pour sécuriser un nombre illimité de serveurs qui sont des sous-domaines du nom de domaine répertorié dans le certificat.

Par défaut, lors du déploiement des dispositifs vCloud Director, vCloud Director génère des certificats auto-signés et les utilise pour configurer la cellule vCloud Director pour la communication HTTPS et du proxy de la console.

Lorsque vous déployez correctement un dispositif principal, la logique de configuration du dispositif copie le fichier `responses.properties` du dispositif principal sur le stockage du service de transfert partagé NFS commun dans `/opt/vmware/vcloud-director/data/transfer`. Les autres dispositifs déployés pour ce groupe de serveurs vCloud Director utilisent ce fichier pour se configurer automatiquement. Le fichier `responses.properties` inclut un chemin d'accès au keystore de certificats SSL, qui inclut les certificats auto-signés générés automatiquement `user.keystore.path`. Par défaut, ce chemin d'accès correspond à un fichier keystore qui est local pour chaque dispositif.

Après avoir déployé le dispositif principal, vous pouvez le reconfigurer pour qu'il utilise des certificats signés. Pour plus d'informations sur la création du keystore avec des certificats signés, reportez-vous à la section Créer et importer des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director.

Si les certificats signés que vous utilisez sur le dispositif vCloud Director principal sont des certificats signés par des caractères génériques, ces certificats peuvent s'appliquer à tous les autres dispositifs du groupe de serveurs vCloud Director, c'est-à-dire aux cellules en veille et aux cellules d'application vCloud Director. Vous pouvez utiliser le déploiement du dispositif avec des certificats génériques signés pour la communication HTTPS et de proxy de la console afin de configurer les cellules supplémentaires avec les certificats SSL génériques signés.

Conditions préalables

- Vérifiez que le keystore contenant les certificats SSL génériques signés pour les alias HTTPS et de proxy de la console est disponible sur le dispositif principal, à savoir `/opt/vmware/vcloud-director/certificates.ks`.
  - Si vous devez créer des paires de clés et importer des fichiers de certificat signés par une autorité de certification, reportez-vous à Créer et importer des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director.
  - Si vous disposez déjà de votre propre clé privée et de fichiers de certificats signés par une autorité de certification, consultez Importer des clés privées et des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director.
- Vérifiez que le mot de passe privé des clés dans le keystore correspond au mot de passe du keystore. Le mot de passe du keystore doit correspondre au mot de passe racine initial utilisé lors du déploiement de tous les dispositifs, par exemple,

  ```
  /opt/vmware/vcloud-director/jre/bin/keytool -keypasswd -alias http_or_consoleproxy -keystore /opt/vmware/vcloud-director/certificates.ks -storetype jceks -storepass root-password
  ```

  .

Procédure

1. Copiez le nouveau fichier `certificats.ks` contenant les certificats signés correctement depuis le dispositif principal vers le partage de transfert à l'adresse `/opt/vmware/vcloud-director/data/transfer/`.

2 Définissez les autorisations du propriétaire et du groupe sur le fichier keystore sur **vcloud**.

```
chown vcloud.vcloud /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

3 Vérifiez que le propriétaire du fichier keystore dispose des autorisations de lecture et d'écriture.

```
chmod 0750 /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

4 Sur le dispositif principal, exécutez la commande pour importer les nouveaux certificats signés dans l'instance de vCloud Director.

Cette commande met également à jour le fichier `responses.properties` dans le partage de transfert, en modifiant la variable *user.keystore.path* pour qu'elle pointe vers le fichier keystore du partage de transfert.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/data/transfer/certificates.ks --keystore-password root-password
```

5 Pour que les nouveaux certificats signés prennent effet, redémarrez le service *vmware-vcd* sur le dispositif principal.

```
service vmware-vcd restart
```

6 Déployez les dispositifs de cellule en veille et de cellule d'application à l'aide du mot de passe racine initial qui correspond au mot de passe du keystore.

Résultats

Tous les dispositifs récemment déployés qui utilisent le même stockage de service de transfert partagé NFS sont configurés avec les mêmes certificats génériques SSL signés que ceux utilisés par le dispositif principal.

Créer et importer des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director

La création et l'importation de certificats signés par une autorité de certification offrent le niveau de confiance le plus élevé pour les communications SSL et vous aident à sécuriser les connexions dans votre cloud.

Chaque serveur vCloud Director nécessite deux certificats SSL pour sécuriser les communications entre les clients et les serveurs. Chaque serveur vCloud Director doit prendre en charge deux points de terminaison SSL différents : pour les communications HTTPS et les communications de proxy de console.

Dans le dispositif vCloud Director, ces deux points de terminaison partagent la même adresse IP ou le même nom d'hôte, mais utilisent deux ports distincts : `443` pour HTTPS et `8443` pour les communications de proxy de la console. Chaque point de terminaison doit disposer de son propre certificat SSL. Vous pouvez utiliser le même certificat pour les deux points de terminaison, par exemple, en utilisant un certificat de caractère générique.

Les certificats pour ces deux points de terminaison doivent inclure un nom distinct X.500 et une extension de nom alternatif d'objet X.509.

Si vous disposez déjà de votre propre clé privée et de fichiers de certificats signés par une autorité de certification, suivez la procédure décrite dans Importer des clés privées et des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director.

Important Lors du déploiement, le dispositif vCloud Director génère des certificats auto-signés avec une taille de clé de 2 048 bits. Vous devez évaluer les exigences de sécurité de votre installation avant de choisir une taille de clé appropriée. Les tailles de clés inférieures à 1 024 bits ne sont plus prises en charge par la publication spéciale NIST 800-131A.

Le mot de passe du keystore utilisé dans cette procédure est le mot de passe de l'utilisateur **racine** qui est représenté par *root_passwd*.

Conditions préalables

Familiarisez-vous avec la commande `keytool`. `keytool` permet d'importer des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director. vCloud Director place une copie de `keytool` dans `/opt/vmware/vcloud-director/jre/bin/keytool`.

Procédure

1. Connectez-vous directement ou via SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.
2. Selon les besoins de votre environnement, choisissez l'une des options suivantes.

   Lorsque vous déployez le dispositif vCloud Director, vCloud Director génère automatiquement des certificats auto-signés avec une taille de clé de 2 048 bits pour le service HTTPS et le service de proxy de la console.

   - Si vous souhaitez que votre autorité de certification signe les certificats générés lors du déploiement, passez à l'Étape étape 5.
   - Si vous souhaitez générer de nouveaux certificats avec des options personnalisées telles qu'une taille de clé supérieure, par exemple, passez à l'Étape étape 3.
3. Exécutez la commande pour sauvegarder le fichier `certificates.ks` existant.

   ```
   cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
   ```

4 Exécutez la commande pour créer des paires de clés publique et privée pour le service HTTPS et pour le service de proxy de la console.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o /opt/vmware/vcloud-director/certificates.ks -w root_passwd
```

La commande crée ou met à jour un keystore dans `certificates.ks` avec le mot de passe que vous avez spécifié. Les certificats sont créés à l'aide des valeurs par défaut de la commande. Selon la configuration DNS de votre environnement, le nom commun (CN) de l'émetteur est défini sur l'adresse IP ou le nom de domaine complet de chaque service. Le certificat utilise la clé 2 048 bits par défaut et expire un an après sa création.

Important En raison de restrictions de configuration du dispositif vCloud Director, vous devez utiliser l'emplacement `/opt/vmware/vcloud-director/certificates.ks` pour le keystore des certificats.

Note Utilisez le mot de passe **racine** du dispositif comme mot de passe du keystore.

5 Créez des demandes de signature de certificats (CSR) pour le service HTTPS et le service de proxy de console.

Important Le dispositif vCloud Director partage la même adresse IP et le même nom d'hôte pour le service HTTPS et le service de proxy de la console. C'est pourquoi les commandes de création de CSR doivent avoir les mêmes DNS et adresses IP pour l'argument d'extension du nom de remplacement du sujet (SAN).

a Créez une demande de signature de certificat dans le fichier `http.csr`.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

b Créez une demande de signature de certificat dans le fichier `consoleproxy.csr`.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias consoleproxy -file consoleproxy.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

6 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.

Vous obtenez les certificats signés par une autorité de certification.

7 Copiez les certificats signés par une autorité de certification, le certificat racine de l'autorité de certification et tous les certificats intermédiaires dans le dispositif vCloud Director.

8 Exécutez les commandes pour importer les certificats signés dans le keystore JCEKS.

a Importez le certificat racine de l'autorité de certification du fichier `root.cer` vers le fichier keystore `certificates.ks`.

```
keytool –import –storetype JCEKS –storepass root_password –keystore /opt/vmware/vcloud–
director/certificates.ks –alias root –file root_certificate_file
```

b Si vous recevez des certificats intermédiaires, importez-les du fichier `intermediate.cer` dans le fichier keystore `certificates.ks`.

```
keytool –import –storetype JCEKS –storepass root_password –keystore /opt/vmware/vcloud–
director/certificates.ks –alias intermediate –file intermediate_certificate_file
```

c Importez le certificat du service HTTPS.

```
keytool –import –storetype JCEKS –storepass root_password –keystore /opt/vmware/vcloud–
director/certificates.ks –alias http –file http_certificate_file
```

d Importez le certificat du service de proxy de la console.

```
keytool –import –storetype JCEKS –storepass root_password –keystore /opt/vmware/vcloud–
director/certificates.ks –alias consoleproxy –file console_proxy_certificate_file
```

Les commandes remplacent le fichier `certificates.ks` par les versions signées par une autorité de certification récemment acquises.

9 Pour vérifier si les certificats sont importés, exécutez la commande pour répertorier le contenu du fichier keystore.

```
keytool –storetype JCEKS –storepass root_password –keystore /opt/vmware/vcloud–director/
certificates.ks –list
```

10 Exécutez la commande pour importer les certificats dans l'instance de vCloud Director.

```
/opt/vmware/vcloud–director/bin/cell–management–tool certificates –j –p ––keystore /opt/vmware/
vcloud–director/certificates.ks ––keystore–password root_password
```

11 Pour que les nouveaux certificats signés prennent effet, redémarrez le service `vmware–vcd` sur le dispositif vCloud Director.

```
service vmware–vcd restart
```

Étape suivante

- Si vous utilisez des certificats génériques, reportez-vous à Déployer le dispositif vCloud Director avec des certificats génériques signés pour la communication HTTPS et du proxy de la console.
- Si vous n'utilisez pas de certificats génériques, répétez cette procédure sur tous les serveurs vCloud Director dans le groupe de serveurs.

- Pour plus d'informations sur le remplacement des certificats pour la base de données PostgreSQL intégrée et pour l'interface utilisateur de gestion des dispositifs vCloud Director, consultez Remplacer un certificat auto-signé de base de données PostgreSQL intégrée et d'interface utilisateur de gestion de dispositifs vCloud Director.

Importer des clés privées et des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director

Si vous disposez de votre propre clé privée et de fichiers de certificats signés par une autorité de certification, vous devez créer des fichiers keystore dans lesquels importer les certificats et les clés privées pour le service HTTPS et le service de proxy de la console avant d'importer les keystores dans votre environnement vCloud Director.

Conditions préalables

- Familiarisez-vous avec la commande `keytool`. `keytool` permet d'importer des certificats SSL signés par une autorité de certification dans le dispositif vCloud Director. vCloud Director place une copie de `keytool` dans `/opt/vmware/vcloud-director/jre/bin/keytool`.
- Copiez vos certificats intermédiaires, le certificat de l'autorité de certification racine, le service HTTPS signé par une autorité de certification ainsi que les clés et certificats privés du service de proxy de console sur le dispositif.

Procédure

1. Connectez-vous directement ou via SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.
2. Si vous disposez de certificats intermédiaires, exécutez la commande pour combiner le certificat racine signé par une autorité de certification avec les certificats intermédiaires et créer une chaîne de certificats.

   ```
   cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
   ```

3. Utilisez OpenSSL pour créer des fichiers keystore PKCS12 intermédiaires pour les services HTTPS et le service de proxy de la console avec la clé privée, la chaîne de certificats et l'alias respectif, et spécifiez un mot de passe pour chaque fichier keystore.
   a. Créez le fichier keystore pour le service HTTPS.

      ```
      openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.pfx -chain
      ```

   b. Créez le fichier keystore pour le service de proxy de la console.

      ```
      openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
      ```

4 Exécutez la commande pour sauvegarder le fichier `certificates.ks` existant.

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

5 Utilisez la commande `keytool` pour importer les keystores PKCS12 dans le keystore JCEKS.

a Importez le keystore PKCS12 pour le service HTTPS.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-
director/certificates.ks -deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -
srcstorepass keystore_password
```

b Importez le keystore PKCS12 pour le service de proxy de la console.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-
director/certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype
PKCS12 -srcstorepass keystore_password
```

6 Vérifiez que l'importation des certificats a réussi.

```
keytool -storetype JCEKS -storepass keystore_password -keystore /opt/vmware/vcloud-director/
certificates.ks -list
```

7 Exécutez la commande pour importer les certificats signés dans l'instance de vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/certificates.ks --keystore-password keystore_password
```

8 Pour que les certificats signés par une autorité de certification prennent effet, redémarrez le service `vmware-vcd` sur le dispositif vCloud Director.

```
service vmware-vcd restart
```

Étape suivante

- Si vous utilisez des certificats génériques, reportez-vous à Déployer le dispositif vCloud Director avec des certificats génériques signés pour la communication HTTPS et du proxy de la console.
- Si vous n'utilisez pas de certificats génériques, répétez cette procédure sur toutes les cellules de dispositif vCloud Director dans le groupe de serveurs.
- Pour plus d'informations sur le remplacement des certificats pour la base de données PostgreSQL intégrée et pour l'interface utilisateur de gestion des dispositifs vCloud Director, consultez Remplacer un certificat auto-signé de base de données PostgreSQL intégrée et d'interface utilisateur de gestion de dispositifs vCloud Director.

Remplacer un certificat auto-signé de base de données PostgreSQL intégrée et d'interface utilisateur de gestion de dispositifs vCloud Director

Par défaut, la base de données PostgreSQL intégrée et l'interface utilisateur de gestion des dispositifs vCloud Director partagent un ensemble de certificats SSL auto-signés. Pour une sécurité accrue, vous pouvez remplacer les certificats auto-signés par défaut par des certificats signés par une autorité de certification.

Lorsque vous déployez le dispositif vCloud Director, il génère des certificats auto-signés avec une période de validité de 365 jours. Le dispositif vCloud Director utilise deux ensembles de certificats SSL. Le service vCloud Director utilise un ensemble de certificats pour les communications HTTPS et de proxy de la console. La base de données PostgreSQL intégrée et l'interface utilisateur de gestion de dispositifs vCloud Director partagent l'autre ensemble de certificats SSL.

Note Le processus de remplacement des certificats de l'interface utilisateur de gestion de base de données et de dispositifs n'affecte pas les certificats pour les communications HTTPS et de proxy de console. Le remplacement de l'un des ensembles de certificats ne signifie pas que vous devez remplacer l'autre ensemble.

Procédure

1. Envoyez la demande de signature de certificat se trouvant dans `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` à l'autorité de certification pour signature.
2. Si vous remplacez le certificat pour la base de données principale, placez tous les autres nœuds en mode de maintenance afin d'éviter tout risque de perte de données.
3. Remplacez le certificat de format PEM existant sur `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` par le certificat signé, obtenu de votre autorité de certification à l'étape 1.
4. Pour récupérer le nouveau certificat, redémarrez les services vpostgres, nginx et vcd_ova_ui.

   ```
   systemctl restart nginx.service && systemctl restart vcd_ova_ui.service
   ```

   ```
   systemctl restart vpostgres.service
   ```

5. Si vous remplacez le certificat de la base de données principale, sortez tous les autres nœuds du mode de maintenance.

Résultats

Le nouveau certificat est importé dans le magasin d'approbations vCloud Director sur les autres cellules vCloud Director lors de la prochaine exécution de la fonction `appliance-sync`. L'opération peut prendre jusqu'à 60 secondes.

Renouveler les certificats du dispositif vCloud Director

Lorsque vous déployez le dispositif vCloud Director, il génère des certificats auto-signés avec une période de validité de 365 jours. Si des certificats expirent ou ont expiré dans votre environnement, vous pouvez générer de nouveaux certificats auto-signés. Vous devez renouveler les certificats pour chaque cellule vCloud Director individuellement.

Le dispositif vCloud Director utilise deux ensembles de certificats SSL. Le service vCloud Director utilise un ensemble de certificats pour les communications HTTPS et de proxy de console. La base de données PostgreSQL intégrée et l'interface utilisateur de gestion de dispositifs vCloud Director partagent l'autre ensemble de certificats SSL.

Vous pouvez modifier les deux ensembles de certificats auto-signés. Si vous utilisez des certificats signés par une autorité de certification pour les communications HTTPS et de proxy de la console de vCloud Director, vous pouvez uniquement modifier la base de données PostgreSQL intégrée et le certificat de l'interface utilisateur de gestion de dispositif. Les certificats signés par une autorité de certification incluent une chaîne d'approbation complète enracinée dans une autorité de certification publique connue.

Conditions préalables

Si vous renouvelez le certificat pour le nœud principal dans un cluster haute disponibilité de base de données, placez tous les autres nœuds en mode de maintenance pour éviter toute perte de données. Consultez Gestion d'une cellule.

Procédure

1. Connectez-vous directement ou via SSH au système d'exploitation du dispositif vCloud Director en tant qu'utilisateur **racine**.
2. Pour arrêter les services vCloud Director, exécutez la commande suivante.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool -u administrator cell --shutdown
   ```

3. Pour générer de nouveaux certificats auto-signés, exécutez la commande suivante.

   ```
   /opt/vmware/appliance/bin/generate-certificates.sh <root-password>
   ```

   Cette commande utilise automatiquement les certificats générés récemment pour la base de données PostgreSQL intégrée et l'interface utilisateur de gestion du dispositif. Les serveurs PostgreSQL et Nginx redémarrent. La commande génère un nouveau keystore de certificats `/opt/vmware/vcloud-director/certificates.ks` avec de nouveaux certificats auto-signés pour la communication HTTPS et de proxy de la console de vCloud Director, qui sont utilisées dans Étape 4.

