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

9 avril 2020

VMware Cloud Director 10.1

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 VMware Cloud Director™

Le *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director* fournit des informations sur l'installation et la mise à niveau du logiciel VMware Cloud Director™, et sa 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 VMware Cloud Director* est destiné à toute personne qui souhaite installer ou mettre à niveau le logiciel VMware Cloud 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.

Architecture de VMware Cloud Director

1

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

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

Pour garantir la haute disponibilité de VMware Cloud Director, vous devez installer au moins deux cellules VMware Cloud 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 VMware Cloud Director à plusieurs systèmes VMware vCenter Server® et aux hôtes VMware ESXi™ qu'ils gèrent. Pour les services réseau, VMware Cloud Director peut utiliser NSX Data Center for vSphere associé avec vCenter Server ou vous pouvez enregistrer NSX-T Data Center avec VMware Cloud Director. NSX Data Center for vSphere et NSX-T Data Center mixtes sont également pris en charge.

Figure 1-1. Diagramme de l'architecture d'installation Linux de VMware Cloud Director

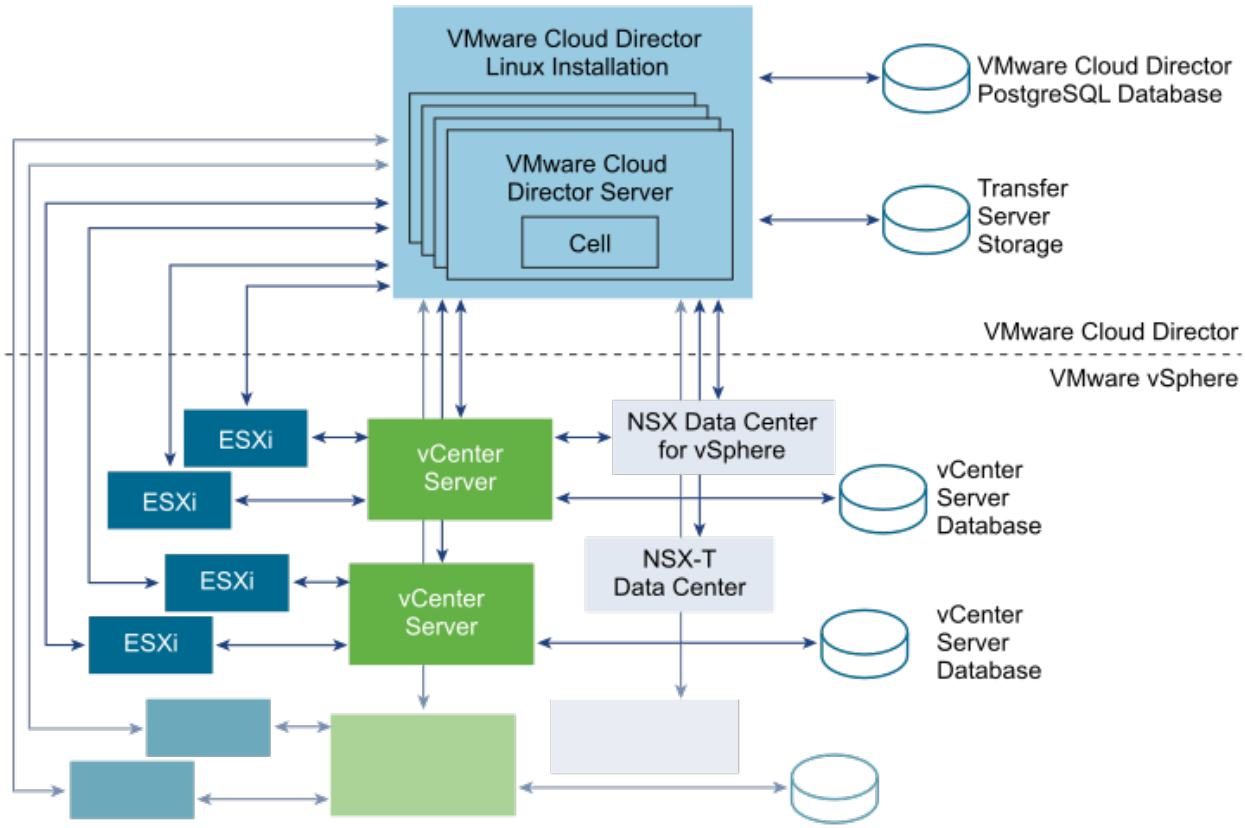
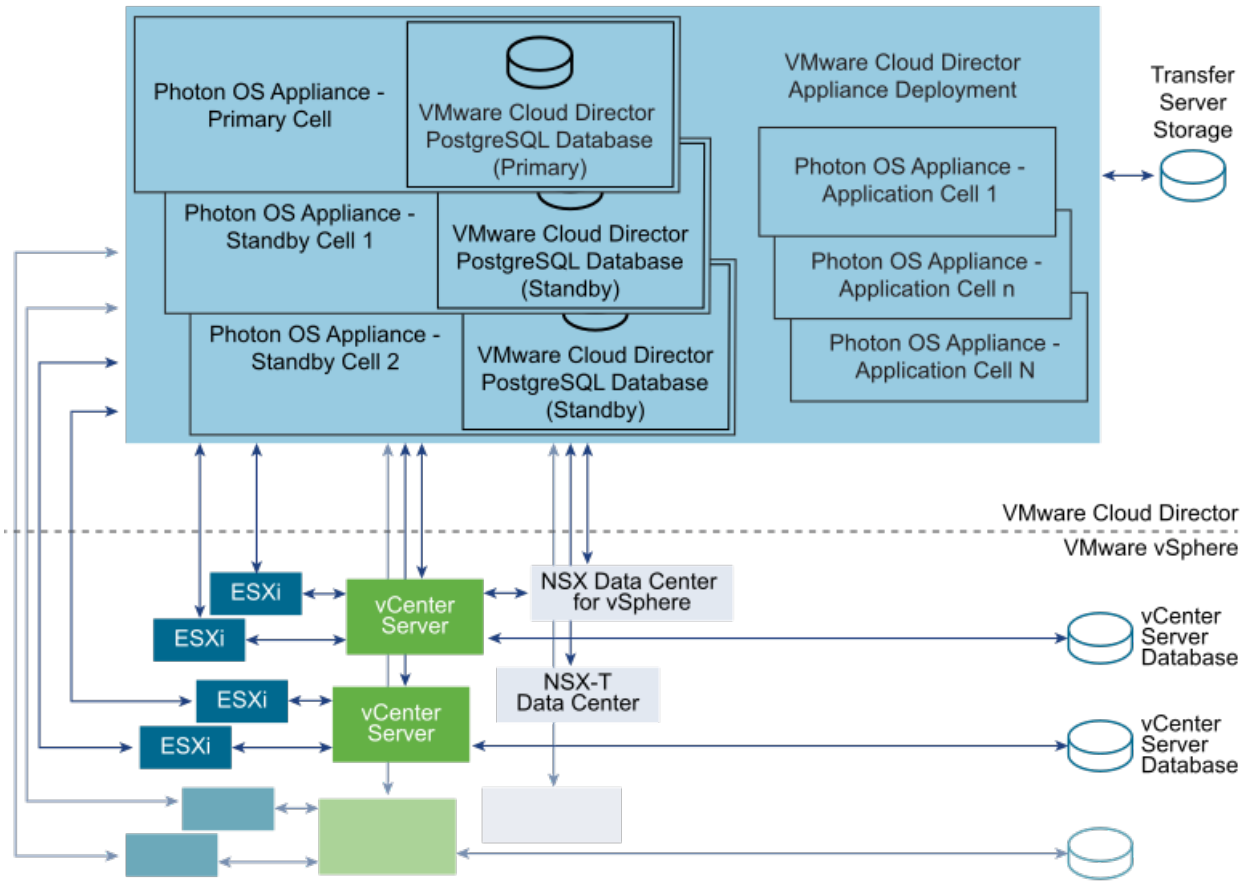