4 Si vous n'utilisez pas de certificats signés par une autorité de certification, exécutez la commande pour importer les certificats auto-signés récemment générés dans vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/certificates.ks --keystore-password <root-password>
```

5 Redémarrez le service vCloud Director.

```
service vmware-vcd start
```

Résultats

Les certificats auto-signés renouvelés sont visibles dans l'interface utilisateur de vCloud Director.

Le nouveau certificat PostgreSQL est importé dans le magasin d'approbations vCloud Director sur les autres cellules vCloud Director lors de la prochaine exécution de la fonction `appliance-sync`. L'opération peut prendre jusqu'à 60 secondes.

Étape suivante

Si nécessaire, un certificat auto-signé peut être remplacé par un certificat signé par une autorité de certification externe ou interne.

Configuration d'un dispositif vCloud Director

8

Vous pouvez afficher l'état des cellules d'un cluster HA de base de données, sauvegarder et restaurer la base de données intégrée, et reconfigurer les paramètres du dispositif.

Après le déploiement du dispositif vCloud Director, vous ne pouvez pas modifier les adresses IP réseau `eth0` et `eth1`, ni le nom d'hôte du dispositif. Si vous souhaitez que le dispositif vCloud Director ait des adresses ou un nom d'hôte différents, vous devez déployer un nouveau dispositif.

Si vous devez effectuer la maintenance d'un dispositif qui nécessite l'arrêt du cluster haute disponibilité de la base de données, vous devez d'abord arrêter le dispositif principal, puis les dispositifs en veille, pour éviter les problèmes de synchronisation.

Ce chapitre contient les rubriques suivantes :

Afficher l'état des cellules dans un cluster haute disponibilité de base de données

Pour afficher l'état des cellules principales et en veille dans un cluster haute disponibilité (HA) de base de données de dispositif, vous pouvez vous connecter à l'interface utilisateur de gestion de dispositif de n'importe quelle cellule du cluster HA de base de données.

Le cluster HA de la base de données de dispositif vCloud Director se compose d'une cellule principale et de deux cellules en veille. Reportez-vous à Déploiements du dispositif et configuration de la haute disponibilité de la base de données.

Procédure

1. Dans un navigateur Web, accédez à l'interface utilisateur de gestion de dispositif, à l'adresse `https://vcd_ip_address:5480`.
2. Connectez-vous en tant qu'utilisateur **racine**.
3. Pour afficher les détails sur les cellules du cluster HA de base de données, cliquez sur **Disponibilité de la base de données vCD**.

Propriété	Description
Nom	Nom DNS de la cellule.
Role	Peut être une cellule principale ou en veille. Un cluster HA de base de données de dispositif se compose d'une cellule principale et de deux cellules en veille.
Status	Peut être en cours d'exécution, inaccessible ou en échec. Un astérisque (*) indique l'état de la cellule principale.
Following	Nom de la cellule principale avec laquelle la cellule en veille est répliquée.

Étape suivante

Si une cellule en veille n'est pas à l'état en cours d'exécution, déployez une nouvelle cellule en veille.

Si la cellule principale n'est pas à l'état en cours d'exécution, Récupérer après une panne de base de données principale dans un cluster haute disponibilité.

Récupérer après une panne de base de données principale dans un cluster haute disponibilité

Si la cellule principale ne fonctionne pas correctement, pour récupérer la base de données vCloud Director, vous pouvez promouvoir l'une des cellules en veille pour qu'elle devienne la nouvelle cellule principale. Ensuite, vous devez déployer une nouvelle cellule en veille.

Conditions préalables

- La cellule principale est à l'état inaccessible ou d'échec.
- Les deux cellules en veille sont à l'état d'exécution.

Reportez-vous à Afficher l'état des cellules dans un cluster haute disponibilité de base de données.

Procédure

1. Connectez-vous en tant qu'utilisateur **racine** à l'interface utilisateur de gestion du dispositif d'une cellule en veille en cours d'exécution, `https://standby_ip_address:5480`.

2 Dans la colonne **Rôle** de la cellule en veille qui doit devenir la nouvelle cellule principale, cliquez sur **Promouvoir**.

   La cellule devient la nouvelle cellule principale à l'état d'exécution. L'autre cellule en veille suit la cellule principale nouvellement promue.

3 Déployez un nouveau dispositif en veille.

Étape suivante

1 Supprimez le dispositif principal ayant échoué à la fois du groupe de serveurs vCloud Director et du cluster à haute disponibilité repmgr. Consultez Supprimer une cellule de cloud et Annuler l'enregistrement d'une cellule principale ayant échoué dans un cluster haute disponibilité de base de données .

2 Si nécessaire, supprimez le dispositif principal ayant échoué.

Sauvegarde et restauration de la base de données intégrée du dispositif vCloud Director

Vous pouvez sauvegarder la base de données PostgreSQL intégrée au dispositif vCloud Director, ce qui peut vous aider à restaurer votre environnement vCloud Director après un échec.

Sauvegarder la base de données intégrée du dispositif vCloud Director

Si votre environnement comprend des déploiements de dispositifs vCloud Director avec des bases de données PostgreSQL intégrées, vous pouvez sauvegarder la base de données vCloud Director à partir de la cellule principale. Le fichier `.tgz` qui en résulte est stocké à l'emplacement de stockage du service de transfert partagé NFS.

Procédure

1 Connectez-vous directement ou via SSH à la cellule principale en tant qu'utilisateur **racine**.

2 Accédez à `/opt/vmware/appliance/bin`.

3 Exécutez la commande `create-db-backup`.

Résultats

Sur le stockage du service de transfert partagé NFS, dans le répertoire *`vcloudapp.nfs_mount.VMware_vCloud_Director`*`/pgdb-backup/`, vous pouvez voir le fichier `db-backup-`*`date_time_format`*`.tgz` qui vient d'être créé. Le fichier `.tgz` contient le fichier de vidage de la base de données, ainsi que les fichiers `global.properties`, `responses.properties`, `certificates` et `proxycertificates` de la cellule principale.

Restauration d'un environnement de dispositif vCloud Director avec une configuration de base de données haute disponibilité

Si vous avez sauvegardé la base de données PostgreSQL intégrée d'un environnement de dispositif vCloud Director avec une configuration de base de données HA, vous pouvez déployer un nouveau cluster de dispositifs et y restaurer la base de données du dispositif.

Pour restaurer un déploiement de dispositif avec une configuration de base de données non-HA, voir Restauration d'un environnement de dispositif vCloud Director sans configuration de base de données haute disponibilité.

Le workflow de restauration inclut trois étapes principales.

- Copie du fichier de sauvegarde `.tar` de la base de données intégrée à partir du stockage partagé NFS du service de transfert.
- Restauration de la base de données dans la base de données intégrée et les cellules de secours.
- Déploiement de toutes les cellules d'application requises.

Conditions préalables

- Vérifiez que vous disposez d'un fichier de sauvegarde `.tar` de la base de données PostgreSQL intégrée. Reportez-vous à la section Sauvegarder la base de données intégrée du dispositif vCloud Director.
- Déployez une cellule de base de données principale et deux cellules de base de données de secours. Reportez-vous à la section Chapitre 6 Déploiement du dispositif vCloud Director.
- Si vous souhaitez que le nouveau cluster de dispositifs utilise le serveur NFS de l'environnement précédent, créez et exportez un nouveau répertoire sur le serveur comme nouvelle part. Le point de montage existant ne peut pas être réutilisé.

Procédure

1 Sur les cellules principale et de secours, connectez-vous en tant que **racine** et exécutez la commande pour arrêter le service vCloud Director.

```
service vmware-vcd stop
```

2 Sur les cellules principale et de secours, copiez le fichier de sauvegarde `.tar` dans le dossier `/tmp`.

Si l'espace libre dans le dossier `/tmp` est insuffisant, utilisez un autre emplacement pour stocker le fichier `.tar`.

3 Sur les cellules principale et de secours, décompressez le fichier de sauvegarde dans l'emplacement `/tmp`.

```
tar -zxvf db-backup-date_time_format.tgz
```

Dans le dossier `/tmp`, vous pouvez voir les fichiers `global.properties`, `responses.properties`, `certificates`, `proxycertficates`, `truststore`, extraits, ainsi que le fichier de vidage de la base de données nommé `vcloud_`*`date_time_format`*.

Note Le fichier `truststore` est uniquement disponible pour vCloud Director 9.7.0.1 et versions ultérieures.

4 Sur la cellule principale uniquement, connectez-vous en tant qu'utilisateur **racine** à la console et exécutez les commandes suivantes.

a Abandonnez la base de données `vcloud`.

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/psql –c 'DROP DATABASE vcloud;'
```

b Exécutez la commande `pg_restore`.

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/pg_restore –C –d postgres /tmp/
vcloud_date_time_name
```

5 Dans les cellules principale et de secours, enregistrez une copie des fichiers de données de configuration, remplacez-les, puis reconfigurez et démarrez le service vCloud Director.

a Sauvegardez les fichiers truststore, de propriétés et de certificats.

Les fichiers `global.properties`, `responses.properties`, `certificates`, `proxycertificates` et `truststore` se trouvent dans `/opt/vmware/vcloud–director/etc/`.

Note Le fichier `truststore` est uniquement disponible pour vCloud Director 9.7.0.1 et versions ultérieures.

```
cd /opt/vmware/vcloud–director/etc
mkdir –p backup
cp global.properties responses.properties certificates proxycertificates truststore backup
```

b Copiez et remplacez les fichiers truststore, de propriétés et de certificats à partir des fichiers de sauvegarde que vous avez extraits à l'étape 3.

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates truststore /opt/
vmware/vcloud–director/etc/.
```

Note Le fichier `truststore` est uniquement disponible pour vCloud Director 9.7.0.1 et versions ultérieures.

```
cp certificates /optvmware/vcloud–director/.
```

c Sauvegardez le fichier keystore qui se trouve à l'emplacement `/opt/vmware/vcloud-director/certificates.ks`.

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

d Exécutez la commande pour reconfigurer le service vCloud Director.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Où :

- L'option `--keystore-password` correspond au mot de passe du keystore pour les certificats sur le dispositif.
- L'option `--database-password` correspond au mot de passe de la base de données que vous avez défini lors du déploiement du dispositif.
- L'option `--database-host` correspond à l'adresse IP réseau `eth1` du dispositif de la base de données principale.
- La valeur `--primary-ip` correspond à l'adresse IP du réseau `eth0` de la cellule du dispositif que vous restaurez. Il ne s'agit pas de l'adresse IP de la cellule de base de données principale.
- L'option `--console-proxy-ip` correspond à l'adresse IP réseau `eth0` du dispositif que vous restaurez.

Pour obtenir des informations sur le dépannage, consultez La reconfiguration du service vCloud Director échoue lors de la migration ou de la restauration vers le dispositif vCloud Director.

e Exécutez la commande pour démarrer le service vCloud Director.

```
service vmware-vcd start
```

Vous pouvez surveiller la progression du démarrage de la cellule à l'adresse `/opt/vmware/vcloud-director/logs/cell.log`.

6 (Facultatif) Déployez d'éventuelles cellules d'application supplémentaires. Reportez-vous à la section Chapitre 6 Déploiement du dispositif vCloud Director.

7 Une fois que toutes les cellules du groupe de serveurs ont terminé le processus de démarrage, vérifiez que la restauration de votre environnement vCloud Director a réussi.

   a Ouvrez la vCloud Director Web Console à l'aide de l'adresse IP du réseau `eth0` de n'importe quelle cellule du nouveau groupe de serveurs, `https://`*`et0_IP_new_cell`*`/cloud`.

   b Connectez-vous à la vCloud Director Web Console avec vos informations d'identification d'**administrateur système** existantes.

   c Confirmez que votre instance de vSphere et que vos ressources de cloud sont disponibles dans le nouvel environnement.

8 Après avoir procédé à la vérification de la restauration de la base de données, utilisez la vCloud Director Web Console pour supprimer les cellules déconnectées appartenant à l'ancien environnement vCloud Director.

   a Dans l'onglet **Gérer et surveiller**, cliquez sur **Cellules de cloud**.

   b Cliquez avec le bouton droit sur le nom d'une cellule et sélectionnez **Supprimer**.

Restauration d'un environnement de dispositif vCloud Director sans configuration de base de données haute disponibilité

Si vous avez sauvegardé la base de données PostgreSQL intégrée d'un environnement de dispositif vCloud Director avec une configuration de base de données non HA, vous pouvez déployer un nouveau cluster de dispositifs et y restaurer la base de données du dispositif.

Pour restaurer le déploiement d'un dispositif avec une configuration de base de données HA, consultez Restauration d'un environnement de dispositif vCloud Director avec une configuration de base de données haute disponibilité.

Le workflow de restauration inclut trois étapes principales.

- Copie du fichier de sauvegarde `.tar` de la base de données intégrée à partir du stockage partagé NFS du service de transfert.
- Restauration de la base de données dans la cellule principale de base de données intégrée.
- Déploiement de toutes les cellules d'application requises.

Conditions préalables

- Vérifiez que vous disposez d'un fichier de sauvegarde `.tar` de la base de données PostgreSQL intégrée. Reportez-vous à la section Sauvegarder la base de données intégrée du dispositif vCloud Director.
- Déployez une seule cellule de base de données principale. Reportez-vous à la section Chapitre 6 Déploiement du dispositif vCloud Director.
- Si vous souhaitez que le nouveau cluster de dispositifs utilise le serveur NFS de l'environnement précédent, créez et exportez un nouveau répertoire sur le serveur comme nouvelle part. Le point de montage existant ne peut pas être réutilisé.

Procédure

1 Sur la cellule principale, connectez-vous en tant qu'utilisateur **racine** à la console et exécutez la commande pour arrêter le service vCloud Director.

```
service vmware-vcd stop
```

2 Copiez le fichier de sauvegarde `.tar` dans le dossier `/tmp`.

Si l'espace libre dans le dossier `/tmp` est insuffisant, utilisez un autre emplacement pour stocker le fichier `.tar`.

3 Décompressez le fichier de sauvegarde à l'emplacement `/tmp`.

```
tar -zxvf db-backup-date_time_format.tgz
```

Dans le dossier `/tmp`, vous pouvez voir les fichiers `global.properties`, `responses.properties`, `certificates`, `proxycertficates`, `truststore`, extraits, ainsi que le fichier de vidage de la base de données nommé `vcloud_date_time_format`.

Note Le fichier `truststore` est uniquement disponible pour vCloud Director 9.7.0.1 et versions ultérieures.

4 Exécutez les commandes pour supprimer la base de données et la restaurer dans le nouveau dispositif.

a Abandonnez la base de données `vcloud`.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

b Exécutez la commande `pg_restore`.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/
vcloud_date_time_name
```

5 Dans la cellule principale, enregistrez une copie des fichiers de données de configuration, remplacez-les, puis reconfigurez et démarrez le service vCloud Director.

a Sauvegardez les fichiers truststore, de propriétés et de certificats.

Les fichiers `global.properties`, `responses.properties`, `certificates`, `proxycertificates` et `truststore` se trouvent dans `/opt/vmware/vcloud-director/etc/`.

Note Le fichier `truststore` est uniquement disponible pour vCloud Director 9.7.0.1 et versions ultérieures.

```
cd /opt/vmware/vcloud-director/etc
mkdir -p backup
cp global.properties responses.properties certificates proxycertificates truststore backup
```

b Copiez et remplacez les fichiers truststore, de propriétés et de certificats à partir des fichiers de sauvegarde que vous avez extraits à l'étape 3.

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates truststore /opt/
vmware/vcloud-director/etc/.
```

Note Le fichier `truststore` est uniquement disponible pour vCloud Director 9.7.0.1 et versions ultérieures.

```
cp certificates /optvmware/vcloud-director/.
```

c Sauvegardez le fichier keystore qui se trouve à l'emplacement `/opt/vmware/vcloud-director/certificates.ks`.

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

d Exécutez la commande pour reconfigurer le service vCloud Director.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Où :

- L'option `--keystore-password` correspond au mot de passe du keystore pour les certificats sur le dispositif.
- L'option `--database-password` correspond au mot de passe de la base de données que vous avez défini lors du déploiement du dispositif.
- L'option `--database-host` correspond à l'adresse IP réseau `eth1` du dispositif de la base de données principale.
- La valeur `--primary-ip` correspond à l'adresse IP du réseau `eth0` de la cellule du dispositif que vous restaurez. Il ne s'agit pas de l'adresse IP de la cellule de base de données principale.
- L'option `--console-proxy-ip` correspond à l'adresse IP réseau `eth0` du dispositif que vous restaurez.

Pour obtenir des informations sur le dépannage, consultez La reconfiguration du service vCloud Director échoue lors de la migration ou de la restauration vers le dispositif vCloud Director.

e Exécutez la commande pour démarrer le service vCloud Director.

```
service vmware-vcd start
```

Vous pouvez surveiller la progression du démarrage de la cellule à l'adresse `/opt/vmware/vcloud-director/logs/cell.log`.

6 (Facultatif) Déployez d'éventuelles cellules d'application supplémentaires. Reportez-vous à la section Chapitre 6 Déploiement du dispositif vCloud Director.

7 Une fois que toutes les cellules du groupe de serveurs ont terminé le processus de démarrage, vérifiez que la restauration de votre environnement vCloud Director a réussi.

a Ouvrez la vCloud Director Web Console à l'aide de l'adresse IP du réseau `eth0` de n'importe quelle cellule du nouveau groupe de serveurs, `https://`*`et0_IP_new_cell`*`/cloud`.

b Connectez-vous à la vCloud Director Web Console avec vos informations d'identification d'**administrateur système** existantes.

c Confirmez que votre instance de vSphere et que vos ressources de cloud sont disponibles dans le nouvel environnement.

8 Après avoir procédé à la vérification de la restauration de la base de données, utilisez la vCloud Director Web Console pour supprimer les cellules déconnectées appartenant à l'ancien environnement vCloud Director.

a Dans l'onglet **Gérer et surveiller**, cliquez sur **Cellules de cloud**.

b Cliquez avec le bouton droit sur le nom d'une cellule et sélectionnez **Supprimer**.

Configurer l'accès externe à la base de données vCloud Director

Vous pouvez activer l'accès depuis des adresses IP externes particulières à la base de données vCloud Director qui est intégrée dans le dispositif principal.

Lors d'une migration vers le dispositif vCloud Director ou si vous prévoyez d'utiliser une solution de sauvegarde de base de données tierce, vous pouvez activer l'accès externe à la base de données vCloud Director intégrée.

Procédure

1 Connectez-vous directement ou via SSH à la cellule principale en tant qu'utilisateur **racine**.

2 Accédez au répertoire de la base de données, `/opt/vmware/appliance/etc/pg_hba.d/`.

3 Créez un fichier texte contenant des entrées pour les adresses IP externes cibles semblable à :

```
#TYPE  DATABASE  USER    ADDRESS        METHOD
host   vcloud    vcloud  CIDR_notation  md5
```

Par exemple :

```
#TYPE  DATABASE  USER    ADDRESS           METHOD
host   vcloud    vcloud  172.168.100.5/32  md5
host   vcloud    vcloud  172.168.20.5/32   md5
```

Vos entrées sont ajoutées au fichier `pg_hba.conf` mis à jour de manière dynamique, qui contrôle l'accès à la base de données principale dans le cluster HA.

Activer ou désactiver l'accès SSH au dispositif vCloud Director

Pendant le déploiement du dispositif, vous pouvez laisser désactivé l'accès SSH au dispositif ou l'activer. Après le déploiement, vous pouvez basculer le paramètre d'accès SSH.

Le démon SSH s'exécute dans le dispositif pour être utilisé par la fonction HA de base de données HA et pour les connexions **racine** à distance. Vous pouvez désactiver l'accès SSH pour l'utilisateur **racine**. L'accès SSH pour la fonction HA de base de données reste inchangé.

Procédure

1. Si vous souhaitez apporter des modifications temporaires à la propriété OVF (par exemple, à des fins de test), modifiez la propriété dans vCloud Director.
   a. Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.
   b. Exécutez le script pour activer ou désactiver l'accès **racine** SSH.
      - Pour activer l'accès **racine** SSH, exécutez le script `/opt/vmware/appliance/bin/enable_root_login.sh`.
      - Pour désactiver l'accès **racine** SSH, exécutez le script `/opt/vmware/appliance/bin/disable_root_login.sh`.
2. Si vous souhaitez apporter des modifications permanentes à la propriété OVF, utilisez l'interface utilisateur de vSphere pour définir la valeur de la propriété `vcloudapp.enable_ssh.VMware_vCloud_Director`.

   Note Vous devez mettre hors tension la machine virtuelle pour modifier la valeur de la propriété dans vSphere.

   - Pour activer SSH, définissez la valeur de `vcloudapp.enable_ssh.VMware_vCloud_Director` sur **`True`**.
   - Pour désactiver SSH, définissez la valeur de `vcloudapp.enable_ssh.VMware_vCloud_Director` sur **`False`**.

Modifier les paramètres DNS du dispositif vCloud Director

Après le déploiement, vous pouvez modifier le ou les serveurs DNS du dispositif vCloud Director.

Important Vous ne pouvez pas modifier le nom d'hôte du dispositif. Vous devez déployer un nouveau dispositif avec le nom d'hôte souhaité.

Procédure

1 Si vous souhaitez modifier temporairement les paramètres DNS, notamment à des fins de test, modifiez les paramètres DNS dans vCloud Director.

   a Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.

   b (Facultatif) Vérifiez la configuration DNS actuelle en exécutant la commande suivante :

   ```
   ovfenv --key vami.DNS.VMware_vCloud_Director
   ```

   c Modifiez le ou les serveurs DNS.

   Pour spécifier plusieurs serveurs DNS, définissez *DNS_server_IP* en tant que liste de serveurs séparés par des virgules sans espace.

   ```
   ovfenv --key vami.DNS.VMware_vCloud_Director --value DNS_server_IP
   ```

   d Pour que les modifications prennent effet, redémarrez le service VAOS.

   ```
   systemctl restart vaos.service
   ```

2 Si vous souhaitez modifier définitivement les paramètres DNS, utilisez l'interface utilisateur de vSphere pour définir la valeur de la propriété `vami.DNS.VMware_vCloud_Director` sur la nouvelle adresse IP du serveur DNS.

   Pour spécifier plusieurs serveurs DNS, entrez une liste de serveurs séparés par des virgules sans espace.

   Note Vous devez mettre hors tension la machine virtuelle pour modifier la valeur de la propriété dans vSphere.

Modifier les routes statiques pour les interfaces réseau du dispositif vCloud Director

Vous pouvez modifier les routes statiques des interfaces réseau `eth0` et `eth1` après le déploiement initial de vCloud Director.

Procédure

1 Si vous souhaitez modifier temporairement la valeur de la route statique, par exemple à des fins de test, modifiez les routes statiques dans vCloud Director.

   a Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.

   b (Facultatif) Vérifiez la configuration de la route statique actuelle.

   - Pour `eth0`, exécutez la commande suivante.

     ```
     ovfenv --key vcloudnet.routes0.VMware_vCloud_Director
     ```

   - Pour `eth1`, exécutez la commande suivante.

     ```
     ovfenv --key vcloudnet.routes1.VMware_vCloud_Director
     ```

   c Modifiez la valeur de la route statique.

   Les routes statiques doivent se trouver dans une liste de routes statiques séparées par des virgules. Par exemple, pour `eth0` vous devez exécuter :

   ```
   ovfenv --key vcloudnet.routes0.VMware_vCloud_Director  --value "172.16.100.253
   172.16.96.0/19, 172.16.100.253 192.168.100.0/24"
   ```

   - Pour `eth0`, exécutez la commande suivante.

     ```
     ovfenv --key vcloudnet.routes0.VMware_vCloud_Director  --value "new_static_routes0"
     ```

   - Pour `eth1`, exécutez la commande suivante.

     ```
     ovfenv --key vcloudnet.routes1.VMware_vCloud_Director  --value "new_static_routes1"
     ```

   d Redémarrez le service réseau sur le dispositif vCloud Director.

   ```
   systemctl restart vcd-ova-netconfig.service
   ```

2 Si vous souhaitez modifier définitivement la valeur de la route statique, modifiez la propriété OVF à l'aide de l'interface utilisateur de vSphere.

   Les routes statiques doivent se trouver dans une liste de spécifications de route séparées par des virgules.

   Note Vous devez mettre hors tension la machine virtuelle pour modifier la valeur de la propriété dans vSphere.

   - Utilisez l'interface utilisateur de vSphere pour définir la valeur de la propriété `vcloudnet.routes0.VMware_vCloud_Director` sur la nouvelle chaîne de spécification de route.
   - Utilisez l'interface utilisateur de vSphere pour définir la valeur de la propriété `vcloudnet.routes1.VMware_vCloud_Director` sur la nouvelle chaîne de spécification de route.

Scripts de configuration dans le dispositif vCloud Director

Le dispositif vCloud Director contient des scripts de configuration spécifiques.

Répertoire	Description
`/opt/vmware/appliance/bin/`	Les scripts de configuration du dispositif.
`/opt/vmware/appliance/etc/`	Les fichiers de configuration du dispositif.
`/opt/vmware/appliance/etc/pg_hba.d/`	Le répertoire dans lequel vous pouvez ajouter des entrées personnalisées au fichier `pg_hba. conf`. Reportez-vous à Configurer l'accès externe à la base de données vCloud Director.

Modifier les configurations PostgreSQL dans le dispositif vCloud Director

Vous pouvez modifier les configurations PostgreSQL du dispositif vCloud Director à l'aide de la commande `ALTER SYSTEM` de PostgreSQL.

La commande `ALTER SYSTEM` écrit les modifications apportées aux configurations de paramètres dans le fichier `postgresql.auto.conf`, lequel est prioritaire par rapport au fichier `postgresql.conf` lors de l'initialisation de PostgreSQL. Certains paramètres nécessitent un redémarrage du service PostgreSQL, tandis que d'autres sont configurés dynamiquement et ne nécessitent pas de redémarrage. Ne modifiez pas le fichier `postgresql.conf`, car ces modifications ne sont pas conservées après le redémarrage.

Procédure

1. Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation du dispositif principal en tant que **racine**.
2. Remplacez l'utilisateur par **postgres**.

   ```
   sudo –i –u postgres
   ```

3. Utilisez la commande `ALTER SYSTEM` de PostgreSQL pour modifier un paramètre.

   ```
   psql –c "ALTER SYSTEM set parameter='value';"
   ```

4. Répétez l'étape Étape 3 pour chaque paramètre de configuration que vous souhaitez modifier.
5. Si certains des paramètres que vous souhaitez modifier nécessitent un redémarrage du service PostgreSQL, redémarrez le processus vpostgres.

   ```
   systemctl restart vpostgres
   ```

6 Si votre environnement dispose de nœuds en veille, copiez le fichier `postgresql.auto.conf` sur les dispositifs en veille, puis redémarrez le service PostgreSQL si nécessaire.

   a Copiez le fichier `postgresql.auto.conf` du nœud principal vers un nœud en veille.

   ```
   scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
   ```

   b Si certains des paramètres du fichier `postgresql.auto.conf` copié nécessitent un redémarrage pour prendre effet, redémarrez le processus vpostgres sur le nœud en veille.

   ```
   systemctl restart vpostgres
   ```

   c Répétez les étapes 6.a et 6.b pour chaque nœud en veille.

Utilisation de la suite d'outils Replication Manager dans une configuration de cluster haute disponibilité

9

La suite d'outils open-source repmgr fait partie de la base de données PostgreSQL intégrée du dispositif vCloud Director. Vous pouvez utiliser repmgr pour configurer, surveiller et contrôler la réplication PostgreSQL et le basculement de base de données dans votre cluster haute disponibilité de base de données vCloud Director.

Vous pouvez utiliser l'interface de ligne de commande repmgr pour vérifier l'état et les événements d'un nœud ou d'un cluster, pour enregistrer un nœud ou en annuler l'enregistrement, pour promouvoir un nœud en veille, pour permuter les rôles d'un nœud principal et d'un nœud en veille, ou pour suivre un nouveau nœud principal.

Pour en savoir plus sur la configuration de haute disponibilité de base de données vCloud Director, reportez-vous à la section Déploiements du dispositif et configuration de la haute disponibilité de la base de données

Pour en savoir plus sur repmgr, visitez repmgr.org.

Ce chapitre contient les rubriques suivantes :

- Vérifier l'état de connectivité d'un cluster haute disponibilité de base de données
- Vérifier l'état de réplication d'un nœud d'un cluster haute disponibilité de base de données
- Vérifier l'état d'un cluster haute disponibilité de base de données
- Détection d'un ancien nœud principal qui revient en ligne dans un cluster haute disponibilité
- Permuter les rôles de la cellule principale et de la cellule en veille dans un cluster haute disponibilité de base de données
- Annuler l'enregistrement d'un nœud en veille ayant échoué ou inaccessible dans un cluster haute disponibilité de base de données
- Annuler l'enregistrement d'une cellule principale ayant échoué dans un cluster haute disponibilité de base de données
- Annuler l'enregistrement d'une cellule en veille en cours d'exécution dans un cluster haute disponibilité de base de données

Vérifier l'état de connectivité d'un cluster haute disponibilité de base de données

Vous pouvez utiliser la suite d'outils de Replication Manager pour vérifier la connectivité entre les nœuds de votre cluster haute disponibilité de base de données.

Procédure

1. Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur **racine** au système d'exploitation de toute cellule en cours d'exécution dans le cluster.
2. Remplacez l'utilisateur par **postgres**.

   ```
   sudo –i –u postgres
   ```

3. Vérifiez la connectivité du cluster.
   - La commande `repmgr cluster matrix` exécute la commande `repmgr cluster show` sur chaque nœud du cluster et présente le résultat sous la forme d'une matrice.

     ```
     /opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf
     cluster matrix
     ```

     Dans l'exemple suivant, le nœud 1 et le nœud 2 sont actifs, et le nœud 3 est inactif. Chaque ligne correspond à un serveur et représente le résultat du test d'une connexion sortante à partir de ce serveur.

     Les trois entrées de la troisième ligne sont marquées d'un symbole `?Symbole` , car le nœud 3 est inactif et il n'y a aucune information sur ses connexions sortantes.

     ```
          Name| Id |  1 |  2  |  3
     ---------+----+----+----+----
       node 1 |  1 |  * |  * |  x
       node 2 |  2 |  * |  * |  x
       node 3 |  3 |  ? |  ? |  ?
     ```

   - La commande `repmgr cluster crosscheck` recoupe les connexions entre chaque combinaison de nœuds et peut fournir une meilleure vue d'ensemble de la connectivité du cluster.

     ```
     /opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf
     cluster crosscheck
     ```

Dans l'exemple suivant, le nœud depuis lequel vous exécutez la commande `repmgr cluster crosscheck` fusionne sa sortie système de matrice de cluster à la sortie des autres nœuds et effectue un recoupement entre les nœuds. Dans ce cas, tous les nœuds sont actifs, mais le pare-feu abandonne les paquets provenant du nœud 1 et dirigés vers le nœud 3. Nous avons ici un exemple de partition réseau asymétrique, où le nœud1 ne peut pas envoyer de paquets au nœud 3.

```
            Name| Id |  1 |  2  |  3
        ---------+----+----+----+----
          node 1 |  1 |  * |  * |  x
          node 2 |  2 |  * |  * |  *
          node 3 |  3 |  * |  * |  *
```

Étape suivante

Pour déterminer l'état de connectivité global de votre cluster haute disponibilité de base de données, exécutez ces commandes sur chaque nœud et comparez les résultats.

Vérifier l'état de réplication d'un nœud d'un cluster haute disponibilité de base de données

Vous pouvez utiliser la suite d'outils de Replication Manager et le terminal interactif PostgreSQL pour vérifier l'état de réplication des nœuds individuels d'un cluster haute disponibilité de base de données.

Procédure

1. Connectez-vous en tant qu'utilisateur **racine** au système d'exploitation de l'un des nœuds en cours d'exécution dans le cluster ou ouvrez une session SSH sur celui-ci.
2. Remplacez l'utilisateur par **postgres**.

   ```
   sudo –i –u postgres
   ```

3. Vérifiez l'état de réplication du nœud.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf node
   status
   ```

   La sortie système fournit des informations sur le nœud, la version de PostgreSQL et les détails de la réplication.

4 (Facultatif) Pour obtenir des informations plus détaillées, utilisez le terminal interactif PostgreSQL pour vérifier l'état de réplication des nœuds.

   Le terminal interactif PostgreSQL peut fournir des informations indiquant si des enregistrements de journaux reçus des nœuds en veille sont en retard par rapport aux journaux envoyés par le nœud principal.

   a Connectez-vous au terminal `psql`

   ```
   /opt/vmware/vpostgres/current/bin/psql
   ```

   b Pour développer l'affichage et faciliter la lecture des résultats de la requête, exécutez la commande `set \x`.

   c Exécutez une requête d'état de réplication en fonction du rôle du nœud.

Option	Action
Exécutez une requête sur le nœud principal.	`/opt/vmware/vpostgres/current/bin/psql`
Exécutez une requête sur un nœud en veille.	`select * from pg_stat_wal_receiver;`

Vérifier l'état d'un cluster haute disponibilité de base de données

Pour résoudre les problèmes dans votre cluster haute disponibilité de base de données, vous devez surveiller l'état des nœuds et des événements dans le cluster.

Procédure

1 Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur **`racine`** au système d'exploitation de toute cellule en cours d'exécution dans le cluster.

2 Remplacez l'utilisateur par **`postgres`**.

   ```
   sudo –i –u postgres
   ```

3 Vérifiez l'état du cluster.

   La colonne **En amont** affiche le nœud principal actuel.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr cluster show
   ```

   La sortie de la console affiche les informations sur le cluster. Dans l'exemple suivant, le nœud principal du cluster, node 3, est inaccessible.

   ```
        ID |  Name    | Role    | Status         | Upstream   | Location | Connection string
   --------+----------+---------+----------------+------------+----------+-----------------------
    Node 1 | Node name | standby |     running   | Node 3 name| default | host=host IP address
   ```

```
user=repmgr dbname=repmgr
 Node 2 | Node name | standby |     running   | Node 3 name| default | host=host IP address
user=repmgr dbname=repmgr
 Node 3 | Node name | primary | ? unreachable |            | default | host=host IP address
user=repmgr dbname=repmgr
```

Dans l'exemple de sortie système suivant, node 3 est le nœud principal d'un cluster en cours d'exécution sain.

```
     ID |  Name     | Role    | Status   | Upstream  | Location| Connection string
--------+-----------+---------+----------+-----------+---------+-----------------------
 Node 1 | Node name | standby |  running | Node3 name| default | host=host IP address user=repmgr
dbname=repmgr
 Node 2 | Node name | standby |  running | Node3 name| default | host=host IP address user=repmgr
dbname=repmgr
 Node 3 | Node name | primary | *running |           | default | host=host IP address user=repmgr
dbname=repmgr
```

4 Vérifiez le journal des événements du cluster.

```
/opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf cluster
event
```

La sortie système affiche les événements de création, de clonage et d'enregistrement dans le cluster.