Figure 1-2. Diagramme de l'architecture du dispositif VMware Cloud Director



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

Un groupe de serveurs VMware Cloud 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 VMware Cloud 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 1-3. Dispositifs VMware Cloud Director comprenant un cluster haute disponibilité de base de données intégrée

Le processus d'installation et de configuration de VMware Cloud 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 ou de NSX-T Manager.

Pour plus d'informations sur l'ajout de ressources vSphere et de réseau, reportez-vous à la *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

Configuration matérielle et logicielle requise pour installer VMware Cloud Director

2

Chaque serveur d'un groupe de serveurs VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director doivent être disponibles pour tous les hôtes de tout cluster devant être utilisés par VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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*.

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

Reportez-vous aux *Notes de mise à jour de VMware Cloud Director* 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 VMware Cloud Director.

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

Pour plus d'informations sur la configuration requise de l'espace disque, de la mémoire et du CPU, reportez-vous à la section Directives de dimensionnement du dispositif VMware Cloud Director.

Stockage partagé

NFS ou autre volume de stockage partagé pour le service de transfert VMware Cloud 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 VMware Cloud Director
- Configuration requise pour la sécurité réseau

Configuration réseau requise pour VMware Cloud Director

Pour fonctionner de façon sécurisée et fiable, VMware Cloud 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 VMware Cloud Director, vérifiez que le réseau respecte ces conditions requises.

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

Adresses IP

Chaque serveur VMware Cloud Director doit prendre en charge deux points de terminaison SSL distincts. Un point de terminaison est destiné au service HTTPS. 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 VMware Cloud 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 depuis le Service Provider Admin Portal. Par exemple, pour le dispositif VMware Cloud 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 VMware Cloud 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.

Pour les déploiements de dispositifs VMware Cloud Director, le serveur NFS utilisé pour le partage de transfert doit utiliser un service d'heure réseau tel que NTP pour synchroniser son horloge sur celle des dispositifs VMware Cloud Director. Le décalage maximal autorisé entre les horloges des serveurs synchronisés ne doit pas dépasser 2 secondes.

Fuseaux horaire des serveurs

Tous les serveurs VMware Cloud Director, y compris le serveur NFS utilisé pour le partage de transfert et 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 qualifié complet ou du nom d'hôte non qualifié. Par exemple, pour un hôte *vcloud.example.com*, les deux commandes suivantes doivent aboutir sur un hôte VMware Cloud 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, VMware Cloud Director nécessite un environnement réseau sécurisé. Configurez et testez cet environnement réseau avant de commencer l'installation de VMware Cloud Director.

Connectez tous les serveurs VMware Cloud Director à un réseau sécurisé et surveillé.

Pour plus d'informations sur les ports réseau et protocoles utilisés par VMware Cloud Director, consultez VMware Ports and Protocols.

Les connexions réseau VMware Cloud Director ont plusieurs conditions requises supplémentaires :

- Ne connectez pas VMware Cloud Director directement à l'Internet public. Protégez toujours les connexions réseau de VMware Cloud 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.

  Pour plus d'informations sur les ports qui doivent autoriser les paquets entrants en provenance des hôtes VMware Cloud Director, reportez-vous à VMware Ports and Protocols.
- Ne connectez pas les ports utilisés pour les connexions sortantes au réseau public.

  Pour plus d'informations sur les ports qui doivent autoriser les paquets sortants en provenance des hôtes VMware Cloud Director, reportez-vous à VMware Ports and Protocols.
- À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et vérifier l'identité du serveur dans le cadre d'une connexion à SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste d'exclusion d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste d'exclusion après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste d'exclusion pour les tests de connexion.
- Acheminez le trafic entre les serveurs VMware Cloud Director et les serveurs suivants sur un réseau privé dédié.
  - Serveur de base de données VMware Cloud Director
  - RabbitMQ
  - Cassandra
- Si possible, acheminez le trafic entre les serveurs VMware Cloud 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 VMware Cloud Director sont disponibles dans l'article 2086127 de la base de connaissances VMware.

Déploiement, mise à niveau et administration du dispositif VMware Cloud Director

3

À partir de la version 9.7, le dispositif VMware Cloud Director inclut une base de données PostgreSQL intégrée avec la fonction HA (High Availability). Lorsque vous déployez, mettez à niveau ou migrez le dispositif VMware Cloud Director, vous pouvez effectuer des opérations d'administration, de surveillance, de correction ou de dépannage.

Ce chapitre contient les rubriques suivantes :

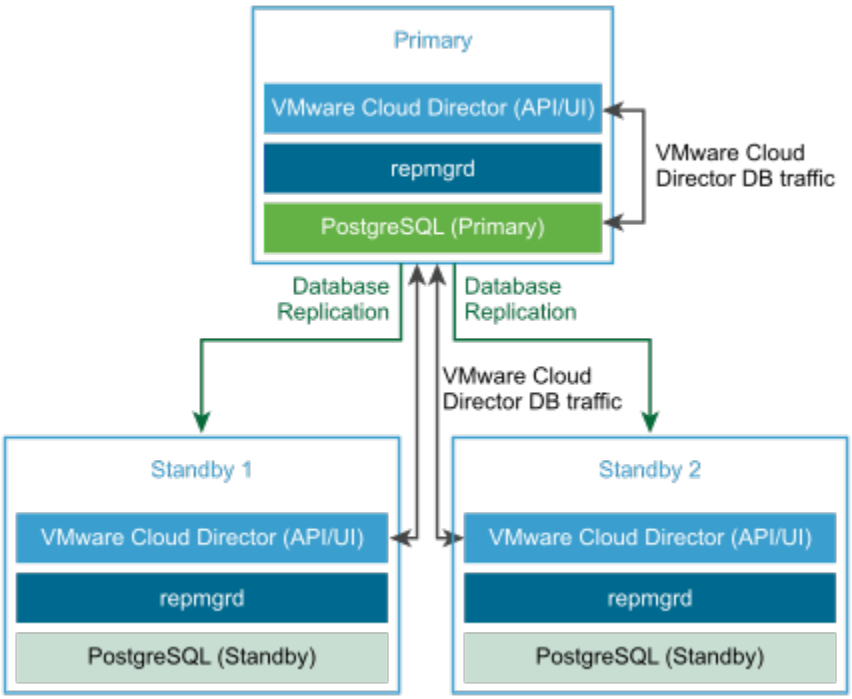
Déploiements du dispositif et configuration de la haute disponibilité de la base de données

Le dispositif VMware Cloud 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 VMware Cloud Director.