Étape suivante

Si l'état du nœud principal est `inaccessible` ou `échec`, vous devez promouvoir un nœud en veille.

Si l'état d'un nœud en veille est `inaccessible` ou `échec`, réparez le nœud et démarrez le service PostgreSQL s'il n'est pas en cours d'exécution.

Détection d'un ancien nœud principal qui revient en ligne dans un cluster haute disponibilité

Si un nœud principal de votre cluster tombe en panne et qu'il revient en ligne lorsque vous promouvez un nœud en veille comme nouveau nœud principal, cela entraîne des inexactitudes dans les données repmgr. Vous pouvez détecter des irrégularités avec la commande `repmgr cluster show`.

Exemple : Exécution de `repmgr cluster show` sur l'ancien nœud principal

Dans l'exemple suivant, l'exécution de la commande `repmgr cluster show` sur un nœud principal précédent qui revient en ligne entraîne la sortie système suivante.

```
     ID |  Name     | Role    | Status            | Upstream  | Location | Connection string
--------+-----------+---------+-------------------+-----------+----------+------------------------
 Node 1 | Node1 name| standby |!running as primary|Node 3 name| default  | host=host IP address
user=repmgr dbname=repmgr
 Node 2 | Node2 name| standby |     running       |Node 3 name| default  | host=host IP address
user=repmgr dbname=repmgr
 Node 3 | Node3 name| primary |   * running       |           | default  | host=host IP address
user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 1(ID: Node 1) is registered as standby but running as primary
```

Dans l'exemple, le nœud 1 est le nœud principal actuel du cluster.

Lorsque vous exécutez la commande `repmgr cluster show`, l'obtention de l'état `!running as primary (exécution en tant que nœud principal)` pour un nœud en veille indique qu'un ancien nœud principal est en cours d'exécution dans le cluster. Dans ce cas, vous devez arrêter l'ancien nœud principal et annuler son enregistrement.

Exemple : Exécution de `repmgr cluster show` sur le nouveau nœud principal

Dans l'exemple suivant, l'exécution de la commande `repmgr cluster show` sur le nouveau nœud principal entraîne la sortie système suivante.

```
     ID |  Name    | Role    | Status     | Upstream   | Location | Connection string
--------+----------+---------+------------+------------+----------+-------------------------
 Node 1 |Node1 name| primary |  * running |            | default  | host=host IP address user=repmgr
dbname=repmgr
 Node 2 |Node2 name| standby |    running | Node1 name | default  | host=host IP address user=repmgr
dbname=repmgr
 Node 3 |Node3 name| primary |  ! running |            | default  | host=host IP address user=repmgr
dbname=repmgr
   WARNING: following issues were detected
  - node 3(ID: Node 3) is running but the repmgr node record is inactive
```

Dans ce cas, les données repmgr sont correctes. Elles indiquent précisément que le nœud 1 est en cours d'exécution et qu'il s'agit du nœud principal actuel. Le message d'avertissement concernant le nœud 3, l'ancien nœud principal, indique que les données repmgr sur ce nœud ne sont pas exactes.

Exemple : Exécution de `repmgr cluster show` après la promotion d'un nœud en veille, sans exécuter `standby follow` sur les nœuds en veille restants

Dans l'exemple suivant, vous pouvez voir les données repmgr sur chaque nœud d'un cluster dans lequel le nœud principal a échoué. Un nœud en veille a été promu manuellement à l'aide de la commande `repmgr standby promote`, mais sans exécuter `repmgr standby follow` sur les nœuds en veille restants.

Lorsque vous exécutez `repmgr cluster show` sur le nouveau nœud principal, la sortie système représente des données repmgr correctes, mais le nouveau nœud principal, node 2, n'est suivi d'aucun nœud en veille.

```
     ID |  Name    | Role    | Status    | Upstream   |Location | Connection string
--------+----------+---------+-----------+------------+---------+-----------------------
 Node 1 |Node1 name| primary | * running |            | default | host=host IP address user=repmgr
dbname=repmgr
 Node 2 |Node2 name| primary | ! running |            | default | host=host IP address user=repmgr
dbname=repmgr
 Node 3 |Node3 name| standby |   running |Node 1 name | default | host=host IP address user=repmgr
dbname=repmgr
   WARNING: following issues were detected
  - node 1(ID: Node 1) is running but the repmgr node record is inactive
```

Le nœud 1, ancien nœud principal, et le nœud 3, nœud en veille qui suit l'ancien nœud principal, fournissent tous deux des données repmgr inexactes.

```
     ID |  Name    | Role    | Status              | Upstream |Location | Connection string
--------+----------+---------+---------------------+----------+---------+-----------------------
 Node 1 |Node1 name| primary |   * running         |          | default | host=host IP address
user=repmgr dbname=repmgr
 Node 2 |Node2 name| standby |! running as primary |Node1 name| default | host=host IP address
user=repmgr dbname=repmgr
 Node 3 |Node3 name| standby |     running         |Node1 name| default | host=host IP address
user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 2(ID: Node 2) is registered as standby but running as primary
```

Exemple : Exécution de `repmgr cluster show` sur un nœud en veille

L'exécution de la commande sur un nœud en veille qui suit le nœud principal actuel entraîne une sortie système avec des données repmgr correctes identiques à celles présentes sur le nœud principal actuel.

L'exécution de la commande sur un nœud en veille qui suit l'ancien nœud principal génère une sortie système comportant des données inexactes de repmgr identiques à celles présentes sur l'ancien nœud principal.

Entrées de journal

Si un ancien nœud principal qui a échoué revient en ligne après que vous avez promu un nœud en veille comme nouveau nœud principal, les entrées suivantes figurent dans le fichier `update-repmgr-data.log` sur tous les nœuds avec des données repmgr inexactes.

```
ERROR: An old primary is running in the repmgr cluster.
ERROR: Manual intervention is required to repair the repmgr cluster.
ERROR: The first step should be to shutdown and unregister the old primary.
```

Permuter les rôles de la cellule principale et de la cellule en veille dans un cluster haute disponibilité de base de données

Vous pouvez utiliser une commande repmgr pour permuter les rôles du nœud principal et de l'un des nœuds en veille dans votre cluster haute disponibilité de votre base de données lors d'une maintenance planifiée.

Conditions préalables

- Placez toutes les cellules vCloud Director faisant partie du cluster haute disponibilité en mode de maintenance.
- Vérifiez que tous les nœuds du cluster sont sains et en ligne.

Procédure

1. Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur **`racine`** au système d'exploitation du nœud en veille que vous souhaitez promouvoir.
2. Remplacez l'utilisateur par **`postgres`**.

   ```
   sudo -i -u postgres
   ```

3. (Facultatif) Vérifiez que les conditions préalables pour la permutation sont remplies en exécutant la commande avec l'option `--dry-run`.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/
   repmgr.conf --siblings-follow --dry-run
   ```

4. Permutez les rôles de la cellule principale et de la cellule en veille.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/
   repmgr.conf --siblings-follow
   ```

Résultats

La dernière ligne de la sortie de la console indique que la permutation de la cellule en veille a abouti.

Étape suivante

1 Exécutez la commande **reconfigure-database** pour mettre à jour l'adresse IP de la base de données sur toutes les cellules vCloud Director. Reportez-vous à la section Mettre à jour les adresses IP de la base de données sur les cellules vCloud Director.

2 Lorsque vous reconfigurez les cellules vCloud Director dans le groupe de serveurs pour qu'elles pointent vers la nouvelle base de données principale, sortez du mode de maintenance toutes les cellules vCloud Director faisant partie du cluster haute disponibilité.

Annuler l'enregistrement d'un nœud en veille ayant échoué ou inaccessible dans un cluster haute disponibilité de base de données

Vous pouvez utiliser repmgr sur un nœud en cours d'exécution sur votre cluster pour annuler l'enregistrement d'un nœud en veille ayant échoué ou inaccessible.

Note Pour que le nœud principal fonctionne normalement, au moins un nœud en veille doit toujours être en cours d'exécution.

Conditions préalables

Pour annuler l'enregistrement d'un nœud en veille qui n'est pas en cours d'exécution, vous devez fournir l'ID du nœud. Pour trouver l'adresse IP, vérifiez l'état du cluster et localisez le nœud. Sur cette ligne, utilisez la valeur de l'hôte de la colonne Chaîne de connexion pour identifier l'adresse IP du nœud. Reportez-vous à Vérifier l'état d'un cluster haute disponibilité de base de données.

Procédure

1 Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur **racine** au système d'exploitation de l'un des nœuds en cours d'exécution du cluster.

2 Remplacez l'utilisateur par **postgres**.

```
sudo -i -u postgres
```

3 Annulez l'enregistrement du nœud ayant échoué ou inaccessible.

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister -f /opt/vmware/vpostgres/current/etc/
repmgr.conf --node-id=ID
```

Résultats

L'annulation de l'enregistrement du nœud supprime les informations du nœud des métadonnées repmgr.

Annuler l'enregistrement d'une cellule principale ayant échoué dans un cluster haute disponibilité de base de données

Si le nœud principal de votre cluster haute disponibilité de base de données échoue et que vous promouvez un nouveau nœud principal, vous devez annuler l'enregistrement du nœud principal ayant échoué pour le supprimer du cluster et éviter des données d'état de cluster incohérentes.

Conditions préalables

- Pour annuler l'enregistrement d'un nœud principal qui n'est pas en cours d'exécution, vous devez fournir l'ID du nœud. Pour trouver l'adresse IP, vérifiez l'état du cluster et localisez le nœud. Sur cette ligne, utilisez la valeur de l'hôte de la colonne Chaîne de connexion pour identifier l'adresse IP du nœud. Consultez Vérifier l'état d'un cluster haute disponibilité de base de données.
- Vérifiez que le nœud principal ayant échoué est inactif et qu'il ne dispose pas des nœuds en veille suivants, puis promouvez un nouveau nœud principal.

Procédure

1. Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur **racine** au système d'exploitation de l'un des nœuds en cours d'exécution dans le cluster.
2. Remplacez l'utilisateur par **postgres**.

   ```
   sudo -i -u postgres
   ```

3. (Facultatif) Pour vérifier que les conditions préalables pour l'annulation de l'enregistrement du nœud sont remplies, exécutez la commande avec l'option `--dry-run`.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID --dry-run
   ```

4. Annulez l'enregistrement du nœud.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID
   ```

Résultats

L'opération supprime le nœud des métadonnées repmgr.

Annuler l'enregistrement d'une cellule en veille en cours d'exécution dans un cluster haute disponibilité de base de données

Si vous souhaitez utiliser un nœud dans un autre rôle, ou si vous souhaitez le supprimer du cluster haute disponibilité, vous devez en annuler l'enregistrement.

Vous pouvez exécuter cette commande pendant le fonctionnement normal du système.

Note Pour que le nœud principal fonctionne normalement, au moins un nœud en veille doit toujours être en cours d'exécution.

Conditions préalables

Pour annuler l'enregistrement d'un nœud en veille, vous devez fournir l'ID du nœud. Pour trouver l'adresse IP, vérifiez l'état du cluster et localisez le nœud. Sur cette ligne, utilisez la valeur de l'hôte de la colonne Chaîne de connexion pour identifier l'adresse IP du nœud. Consultez Vérifier l'état d'un cluster haute disponibilité de base de données.

Procédure

1. Connectez-vous en tant qu'utilisateur **racine** au système d'exploitation de l'un des nœuds en cours d'exécution dans le cluster ou ouvrez une session SSH sur celui-ci.
2. Remplacez l'utilisateur par **postgres**.

   ```
   sudo –i –u postgres
   ```

3. Annulez l'enregistrement du nœud.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr standby unregister ––node–id=node ID –f /opt/vmware/
   vpostgres/current/etc/repmgr.conf
   ```

Résultats

L'annulation de l'enregistrement du nœud supprime l'enregistrement du nœud en veille dans la table de métadonnées interne de la suite d'outils repmgr.

Après l'installation de vCloud Director ou le déploiement du dispositif vCloud Director

10

Après avoir créé le groupe de serveurs vCloud Director, vous pouvez installer les fichiers Microsoft Sysprep et la base de données Cassandra. Si vous utilisez une base de données PostgreSQL, vous pouvez configurer le protocole SSL et ajuster certains paramètres sur la base de données.

Ce chapitre contient les rubriques suivantes :

Installer les fichiers Microsoft Sysprep sur les serveurs

Si votre cloud nécessite la prise en charge de la personnalisation du client pour certains anciens systèmes d'exploitation de Microsoft, vous devez installer les fichiers Microsoft Sysprep appropriés sur chaque membre du groupe de serveurs.

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

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

Conditions préalables

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

Procédure

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

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

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

3 Créez le répertoire `sysprep`.

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

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

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

Tableau 10-1. Affectations de sous-répertoires pour les fichiers Sysprep

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

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

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

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

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

Utilisez la commande `chown` à cet effet.

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

Résultats

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

Personnaliser les points de terminaison publics

Pour répondre aux conditions requises en matière d'équilibrage de charge ou de proxy, vous pouvez modifier les adresses Web du point de terminaison par défaut pour la console Web de vCloud Director, l'API vCloud, le portail de locataires et le proxy de console.

Si vous avez déployé le dispositif vCloud Director, vous devez configurer l'adresse proxy de console publique vCloud Director, car le dispositif utilise une adresse IP unique avec le port personnalisé 8443 pour le service de proxy de console. Reportez-vous à l'étape 5.

Conditions préalables

Seul **l'administrateur système** peut personnaliser les points de terminaison publics.

Procédure

1 Cliquez sur l'onglet **Administration** et, dans le volet de gauche, cliquez sur **Adresses publiques**.

2 Sélectionnez **Personnaliser les points de terminaison publics**.

Décocher cette case rétablit les valeurs par défaut de tous les points de terminaison qui ne sont pas affichées sur la page.

3 Pour personnaliser l'API REST vCloud et les URL OpenAPI, modifiez les points de terminaison de l'**API**.

a Entrez une URL de base HTTP personnalisée.

Par exemple, si vous définissez l'URL de base HTTP sur **`http://vcloud.example.com`**, vous pouvez accéder à l'API vCloud à l'adresse `http://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI vCloud à l'adresse `http://vcloud.example.com/cloudapi`.

b Entrez une URL de base HTTPS personnalisée pour l'API REST et cliquez sur **Parcourir** pour télécharger les certificats qui établissent la chaîne d'approbation pour ce point de terminaison.

Par exemple, si vous définissez l'URL de base HTTPS de l'API REST sur **`https://vcloud.example.com`**, vous pouvez accéder à l'API vCloud à l'adresse `https://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI vCloud à l'adresse `https://vcloud.example.com/cloudapi`.

La chaîne de certificats doit correspondre au certificat utilisé par le point de terminaison de service, qui est le certificat téléchargé vers chaque keystore de la cellule vCloud Director avec l'alias `http` ou le certificat VIP de l'équilibrage de charge si une terminaison SSL est utilisée. La chaîne de certificats doit inclure un certificat de point de terminaison, des certificats intermédiaires et un certificat racine au format `PEM` sans clé privée.

4 Pour personnaliser les URL du portail de locataires vCloud Director, modifiez les points de terminaison du **Portail de locataires**.

- Pour configurer le portail de locataires vCloud Director afin qu'il utilise les mêmes points de terminaison et la même chaîne de certificats que ceux que vous avez spécifiés à l'Étape Étape 3, sélectionnez **Copier les paramètres de l'URL de l'API**.
- Pour configurer le portail de locataires vCloud Director afin qu'il utilise des points de terminaison et une chaîne de certificats différents, procédez comme suit.

  a Désélectionnez **Copier les paramètres de l'URL de l'API**.

b Entrez une URL de base HTTP personnalisée.

Par exemple, si vous définissez l'URL de base HTTP sur **http://vcloud.example.com**, vous pouvez accéder au portail de locataires à l'adresse `http://vcloud.example.com/tenant/`*`org_name`*.

c Entrez une URL de base HTTPS personnalisée pour l'API REST et cliquez sur **Parcourir** pour télécharger les certificats qui établissent la chaîne d'approbation pour ce point de terminaison.

Par exemple, si vous définissez l'URL de base HTTPS de l'API REST sur **https://vcloud.example.com**, vous pouvez accéder au portail de locataires à l'adresse `https://vcloud.example.com/tenant/`*`org_name`*.

La chaîne de certificats doit correspondre au certificat utilisé par le point de terminaison de service, qui est le certificat téléchargé vers chaque keystore de la cellule vCloud Director avec l'alias `http` ou le certificat VIP de l'équilibrage de charge si une terminaison SSL est utilisée. La chaîne de certificats doit inclure un certificat de point de terminaison, des certificats intermédiaires et un certificat racine au format `PEM` sans clé privée.

5 Pour personnaliser les URL de vCloud Director Web Console et l'adresse proxy de la console, modifiez les points de terminaison de la **Console Web**.

a Entrez une URL publique vCloud Director personnalisée pour les connexions HTTP.

L'URL doit inclure `/cloud`.

Par exemple, si vous définissez l'URL publique vCloud Director sur **`http://vcloud.example.com/cloud`**, vous pouvez accéder à la vCloud Director Web Console à l'adresse `http://vcloud.example.com/cloud`.

b Entrez une URL d'API REST personnalisée pour les connexions HTTPS et cliquez sur **Parcourir** pour télécharger les certificats qui établissent la chaîne d'approbation pour ce point de terminaison.

L'URL doit inclure `/cloud`.

Par exemple, si vous définissez l'URL de base sur **`https://vcloud.example.com`**, vous pouvez accéder à la vCloud Director Web Console à l'adresse `https://vcloud.example.com/cloud`.