Vous pouvez déployer le dispositif VMware Cloud Director en tant que cellule principale, cellule en veille ou cellule d'application VMware Cloud Director. Reportez-vous à la section Déployer une instance de VMware Cloud Director Appliance à l'aide de vSphere Client, Déploiement du dispositif VMware Cloud Director avec VMware OVF Tool ou Déployer le dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. Vous pouvez dimensionner horizontalement votre groupe de serveurs en déployant également des cellules d'application. Reportez-vous à la figure Figure 3-1. Cluster HA de base de données du dispositif VMware Cloud Director.

Figure 3-1. Cluster HA de base de données du dispositif VMware Cloud Director



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

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

1 Déployez le dispositif VMware Cloud Director en tant que cellule principale.

   La cellule principale est le premier membre du groupe de serveurs VMware Cloud Director. La base de données intégrée est configurée en tant que base de données VMware Cloud 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 VMware Cloud Director, connectez-vous avec les informations d'identification d'**administrateur système** au VMware Cloud Director Service Provider Admin Portal à l'adresse `https://`*`primary_eth0_ip_address`*`/provider`.

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 VMware Cloud Director en tant que cellules en veille.

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

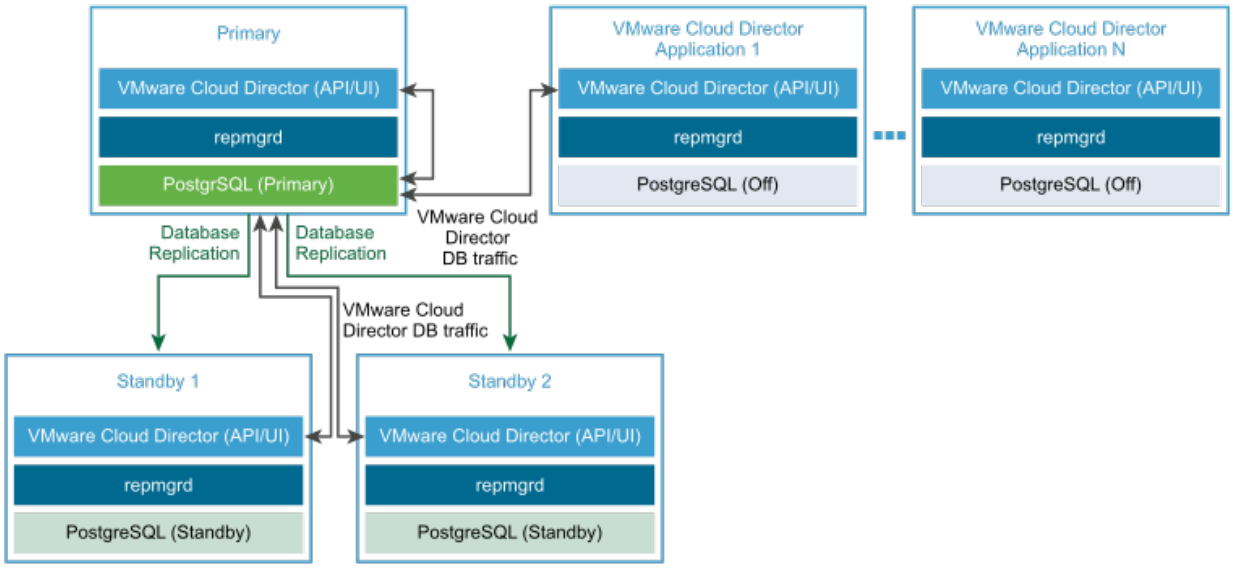
Note Après le déploiement initial du dispositif en veille, le gestionnaire de réplication commence à synchroniser sa base de données avec la base de données du dispositif principal. Pendant ce temps, la base de données VMware Cloud Director et, par conséquent, l'interface utilisateur VMware Cloud Director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

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

Reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

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

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



Note Si votre cluster est configuré pour le basculement automatique, après avoir déployé une ou plusieurs cellules supplémentaires, vous devez utiliser Appliance API pour réinitialiser le mode de basculement sur `Automatic`. Reportez-vous à l'API du dispositif VMware Cloud Director. Le mode de basculement par défaut des nouvelles cellules est `Manual`. Si le mode de basculement est incohérent entre les nœuds du cluster, le mode de basculement du cluster est `Indeterminate`. Le mode `Indeterminate` peut créer des états de cluster incohérents entre les nœuds et les nœuds qui suivent une ancienne cellule principale. Pour afficher le mode de basculement du cluster, reportez-vous à Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

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

Note Vous pouvez déployer un cluster VMware Cloud Director avec une cellule principale et aucune cellule en veille ou cellule d'application. VMware ne prend pas en charge les déploiements à cellule unique dans un environnement de production, car il s'agit d'une source de panne unique du point de vue de la base de données. Les déploiements à cellule unique ne reçoivent pas de prise en charge pour les problèmes liés aux performances ou à la stabilité.

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

1 Déployez le dispositif VMware Cloud Director en tant que cellule principale.

   La cellule principale est le premier membre du groupe de serveurs VMware Cloud Director. La base de données intégrée est configurée en tant que base de données VMware Cloud 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.

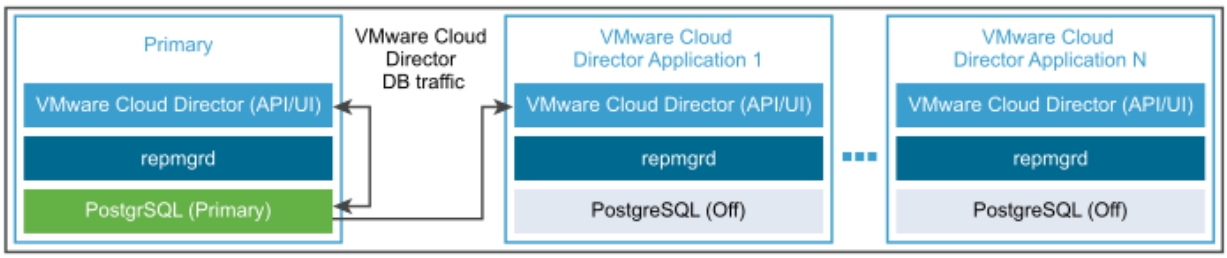
   a Pour vérifier la santé du service VMware Cloud Director, connectez-vous avec les informations d'identification d'**administrateur système** au VMware Cloud Director Service Provider Admin Portal à l'adresse `https://primary_eth0_ip_address/provider`.

   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 VMware Cloud Director en tant que cellules d'application VMware Cloud Director.

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



Basculement automatique du dispositif VMware Cloud Director

À partir de VMware Cloud Director 10.1, si le service de base de données principale échoue, vous pouvez activer VMware Cloud Director pour effectuer un basculement automatique vers un nouveau service de base de données principale.

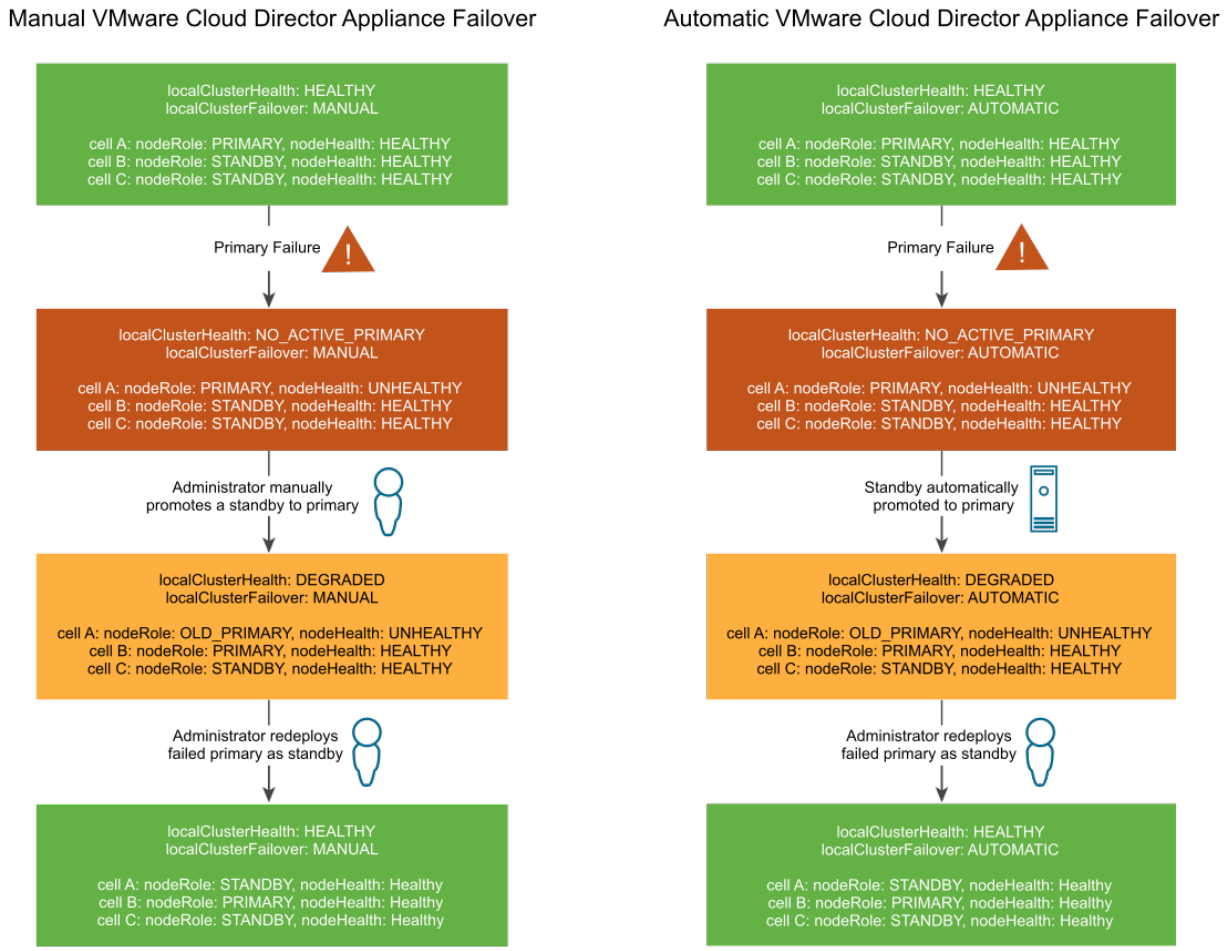
Le basculement automatique élimine la nécessité pour un administrateur de lancer l'action de basculement si le service de base de données principale ne parvient pas à exécuter ses fonctions pour une raison quelconque. Par défaut, le mode de basculement est défini sur manuel. Vous pouvez définir le mode de basculement sur automatique ou sur manuel à l'aide de l'API du dispositif VMware Cloud Director. Reportez-vous à la section *Référence de schéma de l'API du dispositif VMware Cloud Director*.