La chaîne de certificats doit correspondre au certificat utilisé par le point de terminaison de service, qui est le certificat téléchargé vers chaque keystore de la cellule vCloud Director avec l'alias **`HTTP`** ou le certificat VIP de l'équilibrage de charge si une terminaison SSL est utilisée. La chaîne de certificats doit inclure un certificat de point de terminaison, des certificats intermédiaires et un certificat racine au format `PEM` sans clé privée.

c Entrez une adresse proxy de console publique vCloud Director personnalisée.

Cette adresse est le nom de domaine complet (FQDN) du serveur vCloud Director ou de l'équilibrage de charge avec le numéro de port. Le port par défaut est 443.

Important Le dispositif vCloud Director utilise sa carte réseau `eth0` avec le port personnalisé 8443 pour le service de proxy de console.

Les terminaisons SSL des connexions de proxy de console sur un équilibrage de charge ne sont pas prises en charge. Le certificat de proxy de la console est téléchargé sur chaque keystore de la cellule vCloud Director avec l'alias **`consoleproxy`**.

Par exemple, pour une instance de dispositif vCloud Director ayant le nom de domaine complet `vcloud.example.com`, entrez **`vcloud.example.com:8443`**.

La console Web de vCloud Director utilise l'adresse proxy de la console lors de l'ouverture d'une fenêtre de console distante sur une machine virtuelle.

6 Pour enregistrer les modifications, cliquez sur **Appliquer**.

Installer et configurer un broker AMQP RabbitMQ

AMQP (Advanced Message Queuing Protocol) est une norme ouverte de file d'attente de messages qui prend en charge une messagerie flexible pour les systèmes d'entreprise. vCloud

Director utilise le broker AMQP RabbitMQ pour fournir le bus de messages utilisé par les services d'extension, les extensions d'objet et les notifications.

Procédure

1 Téléchargez le serveur RabbitMQ depuis https://www.rabbitmq.com/download.html.

Reportez-vous à la section *Notes de mise à jour de vCloud Director* pour connaître la liste des versions de RabbitMQ prises en charge.

2 Suivez les instructions d'installation de RabbitMQ et installez-le sur un hôte pris en charge.

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 requises pour la configuration de 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`.
- Hôte virtuel RabbitMQ. Par défaut « / ».

Étape suivante

Par défaut, le service AMQP de vCloud Director envoie des messages non chiffrés. Vous pouvez configurer le service AMQP pour chiffrer ces messages en utilisant SSL. Vous pouvez également configurer le service afin de vérifier le certificat du broker à l'aide du magasin d'approbations JCEKS par défaut de l'environnement d'exécution Java sur la cellule vCloud Director, généralement situé à `$VCLOUD_HOME/jre/lib/security/cacerts`.

Pour activer SSL avec le service AMQP de vCloud Director :

1 Dans la console Web de vCloud Director, cliquez sur l'onglet **Administration**, puis sur **Extensibilité**.

2 Cliquez sur **Extensibilité**, puis cliquez sur l'onglet **Paramètres**.

3 Dans la section **Paramètres du courtier AMQP**, sélectionnez **Utiliser SSL**.

4 Cochez la case **Accepter tous les certificats** ou 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

Installer et configurer une base de données Cassandra pour stocker les données de mesure historiques

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

Cassandra est une base de données open source que vous pouvez utiliser pour fournir au magasin de sauvegarde une solution haute performance évolutive pour la collecte des données chronologiques telles que des mesures de machine virtuelle. Si vous souhaitez que vCloud Director prenne en charge la récupération des mesures historiques des machines virtuelles, vous devez installer et configurer un cluster Cassandra et utiliser `cell-management-tool` pour connecter le cluster à vCloud Director. La récupération des mesures historiques ne nécessite pas l'utilisation du logiciel de base de données facultatif.

Conditions préalables

- Vérifiez que vCloud Director est installé et qu'il fonctionne avant de configurer le logiciel de base de données facultatif.
- Si vous ne vous êtes pas encore familiarisé avec Cassandra, consultez la documentation à l'adresse http://cassandra.apache.org/.
- Reportez-vous aux *Notes de mise à jour de vCloud Director* pour une liste des versions de Cassandra prises en charge et pouvant être utilisées comme base de données de mesures. Vous pouvez télécharger Cassandra à l'adresse http://cassandra.apache.org/download/.
- Installez et configurez le cluster Cassandra :
  - Le cluster Cassandra doit inclure au moins quatre machines virtuelles déployées sur plusieurs hôtes.
  - Deux nœuds de valeurs initiales de Cassandra sont requis.
  - Activez le chiffrement client à nœud Cassandra. Reportez-vous à http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html.
  - Activez l'authentification utilisateur de Cassandra. Reportez-vous à http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html.
  - Activez Java Native Access (JNA) version 3.2.7 ou version ultérieure sur chaque cluster Cassandra.
  - Le chiffrement nœud à nœud Cassandra est facultatif.
  - L'utilisation de SSL avec Cassandra est facultative. Si vous décidez de ne pas activer SSL pour Cassandra, vous devez définir le paramètre de configuration `cassandra.use.ssl` sur `0` dans le fichier `global.properties` sur chaque cellule (`$VCLOUD_HOME/etc/global.properties`).

Procédure

1 Utilisez l'utilitaire `cell-management-tool` pour configurer une connexion entre vCloud Director et les nœuds du cluster Cassandra.

   Dans l'exemple de commande suivant, *node1-ip*, *node2-ip*, *node3-ip* et *node4-ip* sont les adresses IP des membres du cluster Cassandra. Le port par défaut (9042) est utilisé. Les données de mesures sont conservées pendant 15 jours.

   ```
   [root@cell1 /opt/vmware/vcloud-director/
   bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
   ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
   ```

   Pour plus d'informations sur l'utilisation de l'outil de gestion des cellules, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.

2 (Facultatif) Si vous mettez à niveau vCloud Director à partir de la version 9.1, utilisez le `cell-management-tool` pour configurer la base de données de mesures afin de stocker les mesures cumulées.

   Exécutez une commande semblable à l'exemple suivant :

   ```
   [root@cell1 /opt/vmware/vcloud-director/
   bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password 'P@55w0rd'
   ```

3 Redémarrez chaque cellule vCloud Director.

Effectuer des configurations supplémentaires sur la base de données PostgreSQL externe

Après avoir créé le groupe de serveurs vCloud Director, vous pouvez configurer la base de données PostgreSQL externe pour exiger des connexions SSL à partir des cellules vCloud Director et ajuster certains paramètres de base de données pour des performances optimales.

Les connexions les plus sécurisées nécessitent un certificat SSL dûment signé, qui inclut une chaîne d'approbation complète associée à une racine dans une autorité de certification publique bien connue. Vous pouvez également utiliser un certificat SSL auto-signé ou un certificat SSL signé par une autorité de certification privée, mais vous devez importer ce certificat dans le truststore vCloud Director.

Pour obtenir les performances optimales correspondant aux spécifications et aux exigences de votre système, vous pouvez ajuster les configurations de base de données et les paramètres de nettoyage automatique dans le fichier de configuration de la base de données.

Procédure

1 Configurer des connexions SSL entre vCloud Director et la base de données PostgreSQL.

   a Si vous avez utilisé un certificat autosigné ou privé pour la base de données PostgreSQL externe, dans chaque cellule vCloud Director, exécutez la commande d'importation du certificat de la base de données dans le truststore vCloud Director.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
cell-management-tool import-trusted-certificates --source path_to_self-signed_or_private_cert
```

   b Exécutez la commande d'activation des connexions SSL entre vCloud Director et PostgreSQL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
 cell-management-tool reconfigure-database --database-ssl true
```

   Vous pouvez exécuter cette commande sur toutes les cellules du groupe de serveurs à l'aide de l'option --private-key-path.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
 cell-management-tool reconfigure-database --database-ssl true --private-key-path
path_to_private_key
```

   Pour plus d'informations sur l'utilisation de l'outil de gestion des cellules, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.

2 Modifiez les configurations de base de données dans le fichier `postgresql.conf` pour qu'elles correspondent aux spécifications de votre système.

   Par exemple, pour un système disposant de 16 Go de mémoire, vous pouvez utiliser le fragment suivant :

```
max_connections = 500
# Set effective cache size to 50% of total memory.
effective_cache_size = 8GB
# Set shared buffers to 25% of total memory
shared_buffers = 4GB
```

3 Modifiez les paramètres de nettoyage automatique dans le fichier `postgresql.conf` pour qu'ils correspondent à la configuration requise.

   Pour les charges de travail vCloud Director standard, vous pouvez utiliser le fragment suivant :

```
autovacuum = on
track_counts = on
autovacuum_max_workers = 3
autovacuum_naptime = 1min
autovacuum_vacuum_cost_limit = 2400
```

   Le système définit une valeur `autovacuum_vacuum_scale_factor` personnalisée pour l'activité et les tables `activity_parameters`.

Étape suivante

Si vous avez modifié le fichier `postgresql.conf`, vous devez redémarrer la base de données.

Mise à niveau de vCloud Director et application de correctifs au dispositif vCloud Director

11

Vous pouvez effectuer une mise à niveau orchestrée, mettre à niveau manuellement vCloud Director vers une nouvelle version ou appliquer des correctifs aux déploiements du dispositif vCloud Director.

Si votre groupe de serveurs vCloud Director existant comprend des installations de vCloud Director sur Linux, vous pouvez utiliser le programme d'installation de vCloud Director pour Linux pour mettre à niveau votre environnement. Vous pouvez également migrer votre environnement vers le dispositif vCloud Director 9.7. Reportez-vous à Chapitre 12 Migration vers le dispositif vCloud Director.

Si votre groupe de serveurs vCloud Director existant se compose de déploiements de dispositifs vCloud Director 9.5, vous pouvez uniquement migrer votre environnement vers le dispositif vCloud Director 9.7. Vous utilisez le programme d'installation de vCloud Director pour Linux pour mettre à niveau l'environnement existant uniquement dans le cadre du workflow de migration. Reportez-vous à Chapitre 12 Migration vers le dispositif vCloud Director.

Vous pouvez soit Effectuer une mise à niveau orchestrée d'une Installation vCloud Director, soit Mettre à niveau manuellement une Installation vCloud Director. Avec la mise à niveau orchestrée, vous exécutez une commande unique qui met à niveau toutes les cellules dans le groupe de serveurs et la base de données. Avec la mise à niveau manuelle, vous mettez à niveau chaque cellule et la base de données dans un ordre donné.

À partir de la version vCloud Director 9.5 :

- Les bases de données Oracle ne sont plus prises en charge. Si votre installation existante de vCloud Director utilise une base de données Oracle, reportez-vous à la section Workflow de mise à niveau d'une installation de vCloud Director avec une base de données Oracle.
- L'activation et la désactivation des hôtes ESXi ne sont plus prises en charge. Avant de démarrer la mise à niveau, vous devez activer tous les hôtes ESXi. Pour mettre les hôtes ESXi en mode de maintenance en utilisant vSphere Web Client.
- vCloud Director utilise Java avec une prise en charge améliorée de LDAP. Si vous utilisez un serveur LDAPS, vous devez vérifier que vous disposez d'un certificat correctement construit pour éviter les échecs de connexion LDAP. Pour plus d'informations, consultez les *Modifications de version de Java 8* à l'adresse https://www.java.com.

Lorsque vous mettez à niveau vCloud Director, la nouvelle version doit être compatible avec les composants suivants de votre installation existante :

- Le logiciel de base de données que vous utilisez actuellement pour la base de données vCloud Director.

  Si votre installation existante de vCloud Director utilise une base de données Oracle, reportez-vous à la section Workflow de mise à niveau d'une installation de vCloud Director avec une base de données Oracle.

- La version de VMware vSphere ® que vous utilisez actuellement.
- La version de VMware NSX® que vous utilisez actuellement.

Pour plus d'informations sur les chemins de mise à niveau et la compatibilité de vCloud Director avec d'autres produits VMware et avec les bases de données de tiers, consultez les *Matrices d'interopérabilité des produits VMware* à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Si vous prévoyez de mettre à niveau les composants vSphere ou NSX dans le cadre de la mise à niveau de vCloud Director, vous devez les mettre à niveau Chapitre 13 Après la mise à niveau ou la migration de vCloud Director.

Après la mise à niveau d'au moins un serveur vCloud Director, vous pouvez mettre à niveau la base de données vCloud Director. La base de données enregistre 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 une mise à niveau, vous devez vérifier qu'aucune tâche n'est active sur un serveur avant de commencer la mise à niveau.

La mise à niveau conserve également les artéfacts suivants, qui ne sont pas stockés dans la base de données vCloud Director :

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

La mise à niveau nécessite une interruption de service vCloud Director suffisante pour mettre à niveau tous les serveurs dans le groupe de serveurs et la base de données. Si vous utilisez un équilibrage de charge, vous pouvez le configurer pour qu'il renvoie un message du style `Le système est hors ligne pour la mise à niveau.`

Workflow de mise à niveau d'une installation de vCloud Director avec une base de données Oracle

Avant de procéder à la mise à niveau d'une installation vCloud Director qui utilise une base de données Oracle, vous devez migrer la base de données vers PostgreSQL à partir de la version 9.1 de vCloud Director.

1 Si votre version actuelle de vCloud Director est antérieure à la version 9.1, effectuez une mise à niveau vers celle-ci.

Pour en savoir plus sur la mise à niveau de vCloud Director vers la version 9.1, reportez-vous au *Guide d'installation, de configuration et de mise à niveau de vCloud Director* 9.1.

2 Lorsque la version de votre installation de vCloud Director est la version 9.1, migrez la base de données Oracle vers une base de données PostreSQL.

Pour plus d'informations sur la migration vers une base de données PostgreSQL, reportez-vous à la référence de l'outil de gestion des cellules dans la documentation *Guide de l'administrateur de vCloud Director*.

3 Mettez à niveau votre installation de vCloud Director à partir de la version 9.1. Vous pouvez utiliser Effectuer une mise à niveau orchestrée d'une Installation vCloud Director ou Mettre à niveau manuellement une Installation vCloud Director.

Application de correctifs au déploiement du dispositif vCloud Director

Vous pouvez appliquer un correctif au dispositif vCloud Director pour améliorer sa fonctionnalité ou sa sécurité. Reportez-vous au Corrigez le déploiement du dispositif vCloud Director. Après l'application du correctif à chaque dispositif vCloud Director et la mise à niveau de la base de données, vous devez redémarrer les services vCloud Director dans le groupe de serveurs pour le remettre en ligne.

Ce chapitre contient les rubriques suivantes :

- Effectuer une mise à niveau orchestrée d'une Installation vCloud Director
- Mettre à niveau manuellement une Installation vCloud Director
- Référence de l'utilitaire de mise à niveau de la base de données
- Corrigez le déploiement du dispositif vCloud Director

Effectuer une mise à niveau orchestrée d'une Installation vCloud Director

Vous pouvez mettre à niveau toutes les cellules dans le groupe de serveurs ainsi que dans la base de données partagée en exécutant le programme d'installation de vCloud Director avec l'option `--private-key-path`.

Vous pouvez utiliser le programme d'installation de vCloud Director pour Linux pour mettre à niveau un groupe de serveurs vCloud Director composé des installations de vCloud Director sur un système d'exploitation Linux pris en charge. Si votre groupe de serveurs vCloud Director se compose des déploiements de dispositifs vCloud Director 9.5, vous utilisez le programme d'installation de vCloud Director pour Linux pour mettre à niveau votre environnement existant uniquement dans le cadre du workflow de migration. Reportez-vous à Chapitre 12 Migration vers le dispositif vCloud Director.

vCloud Director pour Linux est distribué en tant que fichier exécutable signé numériquement portant un nom sous la forme `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, où *v.v.v* représente la version du produit et *nnnnnn* le numéro de build. Par exemple : `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. L'exécution de cet exécutable installe ou met à niveau vCloud Director.

Lorsque vous exécutez le programme d'installation vCloud Director avec l'option `--private-key-path`, vous pouvez ajouter d'autres options de commande de l'utilitaire `upgrade`, par exemple, `--maintenance-cell`. Pour plus d'informations sur les options de l'utilitaire `upgrade` de base de données, consultez Référence de l'utilitaire de mise à niveau de la base de données.

Conditions préalables

- Vérifiez que votre base de données vCloud Director, les composants vSphere et les composants NSX sont compatibles avec la nouvelle version de vCloud Director.

  Important Si votre installation vCloud Director existante utilise une base de données Oracle, vérifiez que vous avez migré vers une base de données PostgreSQL à partir de la version 9.1 de vCloud Director. Reportez-vous à la section Workflow de mise à niveau d'une installation de vCloud Director avec une base de données Oracle.

- 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, il n'est pas nécessaire de la revérifier pendant l'installation. Reportez-vous à Téléchargement et installation de la clé publique VMware.
- Vérifiez que vous disposez d'une clé de licence valide pour utiliser la version du logiciel vCloud Director vers laquelle vous effectuez la mise à niveau.
- Vérifiez que toutes les cellules autorisent les connexions SSH à partir du super utilisateur sans mot de passe. Pour effectuer une vérification, vous pouvez exécuter la commande Linux suivante :

  ```
  sudo -u vcloud ssh -i private-key-path root@cell-ip
  ```

  Cet exemple définit votre identité sur `vcloud`, puis établit une connexion SSH à la cellule dans *cell-ip* en tant que racine, mais ne fournit pas de mot de passe racine. Si la clé privée dans *private-key-path* sur la cellule locale est lisible par l'utilisateur `vcloud.vcloud` et que la clé publique correspondante existe dans le fichier `authorized-keys` pour l'utilisateur racine dans *cell-ip*, la commande aboutit.

  Note L'utilisateur `vcloud`, le groupe `vcloud` et le compte `vcloud.vcloud` sont créés par le programme d'installation de vCloud Director pour servir d'identité sous laquelle les processus de vCloud Director s'exécutent. L'utilisateur de `vcloud` n'a aucun mot de passe.

- Vérifiez que tous les hôtes ESXi sont activés. À partir de vCloud Director 9.5, les hôtes ESXi désactivés ne sont pas pris en charge.
- Vérifiez que tous les serveurs du groupe de serveurs peuvent accéder au stockage partagé du serveur de transfert. Reportez-vous à Préparation du stockage du serveur de transfert.
- Si votre installation de vCloud Director utilise un serveur LDAPS, vérifiez que vous disposez d'un certificat correctement construit pour Java 8 Update 181 afin d'éviter les échecs de connexion LDAP après la mise à niveau. Pour plus d'informations, consultez les *Modifications de version de Java 8* à l'adresse https://www.java.com.

Procédure

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

   Si vous avez acheté le logiciel sur un support, copiez le fichier d'installation vers un emplacement accessible au serveur cible.
3. Vérifiez que la somme de contrôle du téléchargement correspond au total de contrôle publié sur la page de téléchargement.

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

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

   La commande renvoie la somme de contrôle du fichier d'installation qui doit correspondre à la somme de contrôle MD5 à partir de la page de téléchargement.
4. Assurez-vous que le fichier d'installation est exécutable.

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

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

5 Dans une console, un shell ou une fenêtre de terminal, exécutez le fichier d'installation avec l'option `--private-key-path` et le nom du chemin d'accès à la clé privée de la cellule cible.

Vous pouvez ajouter d'autres options de commande de l'utilitaire `upgrade` de base de données.

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

Note 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 détecte une version antérieure de vCloud Director et vous invite à confirmer la mise à niveau.

Si le programme d'installation détecte une version de vCloud Director 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.

6 Entrez **y** et appuyez sur Entrée pour confirmer la mise à niveau.

Résultats

Le programme d'installation démarre le workflow de mise à niveau à plusieurs cellules suivant.

1 Il vérifie que l'hôte de la cellule actuelle répond à toute la configuration requise.

2 Il décompresse le module RPM vCloud Director.

3 Il met à jour le logiciel vCloud Director sur la cellule actuelle.

4 Il met à niveau la base de données vCloud Director.

5 Il met à niveau le logiciel vCloud Director sur chacune des cellules restantes, puis redémarre les services vCloud Director sur la cellule.

6 Redémarre les services vCloud Director sur la cellule actuelle.

Étape suivante

Démarrez les services vCloud Director sur toutes les cellules du groupe de serveurs.

Vous pouvez maintenant Mettre à niveau chaque instance de NSX Manager associée à un système vCenter Server relié, puis Mettre à niveau les systèmes vCenter Server, les hôtes ESXi et les dispositifs NSX Edge .

Mettre à niveau manuellement une Installation vCloud Director

Vous pouvez mettre à niveau une seule cellule en exécutant le programme d'installation vCloud Director sans les options de commande. Avant de redémarrer une cellule mise à niveau, vous devez mettre à niveau le schéma de la base de données. Vous mettez à niveau le schéma de la base de données après la mise à niveau d'au moins une cellule du groupe de serveurs.

Vous pouvez utiliser le programme d'installation de vCloud Director pour Linux pour mettre à niveau un groupe de serveurs vCloud Director composé des installations de vCloud Director sur un système d'exploitation Linux pris en charge. Si votre groupe de serveurs vCloud Director se compose des déploiements de dispositifs vCloud Director 9.5, vous utilisez le programme d'installation de vCloud Director pour Linux pour mettre à niveau votre environnement existant uniquement dans le cadre du workflow de migration. Reportez-vous à Chapitre 12 Migration vers le dispositif vCloud Director.

Pour une installation vCloud Director à plusieurs cellules, au lieu mettre à niveau manuellement chaque cellule et la base de données dans une séquence, vous pouvez Effectuer une mise à niveau orchestrée d'une Installation vCloud Director.

Conditions préalables

- Vérifiez que votre base de données vCloud Director, les composants vSphere et les composants NSX sont compatibles avec la nouvelle version de vCloud Director.

  Important Si votre installation vCloud Director existante utilise une base de données Oracle, vérifiez que vous avez migré vers une base de données PostgreSQL à partir de la version 9.1 de vCloud Director. Reportez-vous à la section Workflow de mise à niveau d'une installation de vCloud Director avec une base de données Oracle.

- Vérifiez que vous disposez des informations d'identification de super utilisateur pour les serveurs dans le groupe de serveurs vCloud Director.
- 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, il n'est pas nécessaire de la revérifier pendant l'installation. Reportez-vous à Téléchargement et installation de la clé publique VMware.
- Vérifiez que vous disposez d'une clé de licence valide pour utiliser la version du logiciel vCloud Director vers laquelle vous effectuez la mise à niveau.
- Vérifiez que tous les hôtes ESXi sont activés. À partir de vCloud Director 9.5, les hôtes ESXi désactivés ne sont pas pris en charge.

Procédure

1. Mise à niveau d'une cellule vCloud Director

   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.

2. Mise à niveau de la base de données vCloud Director

   À partir d'un serveur vCloud Director mis à niveau, vous exécutez un outil qui met à niveau la base de données vCloud Director. Vous ne devez pas redémarrer n'importe quel serveur vCloud Director mis à niveau avant la mise à niveau de la base de données partagée.

Étape suivante

Une fois que vous avez mis à niveau tous les serveurs vCloud Director dans le groupe de serveurs et la base de données, vous pouvez démarrer les services vCloud Director sur toutes les cellules.

Vous pouvez Mettre à niveau chaque instance de NSX Manager associée à un système vCenter Server relié, puis vous pouvez Mettre à niveau les systèmes vCenter Server, les hôtes ESXi et les dispositifs NSX Edge .

Mise à niveau d'une cellule vCloud Director

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.

vCloud Director pour Linux est distribué en tant que fichier exécutable signé numériquement portant un nom sous la forme `vmware-vcloud-director-distribution-`*v.v.v*`-`*nnnnnn*`.bin`, où *v.v.v* représente la version du produit et *nnnnnn* le numéro de build. Par exemple : `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. L'exécution de cet exécutable installe ou met à niveau vCloud Director.

Pour une installation vCloud Director à plusieurs cellule, vous devez exécuter le programme d'installation vCloud Director sur chaque membre du groupe de serveurs vCloud Director.

Procédure

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

   Si vous avez acheté le logiciel sur un support, copiez le fichier d'installation vers un emplacement accessible au serveur cible.
3. Vérifiez que la somme de contrôle du téléchargement correspond au total de contrôle publié sur la page de téléchargement.

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

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

   La commande renvoie la somme de contrôle du fichier d'installation qui doit correspondre à la somme de contrôle MD5 à partir de la page de téléchargement.

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

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

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

5 Exécutez le fichier d'installation.

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

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

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

Note 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 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 le programme d'installation détecte une version antérieure de vCloud Director, il vous invite à confirmer la mise à niveau.

6 Entrez **y** et appuyez sur Entrée pour confirmer la mise à niveau.

Le programme d'installation démarre le workflow de mise à niveau suivant.

a Il vérifie que l'hôte est conforme à toute la configuration requise.

b Il décompresse le module RPM vCloud Director.

c Une fois que tous les travaux vCloud Director actifs sur la cellule sont terminés, arrêtez les services vCloud Director sur le serveur et met à niveau le logiciel vCloud Director installé.

Si vous n'avez pas installé la clé publique VMware sur le serveur cible, le programme d'installation affiche un avertissement au format suivant :

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

Lorsque vous modifiez le fichier `global.properties` existant sur le serveur cible, le programme d'installation affiche un avertissement au format suivant :

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

Note Si vous avez déjà mis à jour le fichier `global.properties` existant, vous pouvez récupérer les modifications à partir de `global.properties.rpmnew`.

7 (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	Pour conserver vos modifications, fusionnez `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` avec le fichier `/opt/vmware/vcloud-director/etc/log4j.properties` existant.

Résultats

Lorsque la mise à niveau de vCloud Director se termine, le programme d'installation affiche un message avec des informations sur l'emplacement des anciens fichiers de configuration. Ensuite, le programme d'installation vous invite à exécuter l'outil de mise à niveau de base de données.

Étape suivante

Si ce n'est pas déjà fait, vous pouvez mettre à niveau la base de données vCloud Director.

Répétez cette procédure sur chaque cellule vCloud Director du groupe de serveurs.

Important Ne démarrez pas les services vCloud Director tant que vous n'avez pas mis à niveau toutes les cellules dans le groupe de serveurs et la base de données.

Mise à niveau de la base de données vCloud Director

À partir d'un serveur vCloud Director mis à niveau, vous exécutez un outil qui met à niveau la base de données vCloud Director. Vous ne devez pas redémarrer n'importe quel serveur vCloud Director mis à niveau avant la mise à niveau de la base de données partagée.

Les informations sur les tâches en cours et récemment terminées sont conservées dans la base de données vCloud Director. Comme la mise à niveau de la base de données invalide ces informations, l'utilitaire de mise à niveau de base de données vérifie qu'aucune tâche n'est en cours d'exécution lorsque la mise à niveau commence.

Toutes les cellules d'un groupe de serveurs vCloud Director partagent la même base de données. Quel que soit le nombre de cellules que vous mettez à niveau, vous ne mettez à niveau la base de données qu'une seule fois. Après la mise à niveau de la base de données, les cellules vCloud Director qui ne sont pas mises à niveau ne peuvent pas se connecter à la base de données. Vous devez mettre à niveau toutes les cellules afin qu'elles se connectent à la base de données mise à niveau.

Conditions préalables

- Sauvegardez votre base de données existante. Suivez pour cela la procédure recommandée par le fournisseur du logiciel de base de données.

- Vérifiez que toutes les cellules vCloud Director du groupe de serveurs sont arrêtées. Les cellules mises à niveau sont arrêtées pendant la mise à niveau. S'il existe des serveurs vCloud Director qui ne sont pas mis à niveau, vous pouvez utiliser l'outil de gestion de cellules pour mettre en veille et arrêter leurs services. Pour plus d'informations sur la façon de gérer une cellule à l'aide de l'outil de gestion des cellules, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.
- Si votre installation vCloud Director utilise une base de données Oracle, migrez vers une base de données PostgeSQL. Pour plus d'informations sur la migration vers une base de données PostgreSQL, reportez-vous à la référence de l'outil de gestion des cellules dans *Guide de l'administrateur de vCloud Director*.
- Vérifier la Référence de l'utilitaire de mise à niveau de la base de données. Les options et arguments ne sont pas obligatoires.

Procédure

1 Exécutez l'utilitaire `upgrade` de base de données avec ou sans options.

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

Si l'utilitaire de mise à niveau de base de données détecte une version incompatible de NSX Manager, il affiche un message d'avertissement et annule la mise à niveau.

2 Sur l'invite, entrez **y** et appuyez sur Entrée pour confirmer la mise à niveau de la base de données.

3 À l'invite, entrez **y** et appuyez sur Entrée pour confirmer que vous avez sauvegardé la base de données.

Si vous avez utilisé l'option `--backup-completed`, l'utilitaire ignore cette invite.

4 Si l'utilitaire détecte une cellule active, sur l'invite pour continuer, entrez **n** pour quitter le shell, puis vérifiez qu'aucune cellule n'est en cours d'exécution et réessayez la mise à niveau de Étape Étape 1.

Résultats

L'outil de mise à niveau de la base de données s'exécute et affiche des messages de progression. Lorsque la mise à niveau est terminée, vous êtes invité à démarrer le service vCloud Director sur le serveur en cours.

Étape suivante

Entrez **o** et appuyez sur Entrée ou démarrez le service ultérieurement en exécutant la commande `service vmware-vcd start`.

Vous pouvez démarrer les services des serveurs vCloud Director mis à niveau.

Vous pouvez mettre à niveau les autres vCloud Director membres du serveur de groupe et démarrer leurs services. Reportez-vous à Mise à niveau d'une cellule vCloud Director.

Référence de l'utilitaire de mise à niveau de la base de données

Lorsque vous exécutez l'utilitaire `upgrade`, vous fournissez les informations de configuration en ligne de commande sous forme d'options et d'arguments.

Tableau 11-1. Arguments et options de l'utilitaire de mise à niveau de base de données

Option	Argument	Description
`--backup-completed`	Aucun	Indique que vous avez effectué une sauvegarde de vCloud Director. Lorsque vous incluez cette option, l'utilitaire de mise à niveau ne vous invite pas à sauvegarder la base de données.
`--ceip-user`	Nom d'utilisateur du compte de service CEIP.	Un échec de la mise à niveau se produira si un utilisateur avec ce nom d'utilisateur existe déjà dans l'organisation Système. Par défaut : `phone-home-system-account`
`--enable-ceip`	Choisissez-en un : ■ true ■ false	Spécifie si cette installation participe au programme d'amélioration du produit (CEIP) VMware. Cette option est définie par défaut sur true si elle n'est pas fournie ni définie sur false dans la configuration actuelle. Le programme d'amélioration du produit (CEIP) VMware fournit des informations supplémentaires concernant les données collectées via le CEIP et les fins auxquelles elles sont utilisées par VMware sont définis dans le Centre de confiance et assurance à l'adresse http://www.vmware.com/trustvmware/ceip.html. Vous pouvez utiliser l'outil de gestion de cellules pour joindre ou quitter le programme d'amélioration du produit VMware pour ce produit à tout moment. Reportez-vous à la section « Référence de l'outil de gestion de cellules » dans *Guide de l'administrateur de vCloud Director*.

Tableau 11-1. Arguments et options de l'utilitaire de mise à niveau de base de données (suite)

Option	Argument	Description
`--installer-path`	Chemin d'accès complet au fichier d'installation de vCloud Director. Le fichier d'installation et le répertoire dans lequel il est stocké doivent être accessibles par l'utilisateur vcloud.vcloud.	Ce produit participe au Programme d'amélioration du produit VMware. Les détails concernant les données collectées via le CEIP et les fins auxquelles elles sont utilisées par VMware sont définis dans le Centre de confiance et assurance à l'adresse http://www.vmware.com/trustvmware/ceip.html. Vous pouvez utiliser l'outil de gestion des cellules pour rejoindre ou quitter le Programme d'amélioration du produit VMware à tout moment. Reportez-vous à la section « Référence de l'outil de gestion de cellules » dans le *Guide de l'administrateur de vCloud Director*. Option requise : `--private-key-path` .
`--maintenance-cell`	adresse IP	Adresse IP d'une cellule qui permet à l'utilitaire de mise à niveau de s'exécuter en mode de maintenance pendant la mise à niveau. Cette cellule entre en mode de maintenance avant l'arrêt des autres cellules et reste en mode de maintenance lors de la mise à niveau des autres cellules. Une fois que les autres cellules ont été mises à niveau et qu'une d'elles au moins a redémarré, cette cellule est arrêtée et mise à niveau. Option requise : `--private-key-path` .
`--multisite-user`	Nom d'utilisateur du compte système multi-site.	Ce compte est utilisé par la fonctionnalité multi-site de vCloud Director . Un échec de la mise à niveau se produira si un utilisateur avec ce nom d'utilisateur existe déjà dans l'organisation Système. Par défaut : `multisite-system-account`

Tableau 11-1. Arguments et options de l'utilitaire de mise à niveau de base de données (suite)

Option	Argument	Description
`--private-key-path`	chemin d'accès	Chemin d'accès complet vers la clé privée de la cellule. Lorsque vous utilisez cette option, toutes les cellules du groupe de serveurs sont normalement arrêtées, mises à niveau, puis redémarrées après la mise à niveau de la base de données. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation vCloud Director pour plus d'informations sur ce workflow de mise à niveau.
`--unattended-upgrade`	Aucun	Spécifie une mise à niveau sans assistance.

Si vous utilisez l'option `--private-key-path`, toutes les cellules doivent être configurées pour autoriser les connexions `ssh` depuis le superutilisateur sans mot de passe. Vous pouvez utiliser une ligne de commande Linux semblable à celle indiquée ici pour vérifier cela. Cet exemple définit votre identité sur `vcloud`, puis établit une connexion `ssh` à la cellule dans *cell-ip* en tant que `root`, mais ne fournit pas de mot de passe racine.

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

Si la clé privée dans *private-key-path* sur la cellule locale est lisible par l'utilisateur `vcloud.vcloud` et que la clé publique correspondante a été ajoutée au fichier `authorized-keys` pour l'utilisateur racine dans *cell-ip*, la commande aboutit.

Note L'utilisateur `vcloud`, le groupe `vcloud` et le compte `vcloud.vcloud` sont créés par le programme d'installation de vCloud Director pour servir d'identité sous laquelle les processus de vCloud Director s'exécutent. L'utilisateur de `vcloud` n'a aucun mot de passe.

Corrigez le déploiement du dispositif vCloud Director

Vous pouvez mettre à jour le dispositif vCloud Director avec des correctifs qui peuvent être associés à des améliorations de la fonctionnalité et de la sécurité du produit.

Pendant le correctif du déploiement du dispositif vCloud Director, le service vCloud Director cesse de fonctionner et une interruption de service peut être attendu. L'interruption de service dépend du temps nécessaire pour corriger chaque dispositif vCloud Director et pour exécuter le script de mise à niveau de la base de données vCloud Director. Le nombre de cellules de travail dans le groupe de serveurs vCloud Director diminue jusqu'à ce que vous arrêtiez le service vCloud Director sur le dernier dispositif vCloud Director. Un équilibrage de charge correctement configuré devant les points de terminaison HTTP vCloud Director doit arrêter le routage du trafic vers les cellules qui sont arrêtées.

Après l'application du correctif à chaque dispositif vCloud Director et la mise à niveau de la base de données, vous devez redémarrer les services vCloud Director dans le groupe de serveurs pour le remettre en ligne.

Procédure

1 Dans un navigateur Web, connectez-vous à l'interface utilisateur de gestion de dispositif d'une instance du dispositif vCloud Director pour identifier le dispositif principal, `https://appliance_ip_address:5480`.

   Notez le nom du dispositif principal. Vous devez utiliser le nom du dispositif principal lors de la mise à niveau de la base de données.

2 Téléchargez le module de mise à jour sur un dispositif.

   vCloud Director est distribué sous la forme d'un fichier exécutable avec un nom au format `VMware_vCloud_Director_`*v.v.v.v*`–`*nnnnnnnn*`_update.tar.gz`, où *v.v.v.v* représente la version du produit et *nnnnnnnn* le numéro de build. Par exemple, `VMware_vCloud_Director_9.7.0.4248–13560441_update.tar.gz`.

3 Créez le répertoire `local–update–package` dans lequel extraire le module de mise à jour.