Note Si votre cluster est configuré pour le basculement automatique, après avoir déployé une ou plusieurs cellules supplémentaires, vous devez utiliser Appliance API pour réinitialiser le mode de basculement sur `Automatic`. Reportez-vous à l'API du dispositif VMware Cloud Director. Le mode de basculement par défaut des nouvelles cellules est `Manual`. Si le mode de basculement est incohérent entre les nœuds du cluster, le mode de basculement du cluster est `Indeterminate`. Le mode `Indeterminate` peut créer des états de cluster incohérents entre les nœuds et les nœuds qui suivent une ancienne cellule principale. Pour afficher le mode de basculement du cluster, reportez-vous à Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

Si votre environnement comporte au moins deux cellules en veille actives, en cas d'échec d'une base de données principale, un basculement de base de données est automatiquement initié. Après le basculement, vous devez disposer d'au moins une cellule en veille active pour que la nouvelle base de données principale puisse être mise à jour. Dans des circonstances normales, le déploiement de votre dispositif VMware Cloud Director doit disposer d'au moins deux cellules en veille actives à tout moment. S'il n'y a qu'une seule cellule en veille active pendant une courte période, par exemple en raison de l'échec de la cellule principale et de la promotion de l'une des cellules en veille, l'ancienne cellule principale ayant échoué doit être remplacée par une nouvelle cellule en veille dès que possible.

Lorsqu'il existe une cellule principale active et au moins deux cellules en veille actives, le cluster est considéré comme étant dans un état `Healthy`. S'il existe une cellule principale active et une seule en veille active, le cluster est dans un état `Degraded`. En cas d'échec d'une autre base de données alors que le cluster est dans un état `Degraded`, la cellule principale ne peut pas être mise à jour tant qu'une autre cellule en veille n'est pas en ligne. Lorsque la base de données principale ne peut pas être mise à jour, VMware Cloud Director n'est pas disponible, car les cellules VMware Cloud Director ne parviennent pas à mettre à jour la base de données tant qu'il n'y a pas au moins une cellule en veille active pour traiter une réplication en continu depuis la base de données principale. Le concept d'un cluster `Healthy` et `Degraded` est le même que vous activiez le basculement de façon manuelle ou automatique.

Figure 3-2. Basculement manuel et automatique du dispositif VMware Cloud Director



Clôture automatique d'une cellule principale ayant échoué

Si une nouvelle cellule principale est promue après une panne de cellule principale, VMware Cloud Director isole automatiquement l'ancienne cellule principale pour l'empêcher de redémarrer.