```
mkdir /tmp/local–update–package
```

4 Extrayez le module de mise à jour dans le répertoire qui vient d'être créé.

```
tar –zxf VMware_vCloud_Director_v.v.v.v–nnnnnnnn_update.tar.gz \
               –C /tmp/local–update–package
```

5 Définissez le répertoire `local–update–package` comme référentiel de mise à jour.

```
vamicli    update ––repo file:///tmp/local–update–package
```

6 Contrôlez les mises à jour pour vérifier que vous avez correctement établi le référentiel.

```
vamicli update ––check
```

   La version du correctif s'affiche sous la forme d'une `Mise à jour disponible`.

7 Arrêtez vCloud Director en exécutant la commande suivante :

```
/opt/vmware/vcloud–director/bin/cell–management–tool –u <admin username> cell ––shutdown
```

8 Depuis le dispositif principal, sauvegardez la base de données intégrée du dispositif vCloud Director.

   Note Si vous effectuez une mise à niveau de vCloud Director 9.7.0.1 vers une version ultérieure, sauvegardez manuellement le fichier du magasin d'approbations se trouvant à l'emplacement `/opt/vmware/vcloud–director/etc/truststore`.

```
/opt/vmware/appliance/bin/create–db–backup
```

9 Appliquez le correctif disponible.

```
vamicli update --install latest
```

10 Répétez les étapes Étape 2 à Étape 7 et Étape 9 sur chaque dispositif.

11 Depuis n'importe quel dispositif, exécutez le script de mise à niveau de la base de données vCloud Director.

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

12 Démarrez les services vCloud Director sur chaque dispositif.

```
service vmware-vcd start
```

Migration vers le dispositif vCloud Director 12

À partir de la version 9.7, le dispositif vCloud Director inclut une base de données PostgreSQL intégrée avec la fonction HA (High Availability). Vous pouvez migrer votre environnement vCloud Director existant d'une version antérieure vers un environnement vCloud Director qui se compose de déploiements de dispositifs vCloud Director 9.7.

Vous pouvez migrer un environnement vCloud Director composé d'installations de vCloud Director sur les déploiements de dispositifs Linux ou vCloud Director. Vous pouvez migrer un environnement vCloud Director qui utilise une base de données Microsoft SQL externe ou une base de données PostgreSQL externe.

Si votre environnement vCloud Director utilise une base de données Oracle externe, avant la migration vers le dispositif vCloud Director, vous devez migrer la base de données vers PostgreSQL depuis la version vCloud Director 9.1. Pour plus d'informations sur le workflow de mise à niveau d'une installation de vCloud Director avec une base de données Oracle, reportez-vous à la section Chapitre 11 Mise à niveau de vCloud Director et application de correctifs au dispositif vCloud Director.

Ce chapitre contient les rubriques suivantes :

Migration de vCloud Director avec une base de données Microsoft SQL externe vers le dispositif vCloud Director

Si votre environnement vCloud Director actuel d'une version antérieure utilise une base de données Microsoft SQL externe, vous pouvez migrer vers un nouvel environnement vCloud Director qui se compose de déploiements de dispositifs vCloud Director 9.7. Votre environnement vCloud Director actuel peut se composer d'installations de vCloud Director sur des déploiements de dispositifs Linux ou vCloud Director. Le nouvel environnement vCloud Director peut utiliser les bases de données PostgreSQL intégrées du dispositif en mode haute disponibilité.

Le workflow de migration inclut quatre grandes étapes.

- Création du groupe de serveurs vCloud Director en déployant une ou plusieurs instances du dispositif vCloud Director 9.7.
- Mise à niveau de l'environnement vCloud Director existant.
- Migration de la base de données externe vers la base de données intégrée.
- Copie des données du service de transfert partagé et des données de certificats.

Procédure

1 Mettez à niveau l'environnement vCloud Director actuel vers la version 9.7, puis mettez à niveau le schéma de base de données source.

Reportez-vous à Chapitre 11 Mise à niveau de vCloud Director et application de correctifs au dispositif vCloud Director.

2 Vérifiez que le redémarrage de la source de migration vCloud Director a réussi.

3 Si vous souhaitez que le nouvel environnement vCloud Director utilise les adresses IP de l'environnement existant, modifiez les adresses IP des cellules existantes en adresses IP temporaires.

4 Si vous souhaitez que le nouvel environnement vCloud Director utilise le serveur NFS de l'environnement existant, créez et exportez un nouveau répertoire sur ce serveur NFS en tant que nouveau point de montage NFS partagé.

Vous ne pouvez pas réutiliser le point de montage existant, car les ID d'utilisateur et de groupe (UID/GID) des utilisateurs de l'ancien NFS peuvent ne pas correspondre aux ID d'utilisateur et de groupe du nouveau NFS.

5 Créez le nouveau groupe de serveurs en déployant une ou plusieurs instances du dispositif vCloud Director 9.7.

- Si vous souhaitez utiliser la fonction de haute disponibilité de la base de données, déployez une seule cellule principale et deux cellules en veille et, éventuellement, une ou plusieurs cellules d'application vCD.
- Si vous avez modifié les adresses IP des cellules existantes en adresses IP temporaires, vous pouvez utiliser les adresses IP d'origine pour les nouvelles cellules.
- Si vous avez exporté un nouveau chemin sur le serveur NFS existant, vous pouvez utiliser ce nouveau point de montage partagé pour le nouvel environnement.

Reportez-vous à Chapitre 6 Déploiement du dispositif vCloud Director.

6 Sur chaque cellule existante et chaque nouvelle cellule déployée, exécutez la commande pour arrêter le service vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

7 Choisissez l'une des cellules existantes qui servira de source de migration.

La source de migration doit avoir accès à l'adresse IP du réseau `eth1` de la nouvelle cellule principale déployée.

8 Dans la nouvelle cellule principale, activez l'accès à la base de données intégrée à partir de la source de migration.

Reportez-vous à Configurer l'accès externe à la base de données vCloud Director.

9 Sur la source de migration, exécutez l'outil de gestion des cellules pour migrer la base de données externe vers la base de données qui est intégrée dans la nouvelle cellule principale.

La base de données intégrée utilise l'adresse IP du réseau `eth1` du dispositif.

```
/opt/vmware/vcloud-director/bin/cell-management-tool dbmigrate -dbhost eth1_IP_new_primary \
-dbport 5432 -dbuser vcloud -dbname vcloud -dbpassword database_password_new_primary
```

Pour plus d'informations sur l'utilisation de l'outil de gestion des cellules, reportez-vous à la section *Guide de l'administrateur de vCloud Director*.

10 Sur chaque nouvelle cellule déployée, sauvegardez et remplacez les données de configuration, puis reconfigurez et démarrez le service vCloud Director.

a Sauvegardez les fichiers de propriétés et de certificats, puis copiez et remplacez ces fichiers à partir de la source de migration.

Les fichiers `global.properties`, `responses.properties`, `certificates` et `proxycertificates` se trouvent dans `/opt/vmware/vcloud-director/etc/`.

Important Si vous migrez vers vCloud Director version 9.7.0.1 ou version ultérieure, vous devez également sauvegarder, copier et remplacer le fichier `truststore` depuis la source de migration, ainsi que les autres fichiers.

b Sauvegardez le fichier keystore qui se trouve à l'emplacement `/opt/vmware/vcloud-director/certificates.ks`.

Ne copiez pas et ne remplacez pas le fichier keystore de la source de migration.

c Exécutez la commande pour reconfigurer le service vCloud Director.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Où :

- La valeur `--keystore-password` correspond au mot de passe **racine** initial de ce dispositif.

- La valeur `--database-password` correspond au mot de passe de la base de données que vous avez défini lors du déploiement du dispositif.
- La valeur `--database-host` correspond à l'adresse IP réseau `eth1` du dispositif principal.
- La valeur `--keystore` est le chemin d'accès au fichier `certificats.ks` que vous avez sauvegardé à l'étape 10.b.
- La valeur `--primary-ip` correspond à l'adresse IP du réseau `eth0` du dispositif.
- La valeur `--console-proxy-ip` correspond à l'adresse IP du réseau `eth0` du dispositif.

Pour obtenir des informations sur le dépannage, consultez La reconfiguration du service vCloud Director échoue lors de la migration ou de la restauration vers le dispositif vCloud Director.

d Exécutez la commande pour démarrer le service vCloud Director.

```
service vmware-vcd start
```

Vous pouvez surveiller la progression du démarrage de la cellule à l'adresse `/opt/vmware/vcloud-director/logs/cell.log`.

11 Une fois que toutes les cellules du nouveau groupe de serveurs ont terminé le processus de démarrage, vérifiez que la migration de votre environnement vCloud Director a réussi.

a Ouvrez la vCloud Director Web Console à l'aide de l'adresse IP du réseau `eth0` de n'importe quelle cellule du nouveau groupe de serveurs, `https://`*`et0_IP_new_cell`*`/cloud`.

b Connectez-vous à la vCloud Director Web Console avec vos informations d'identification d'**administrateur système** existantes.

c Confirmez que votre instance de vSphere et que vos ressources de cloud sont disponibles dans le nouvel environnement.

12 Après avoir procédé à la vérification de la migration de vCloud Director, utilisez la vCloud Director Web Console pour supprimer les cellules déconnectées appartenant à l'ancien environnement vCloud Director.

a Dans l'onglet **Gérer et surveiller**, cliquez sur **Cellules de cloud**.

b Cliquez avec le bouton droit sur le nom d'une cellule et sélectionnez **Supprimer**.

Vous pouvez déployer le dispositif vCloud Director pour ajouter des membres au groupe de serveurs de l'environnement migré.

Étape suivante

L'environnement du nouveau dispositif vCloud Director migré utilise des certificats auto-signés. Pour utiliser les certificats signés à partir de l'ancien environnement, procédez comme suit sur chaque cellule du nouvel environnement :

1 Copiez et remplacez le fichier keystore de l'ancienne cellule par `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.

2 Exécutez la commande de l'outil de gestion des cellules pour remplacer les certificats.

Assurez-vous que `vcloud.vcloud` est le propriétaire de ce fichier.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

3 Redémarrez le service vCloud Director.

```
service vmware-vcd restart
```

Si vous ajoutez de nouveaux membres à ce groupe de serveurs, les nouvelles cellules du dispositif sont déployées avec ces certificats signés correctement.

Migration de vCloud Director avec une base de données PostgreSQL externe vers le dispositif vCloud Director

Si votre environnement vCloud Director actuel d'une version antérieure utilise une base de données PostgreSQL externe, vous pouvez migrer vers un nouvel environnement vCloud Director qui se compose de déploiements de dispositifs vCloud Director 9.7 Votre environnement vCloud Director actuel peut se composer d'installations de vCloud Director sur des déploiements de dispositifs Linux ou vCloud Director. Le nouvel environnement vCloud Director peut utiliser les bases de données PostgreSQL intégrées du dispositif en mode haute disponibilité.

Le workflow de migration inclut quatre grandes étapes.

- Mise à niveau de l'environnement vCloud Director existant.
- Création du groupe de serveurs vCloud Director en déployant une ou plusieurs instances du dispositif vCloud Director 9.7.
- Migration de la base de données externe vers la base de données intégrée.
- Copie des données du service de transfert partagé et des données de certificats.

Procédure

1 Si votre base de données PostgreSQL externe actuelle est dans une version 9.x, mettez à niveau la base de données PostgreSQL externe vers la version 10.

2 Mettez à niveau votre environnement vCloud Director vers la version 9.7.

Reportez-vous à Chapitre 11 Mise à niveau de vCloud Director et application de correctifs au dispositif vCloud Director.

3 Vérifiez que le redémarrage de la source de migration vCloud Director a réussi.

4 Sur chaque cellule de l'environnement vCloud Director mis à niveau, exécutez la commande pour arrêter le service vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

5 Sur la base de données PostgreSQL externe, sauvegardez la base de données actuelle.

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

Si l'espace libre dans le dossier `/tmp` est insuffisant, utilisez un autre emplacement pour stocker le fichier de vidage.

6 Si le propriétaire de la base de données et le nom de la base de données sont différents de `vcloud`, notez le nom d'utilisateur et le nom de la base de données.

Vous devez créer cet utilisateur dans le nouvel environnement et renommer la base de données à l'étape 13.

7 Si vous souhaitez que le nouvel environnement vCloud Director utilise les adresses IP de l'environnement existant, vous devez copier les propriétés et les fichiers de certificats dans un emplacement de la base de données PostgreSQL externe et mettre les cellules hors tension.

a Copiez les fichiers `global.properties`, `responses.properties`, `certificates` et `proxycertificates` se trouvant à l'emplacement `/opt/vmware/vcloud-director/etc/` dans `/tmp` ou à un emplacement préféré dans la base de données PostgreSQL externe.

b Mettez les cellules hors tension dans l'environnement existant.

8 Si vous souhaitez que le nouvel environnement vCloud Director utilise le serveur NFS de l'environnement existant, créez et exportez un nouveau répertoire sur ce serveur NFS en tant que nouveau point de montage NFS partagé.

Vous ne pouvez pas réutiliser le point de montage existant, car les ID d'utilisateur et de groupe (UID/GID) des utilisateurs de l'ancien NFS peuvent ne pas correspondre aux ID d'utilisateur et de groupe du nouveau NFS.

9 Créez le nouveau groupe de serveurs en déployant une ou plusieurs instances du dispositif vCloud Director 9.7.

- Si vous souhaitez utiliser la fonction de haute disponibilité de la base de données, déployez une seule cellule principale et deux cellules en veille et, éventuellement, une ou plusieurs cellules d'application vCD.
- Si vous avez mis hors tension les cellules dans l'environnement existant, vous pouvez utiliser les adresses IP d'origine pour les nouvelles cellules.

- Si vous avez exporté un nouveau chemin sur le serveur NFS existant, vous pouvez utiliser ce nouveau point de montage partagé pour le nouvel environnement.

Reportez-vous à Chapitre 6 Déploiement du dispositif vCloud Director.

10 Sur chaque nouvelle cellule déployée, exécutez la commande pour arrêter le service vCloud Director.

```
service vmware-vcd stop
```

11 Copiez le fichier de vidage du dossier `/tmp` dans la base de données PostgreSQL externe vers le dossier `/tmp` sur la cellule principale du nouvel environnement.

Reportez-vous à l'étape 5.

12 Modifiez les autorisations sur le fichier de vidage.

```
chmod a+r /tmp/db_dump_name
```

13 Connectez-vous en tant que **racine** à la console de la nouvelle cellule principale déployée et transférez la base de données vCloud Director depuis la base de données externe vers la base de données intégrée.

a Basculez l'utilisateur sur `postgres`, connectez-vous au terminal de base de données `psql` et exécutez l'instruction pour supprimer la base de données `vcloud`.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

b Si le propriétaire de la base de données externe existante est différent de `vcloud`, créez un utilisateur sous le nom que vous avez noté à l'étape 6.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'CREATE USER
<db_owner_external_pg>;'
```

c Exécutez la commande `pg_restore`.

```
sudo -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/db_dump_name
```

d Si le nom de la base de données externe existante est différent de `vcloud`, renommez la base de données en `vcloud` en utilisant le nom que vous avez noté à l'étape 6.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE
<db_name_external_pg> RENAME TO vcloud;'
```

e Si le propriétaire de la base de données de l'environnement vCloud Director existant est différent de `vcloud`, renommez le propriétaire de la base de données en `vcloud` et réattribuez les tables à `vcloud`.

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/psql –c 'ALTER DATABASE vcloud OWNER TO
vcloud;'
```

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/psql –d vcloud –c 'REASSIGN OWNED BY
<db_owner_external_pg> TO vcloud;'
```

14 Sur chaque nouvelle cellule déployée, sauvegardez et remplacez les données de configuration, puis reconfigurez et démarrez le service vCloud Director.

a Sauvegardez les fichiers de propriétés et de certificats, puis remplacez ces fichiers par ceux de l'emplacement de la base de données PostgreSQL externe de la source de migration dans lequel vous avez copié les fichiers à l'étape 7a.

Les fichiers `global.properties`, `responses.properties`, `certificates` et `proxycertificates` se trouvent dans `/opt/vmware/vcloud–director/etc/`.

Important Si vous migrez vers vCloud Director version 9.7.0.1 ou version ultérieure, vous devez également sauvegarder, copier et remplacer le fichier `truststore` depuis la source de migration, ainsi que les autres fichiers.

b Sauvegardez le fichier keystore qui se trouve à l'emplacement `/opt/vmware/vcloud–director/certificates.ks`.

Ne copiez pas et ne remplacez pas le fichier keystore de la source de migration.

c Exécutez la commande pour reconfigurer le service vCloud Director.