En cas de basculement, si une base de données principale ayant échoué redémarre après la promotion d'une nouvelle cellule principale, VMware Cloud Director isole automatiquement l'ancienne cellule principale. Cette automatisation permet d'éviter le syndrome de Split-Brain dans lequel deux bases de données actives peuvent diverger l'une de l'autre. L'automatisation de la clôture s'arrête et désactive le service vpostgres sur l'ancien nœud principal. Ensuite, vous pouvez redéployer la cellule principale ayant échoué en tant que cellule en veille pour restaurer la santé du cluster sur `Healthy`.

Pour plus d'informations sur l'affichage de l'état de santé du cluster et le mode de basculement, reportez-vous à Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

Préparation du déploiement du dispositif VMware Cloud Director

Avant de déployer le dispositif VMware Cloud Director, vous devez préparer votre environnement.

Préparation du stockage du serveur de transfert pour le dispositif VMware Cloud Director

Vous devez rendre un système de stockage NFS ou un autre volume de stockage partagé accessible à tous les serveurs d'un groupe de serveurs VMware Cloud Director. Cela permet de gérer les clusters de dispositifs et de fournir un stockage temporaire pour les chargements, les téléchargements et les éléments de catalogue qui sont publiés ou abonnés en externe.

Important Le dispositif VMware Cloud 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. Le dispositif VMware Cloud Director configure également la plupart des détails du serveur NFS pendant le déploiement, y compris les autorisations et la propriété des répertoires. Vous devez vérifier qu'il existe un point de montage NFS valide et accessible aux instances du dispositif VMware Cloud Director.

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.
- Les sauvegardes de la base de données de dispositif peuvent consommer plus d'espace que les chargements et les téléchargements.
- Le collecteur de bundle de journaux multi-cellules occupe cet espace.

- Les données des nœuds du dispositif et le fichier `response.properties` occupent cet espace.

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

Note L'interruption de NFS peut entraîner un dysfonctionnement des fonctionnalités du cluster du dispositif VMware Cloud Director. L'interface utilisateur HTML5 ne répond pas lorsque le NFS est arrêté ou est inaccessible. Les autres fonctionnalités susceptibles d'être affectées sont la clôture d'une cellule principale ayant échoué, le basculement, la promotion d'une cellule en veille, etc.

Note Lorsque vous utilisez des distributions Linux basées sur Ubuntu ou Debian pour NFS, la création de sauvegardes de base de données échoue.

Exigences pour la configuration du serveur NFS

Il existe des exigences spécifiques pour la configuration du serveur NFS, afin que VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 la ligne suivante 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 VMware Cloud 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.

Installer et configurer NSX Data Center for vSphere pour VMware Cloud Director

Si vous planifiez l'installation de VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Important Cette procédure ne s'applique que dans le cas d'une nouvelle installation de VMware Cloud Director. Si vous mettez à niveau une installation de VMware Cloud Director existante, consultez Mise à niveau de VMware Cloud Director sous Linux.

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 VMware Cloud Director dans votre installation de VMware Cloud Director.

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

   VMware Cloud 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 VMware Cloud Director

Si vous planifiez l'installation de VMware Cloud Director pour utiliser les ressources réseau de NSX-T Data Center, vous devez installer et configurer NSX-T Data Center.

Important Pour configurer les objets et les outils NSX-T Data Center, utilisez l'interface utilisateur de stratégie simplifiée et les API de stratégie qui correspondent à l'interface utilisateur simplifiée. Pour plus d'informations, consultez la présentation de NSX-T Manager à la section *Guide d'administration de NSX-T Data Center* .

Pour obtenir les informations les plus récentes sur la compatibilité entre VMware Cloud Director et d'autres produits VMware, reportez-vous aux Matrices d'interopérabilité des produits VMware.

Pour plus d'informations sur les conditions requises en matière de réseau, consultez Configuration réseau requise pour VMware Cloud Director.

Cette procédure ne s'applique que dans le cas d'une nouvelle installation de VMware Cloud Director. Si vous mettez à niveau une installation de VMware Cloud Director existante, consultez Mise à niveau de VMware Cloud Director sous Linux.

Conditions préalables

Familiarisez-vous avec NSX-T Data Center.

Procédure

1 Déployez et configurez les dispositifs virtuels NSX-T Manager.

   Pour plus d'informations sur le déploiement de NSX-T Manager, consultez la section *Guide d'installation de NSX-T Data Center* .

2 Créez des zones de transport en fonction de vos exigences de mise en réseau.

   Pour plus d'informations sur la création de zones de transport, consultez la section *Guide d'installation de NSX-T Data Center* .

   Note

3 Déployez et configurez des nœuds Edge et un cluster Edge.

   Pour plus d'informations sur la création de NSX Edge, consultez la section *Guide d'installation de NSX-T Data Center* .