```
/opt/vmware/vcloud–director/bin/configure ––unattended–installation ––database–type postgres
––database–user vcloud \
––database–password db_password_new_primary ––database–host eth1_ip_new_primary ––database–
port 5432 \
––database–name vcloud ––database–ssl true ––uuid ––keystore /opt/vmware/vcloud–director/
certificates.ks \
––keystore–password root_password_new_primary ––primary–ip appliance_eth0_ip \
––console–proxy–ip appliance_eth0_ip ––console–proxy–port–https 8443
```

Où :

- La valeur `––keystore–password` correspond au mot de passe **racine** initial de ce dispositif.
- La valeur `––database–password` correspond au mot de passe de la base de données que vous avez défini lors du déploiement du dispositif.
- La valeur `––database–host` correspond à l'adresse IP réseau `eth1` du dispositif principal.
- La valeur `––primary–ip` correspond à l'adresse IP du réseau `eth0` du dispositif.
- La valeur `––console–proxy–ip` correspond à l'adresse IP du réseau `eth0` du dispositif.

- La valeur `--console-proxy-port` correspond au port 8443 du proxy de la console du dispositif

Pour obtenir des informations sur le dépannage, consultez La reconfiguration du service vCloud Director échoue lors de la migration ou de la restauration vers le dispositif vCloud Director.

d Exécutez la commande pour démarrer le service vCloud Director.

```
service vmware-vcd start
```

Vous pouvez surveiller la progression du démarrage de la cellule à l'adresse `/opt/vmware/vcloud-director/logs/cell.log`.

15 Une fois que toutes les cellules du nouveau groupe de serveurs ont terminé le processus de démarrage, vérifiez que la migration de votre environnement vCloud Director a réussi.

a Ouvrez la vCloud Director Web Console à l'aide de l'adresse IP du réseau `eth0` de n'importe quelle cellule du nouveau groupe de serveurs, `https://`*`et0_IP_new_cell`*`/cloud`.

b Connectez-vous à la vCloud Director Web Console avec vos informations d'identification d'**administrateur système** existantes.

c Confirmez que votre instance de vSphere et que vos ressources de cloud sont disponibles dans le nouvel environnement.

16 Après avoir procédé à la vérification de la migration de vCloud Director, utilisez la vCloud Director Web Console pour supprimer les cellules déconnectées appartenant à l'ancien environnement vCloud Director.

a Dans l'onglet **Gérer et surveiller**, cliquez sur **Cellules de cloud**.

b Cliquez avec le bouton droit sur le nom d'une cellule et sélectionnez **Supprimer**.

Vous pouvez déployer le dispositif vCloud Director pour ajouter des membres au groupe de serveurs de l'environnement migré.

Étape suivante

L'environnement du nouveau dispositif vCloud Director migré utilise des certificats auto-signés. Pour utiliser les certificats signés à partir de l'ancien environnement, procédez comme suit sur chaque cellule du nouvel environnement :

1 Copiez et remplacez le fichier keystore de l'ancienne cellule par `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.

2 Exécutez la commande de l'outil de gestion des cellules pour remplacer les certificats.

Assurez-vous que `vcloud.vcloud` est le propriétaire de ce fichier.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

3 Redémarrez le service vCloud Director.

```
service vmware-vcd restart
```

Si vous ajoutez de nouveaux membres à ce groupe de serveurs, les nouvelles cellules du dispositif sont déployées avec ces certificats signés correctement.

Après la mise à niveau ou la migration de vCloud Director

13

Après avoir mis à niveau ou migré l'ensemble des serveurs vCloud Director et la base de données partagée, vous pouvez mettre à niveau les instances NSX Manager qui fournissent des services réseau à votre cloud. Vous pouvez ensuite mettre à niveau les hôtes ESXi et les instances vCenter Server qui sont enregistrés dans votre installation vCloud Director.

Important À partir de la version 9.7, vCloud Director prend uniquement en charge les passerelles Edge avancées. Vous devez convertir une passerelle Edge non avancée héritée en une passerelle avancée. Reportez-vous à https://kb.vmware.com/kb/66767.

Ce chapitre contient les rubriques suivantes :

Mettre à niveau chaque instance de NSX Manager associée à un système vCenter Server relié

Avant de mettre à niveau une instance de vCenter Server et des hôtes ESXi enregistrés dans vCloud Director, vous devez mettre à niveau chaque instance de NSX Manager associée à cette instance de vCenter Server.

La mise à niveau de NSX Manager interrompt l'accès aux fonctions administratives de NSX, mais elle n'interrompt pas les services réseau. Vous pouvez mettre à niveau NSX Manager avant ou après la mise à niveau de vCloud Director, que des cellules vCloud Director soient ou non en cours d'exécution.

Pour plus d'informations sur la mise à niveau de NSX, reportez-vous à la documentation NSX pour vSphere à l'adresse https://docs.vmware.com.

Procédure

1. Mettez à niveau l'instance de NSX Manager associée à chaque instance de vCenter Server enregistrée dans votre installation de vCloud Director.
2. Après la mise à niveau de toutes vos instances de NSX Manager, vous pouvez mettre à niveau vos systèmes vCenter Server et hôtes ESXi enregistrés.

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

Après la mise à niveau vCloud Director et NSX Manager, vous devez mettre à niveau les systèmes vCenter Server et les hôtes ESXi qui sont enregistrés sur vCloud Director. Après la mise à niveau de tous les systèmes vCenter Server attachés et les hôtes ESXi, vous pouvez mettre à niveau les dispositifs Edge NSX.

Conditions préalables

Assurez-vous que toutes les instances de NSX Manager associées aux systèmes vCenter Server reliés à votre Cloud ont bien été mises à niveau. Reportez-vous à Mettre à niveau chaque instance de NSX Manager associée à un système vCenter Server relié.

Procédure

1. Désactiver l'instance vCenter Server.
   a. Dans la Console Web vCloud Director, cliquez sur l'onglet **Gérer et surveiller** et, dans le volet de gauche, cliquez sur **vCenters**.
   b. Cliquez avec le bouton droit sur le nom de vCenter Server cible et cliquez sur **Désactiver**.
   c. Cliquez sur **Oui**.
2. Mettez à niveau le système vCenter Server.

   Pour plus d'informations, reportez-vous à *Mise à niveau de vCenter Server*.
3. Vérifiez l'ensemble des URL publiques et des chaînes de certificat de vCloud Director.
   a. Dans la Console Web vCloud Director, cliquez sur l'onglet **Administration** et, dans le volet de gauche, cliquez sur **Adresses publiques**.
   b. Vérifiez toutes les adresses publiques.
4. Actualisez l'enregistrement vCenter Server avec vCloud Director.
   a. Dans la Console Web vCloud Director, cliquez sur l'onglet **Gérer et surveiller** et, dans le volet de gauche, cliquez sur **vCenters**.
   b. Cliquez avec le bouton droit sur le nom de vCenter Server cible et cliquez sur **Actualiser**.
   c. Cliquez sur **Oui**.

5 Mettez à niveau chaque hôte ESXi que le système vCenter Server mis à niveau prend en charge.

Voir la rubrique *Mise à niveau de VMware ESXi*.

Important 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.

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

b Mettez à niveau l'hôte.

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

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

6 (Facultatif) Mettez à niveau les dispositifs NSX Edge gérés par l'instance de NSX Manager associée au système vCenter Server mis à niveau.

Les dispositifs NSX Edge mis à niveau apportent des améliorations en termes de performance et d'intégration. Vous pouvez utiliser NSX Manager ou vCloud Director pour mettre à niveau des dispositifs NSX Edge.

- Pour plus d'informations sur l'utilisation de NSX Manager pour mettre à niveau des dispositifs Edge NSX, reportez-vous à la documentation de NSX pour vSphere à l'adresse https://docs.vmware.com.
- Pour utiliser vCloud Director pour mettre à niveau des dispositifs NSX Edge, vous devez agir sur l'objet réseau vCloud Director que le dispositif Edge prend en charge :
  - Une mise à niveau appropriée d'une passerelle Edge s'exécute automatiquement lorsque vous utilisez la console Web de vCloud Director ou l'API vCloud pour réinitialiser un réseau protégé par la passerelle Edge.
  - Le redéploiement d'une passerelle Edge met à niveau le dispositif NSX Edge associé.
  - La réinitialisation d'un réseau vApp dans le contexte du vApp met à niveau le dispositif NSX Edge associé à ce réseau. Pour utiliser la console Web de vCloud Director pour réinitialiser un réseau vApp dans le contexte d'un vApp, accédez à l'onglet **Mise en réseau** du vApp, affichez ses détails de mise en réseau, cliquez avec le bouton droit sur le réseau vApp, puis sélectionnez **Réinitialiser le réseau**.

  Pour plus d'informations sur le redéploiement de passerelles Edge et la réinitialisation de réseaux vApp, reportez-vous à l'aide en ligne de la console Web de vCloud Director ou au *Guide de programmation de vCloud API*.

Étape suivante

Reprenez cette procédure pour les autres systèmes vCenter Server enregistrés dans votre installation vCloud Director.

Nouveaux droits dans cette version

vCloud Director 9.7 introduit de nouveaux droits, que vous pouvez ajouter à un rôle global existant que vous avez publié au niveau de vos locataires.

Droit	Description	Rôle par défaut
SDDC : Afficher le SDDC	Vous permet d'afficher tous les SDDC publiés dans votre organisation. L'**administrateur système** peut afficher tous les SDDC.	**Administrateur système** et **administrateur d'organisation**
SDDC : Gérer le SDDC	Vous permet d'ajouter, de supprimer et de modifier des SDDC.	**Administrateur système**
SDDC : Gérer le proxy SDDC	Vous permet d'ajouter, de supprimer, d'activer et de désactiver des proxys SDDC.	**Administrateur système**
Applications de service : Afficher les applications de service	Vous permet d'afficher la liste des applications de service enregistrées. Utilisé pour les comptes VMC.	**Administrateur système**
Applications de service : Enregistrer le SDDC VMC	Vous permet de créer, d'afficher, de modifier et de supprimer des applications de service. Utilisé pour les comptes VMC.	**Administrateur système**
Applications de service : Gérer les applications de service	Vous permet d'enregistrer des applications de service. Utilisé pour les comptes VMC.	**Administrateur système**
Cluster Edge : Afficher le cluster Edge	Vous permet d'afficher une liste de clusters Edge et de récupérer un cluster Edge spécifique.	**Administrateur système** et **administrateur d'organisation**
Cluster Edge : Gérer le cluster Edge	Vous permet de créer, de modifier et de supprimer des clusters Edge.	**Administrateur système** et **administrateur d'organisation**
vApp : Modifier la stratégie de calcul de la VM	Permet aux utilisateurs de modifier la stratégie de calcul d'une machine virtuelle.	**administrateur système**, **administrateur d'organisation**, **auteur de catalogue** et **auteur de vApp**
Passerelle : Importer la passerelle Edge	Vous permet d'importer un routeur de niveau 1 en tant que passerelle Edge.	**Administrateur système** et **administrateur d'organisation**

Pour plus d'informations sur la gestion des droits et des rôles, consultez le *Guide du portail d'administration des fournisseurs de services vCloud Director*.

Dépannage du dispositif vCloud Director 14

Si le déploiement du dispositif vCloud Director échoue ou si le dispositif ne fonctionne pas correctement, vous pouvez examiner les fichiers journaux du dispositif pour déterminer la cause du problème.

Le support technique de VMware demande régulièrement des informations de diagnostic lors du traitement de demandes de support. Vous pouvez utiliser le script `vmware-vcd-support` pour collecter des informations de journalisation de l'hôte et des journaux vCloud Director. Pour plus d'informations sur la collecte d'informations de diagnostic pour vCloud Director, reportez-vous à la section https://kb.vmware.com/s/article/1026312. Lors de l'exécution du script `vmware-vcd-support`, les journaux peuvent inclure des informations sur les cellules désaffectées ou remplacées ayant l'état FAIL. Reportez-vous à la section https://kb.vmware.com/s/article/71349.

Ce chapitre contient les rubriques suivantes :

- Examiner les fichiers journaux dans le dispositif vCloud Director
- La cellule vCloud Director ne parvient pas à démarrer après le déploiement du dispositif
- La reconfiguration du service vCloud Director échoue lors de la migration ou de la restauration vers le dispositif vCloud Director
- Utilisation de fichiers journaux pour dépanner les mises à jour et les correctifs de vCloud Director
- Échec de la vérification des mises à jour vCloud Director
- Échec de l'installation de la dernière mise à jour de vCloud Director

Examiner les fichiers journaux dans le dispositif vCloud Director

Après avoir déployé le dispositif vCloud Director, vous pouvez examiner les journaux de premier démarrage et de base de données pour y rechercher des erreurs et des avertissements.

Procédure

1. Connectez-vous directement ou via SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.
2. Accédez à `/opt/vmware/var/log`.

3 Examinez les fichiers journaux.

- Le fichier `firstboot` contient des informations de journalisation liées au premier démarrage du dispositif.
- Le répertoire `/opt/vmware/var/log/vcd/` contient des journaux liés à la configuration et la reconfiguration de la suite d'outils Replication Manager (repmgr) et à la synchronisation de dispositifs.
- Le répertoire `/opt/vmware/var/log/vcd/pg/` contient des journaux liés à la sauvegarde de la base de données de dispositif intégrée.
- Le fichier `/opt/vmware/etc/vami/ovfEnv.xml` contient les paramètres OVF du déploiement.

La cellule vCloud Director ne parvient pas à démarrer après le déploiement du dispositif

Vous avez correctement déployé le dispositif vCloud Director, mais les services vCloud Director peuvent ne pas démarrer.

Problème

Le service `vmware-vcd` est inactif après le déploiement du dispositif.

Cause

Si vous avez déployé une cellule principale, les services vCloud Director peuvent ne pas démarrer en raison d'un stockage de service de transfert partagé NFS pré-rempli. Avant que vous ne déployiez le dispositif principal, le stockage de service de transfert partagé ne doit pas contenir un fichier `responses.properties` ni un répertoire `appliance-nodes`.

Si vous avez déployé une cellule d'application en veille ou vCD, les services vCloud Director peuvent ne pas démarrer en raison d'un fichier `responses.properties` manquant dans le stockage de transfert partagé NFS. Avant que vous ne déployiez un dispositif d'applications en veille ou vCD, le stockage du service de transfert partagé doit contenir le fichier `responses.properties`.

Solution

1 Connectez-vous directement ou via SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.

2 Dans le fichier journal `/opt/vmware/var/log/vcd/setupvcd.log`, recherchez les messages d'erreur relatif au stockage NFS.

3 Préparez le stockage NFS au type de dispositif.

4 Redéployez la cellule.

La reconfiguration du service vCloud Director échoue lors de la migration ou de la restauration vers le dispositif vCloud Director

Lorsque vous migrez ou restaurez vers un dispositif vCloud Director, l'exécution de la commande `configure` peut échouer.

Problème

Pendant la procédure de migration ou de restauration de vCloud Director vers un nouvel environnement de dispositif vCloud Director, vous exécutez la commande `configure` pour reconfigurer le service vCloud Director dans chaque nouvelle cellule. La commande `configure` peut échouer avec le message d'erreur `sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed`.

Solution

1 Sur la cellule cible, exécutez la commande.

```
sed –i '/vcd_ova.crt/ s/$/ ––force /' /opt/vmware/appliance/bin/appliance–sync.sh
```

2 Patientez 1 minute, puis exécutez à nouveau la commande `configure`.

Utilisation de fichiers journaux pour dépanner les mises à jour et les correctifs de vCloud Director

Vous pouvez examiner les fichiers journaux pour rechercher des erreurs et des avertissements lorsque vous appliquez des correctifs au dispositif vCloud Director.

Problème

Si la commande `vamicli` renvoie une erreur, vous pouvez utiliser les fichiers journaux pour procéder au dépannage.

Solution

1 Connectez-vous directement ou via SSH à la console du dispositif vCloud Director en tant qu'utilisateur **racine**.

2 Accédez au fichier journal approprié.

- Si la commande `vamicli update ––check` échoue, accédez à `/opt/vmware/var/log/vami/vami.log`.
- Si la commande `vamicli update ––install latest` échoue, accédez à `/opt/vmware/var/log/vami/updatecli.log`.

3 Examinez le fichier journal.

Échec de la vérification des mises à jour vCloud Director

Lorsque vous vérifiez la présence de mises à jour au dispositif vCloud Director, l'exécution de la commande `vamicli update --check` peut échouer.

Problème

Pendant la procédure d'application d'un correctif au dispositif vCloud Director, exécutez la commande `vamicli update --check` pour vérifier les mises à jour disponibles. La commande `vamicli update --check` peut échouer avec le message `Échec : erreur lors du téléchargement du manifeste. Contactez votre fournisseur.`

Cause

Le chemin d'accès au répertoire du référentiel de mise à jour est incorrect.

Solution

1 Exécutez la commande `vamicli` avec le chemin d'accès approprié.

```
vamicli update --repo file:/root/local-update-repo
```

2 Exécutez à nouveau la commande pour vérifier les mises à jour.

```
vamicli update --check
```

Échec de l'installation de la dernière mise à jour de vCloud Director

Lorsque vous installez les dernières mises à jour au dispositif vCloud Director, l'exécution de la commande `vamicli update --install latest` peut échouer.

Problème

Pendant la procédure d'application d'un correctif au dispositif vCloud Director, vous exécutez la commande `vamicli update --install latest` pour appliquer le correctif disponible le plus récent. La commande `vamicli update --install latest` peut échouer avec le message `Échec : erreur lors de l'exécution de l'installation du module`

Cause

L'erreur se produit lorsque le serveur NFS est inaccessible.

Solution

1 Vérifiez que le serveur NFS monté à l'emplacement `/opt/vmware/vcloud-director/data/transfer` est accessible.

2 Exécutez de nouveau la commande pour appliquer le correctif disponible.

```
vamicli update --install latest
```

Désinstallation du logiciel vCloud Director

15

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 **racine**.
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 Linux `rpm`.

   ```
   rpm -e vmware-phonehome vmware-vcloud-director vmware-vcloud-director-rhel
   ```

   Si d'autres modules installés dépendent du module `vmware-vcloud-director`, le système vous invite à désinstaller ces modules avant de désinstaller vCloud Director.