4 Configurez les nœuds de transport de l'hôte ESXi.

   Pour plus d'informations sur la configuration du nœud de transport d'un hôte géré, consultez la section *Guide d'installation de NSX-T Data Center* .

5 Créez une passerelle de niveau 0.

   Pour plus d'informations sur la création de passerelles de niveau 0, consultez la section *Guide d'administration de NSX-T Data Center* .

Étape suivante

Après l'installation de VMware Cloud Director, vous pouvez :

1 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 la section *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

2 Créer un pool de réseaux reposant sur une zone de transport NSX-T Data Center.

   Pour plus d'informations sur la création d'un pool de réseaux dépendant d'une zone de transport NSX-T Data Center, reportez-vous à la section *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

3 Importer la passerelle de niveau 0 en tant que réseau externe.

   Pour plus d'informations sur l'ajout d'un réseau externe dépendant d'un routeur logique de niveau 0 NSX-T Data Center, reportez-vous à la section *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

Déploiement et configuration initiale du dispositif VMware Cloud Director

Vous pouvez créer un groupe de serveurs VMware Cloud Director en déployant une ou plusieurs instances du dispositif VMware Cloud Director. Vous déployez une instance du dispositif VMware Cloud Director à l'aide de vSphere Client ou de VMware OVF Tool.

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

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

Le dispositif est distribué avec un nom sous la forme `VMware Cloud 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 Cloud Director-9.7.0.0-9229800_OVA10.ova`.

Le module du dispositif VMware Cloud Director comporte les logiciels suivants :

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

Les tailles de petit dispositif principal et de petit dispositif en veille VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director comme cellule principale et deux instances comme cellules en veille. Vous pouvez déployer des instances supplémentaires du dispositif VMware Cloud Director dans le groupe de serveurs comme cellules d'application vCD, qui exécutent uniquement le groupe de services VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Note Le dispositif VMware Cloud 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 VMware Cloud 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.

Note Les réseaux `eth0` et `eth1` doivent être placés sur des sous-réseaux distincts.

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

Après la création du dispositif VMware Cloud Director, vous pouvez utiliser les fonctionnalités de mise en réseau vSphere pour ajouter une nouvelle carte réseau (NIC). Consultez les informations de Ajouter un adaptateur réseau à une machine virtuelle dans le guide *Administration d'une machine virtuelle vSphere*.

Le dispositif VMware Cloud 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`.

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Directives de dimensionnement du dispositif VMware Cloud Director

Selon vos besoins, vous pouvez définir différentes configurations pour le groupe de serveurs basé sur un dispositif VMware Cloud Director et différentes tailles pour les instances de dispositif virtuel VMware Cloud Director.

Présentation

Pour s'assurer que le cluster peut prendre en charge un basculement automatisé en cas d'échec d'une cellule principale, le déploiement minimal de VMware Cloud Director doit être composé d'une cellule principale et de deux cellules en veille. L'environnement reste disponible en cas d'échec lorsque l'une des cellules se déconnecte pour une raison quelconque. Si un échec de la cellule en veille se produit, le cluster fonctionne dans un état entièrement fonctionnel avec une certaine dégradation des performances jusqu'à ce que vous redéployiez la cellule en échec. Reportez-vous à Déploiements du dispositif et configuration de la haute disponibilité de la base de données.

Le dispositif VMware Cloud Director a quatre tailles que vous pouvez sélectionner lors du déploiement : Petit, Moyen, Grand et Très grand (VVD). La taille de dispositif Petit convient à une évaluation de laboratoire et ce document ne fournit pas de conseils sur la configuration de cette taille. Le tableau des options de taille fournit des spécifications sur les options restantes et les cas d'utilisation les plus adaptés à un environnement de production. La configuration Très grand correspond au profil d'échelle VMware Validated Designs (VVD) for Cloud Providers.

Pour créer des tailles personnalisées plus grandes, les **administrateurs système** peuvent ajuster la taille des cellules déployées.

La configuration la plus petite recommandée pour les déploiements de production est un déploiement à trois nœuds des dispositifs virtuels de taille moyenne.

Note Vous pouvez déployer un cluster VMware Cloud Director avec une cellule principale et aucune cellule en veille ou cellule d'application. VMware ne prend pas en charge les déploiements à cellule unique dans un environnement de production, car il s'agit d'une source de panne unique du point de vue de la base de données. Les déploiements à cellule unique ne reçoivent pas de prise en charge pour les problèmes liés aux performances ou à la stabilité.

Options de dimensionnement du dispositif VMware Cloud Director

Vous pouvez utiliser le guide de décision suivant pour estimer la taille du dispositif pour votre environnement.

	Medium	Large	Très grand (VVD)
Cas d'utilisation recommandés	Environnements de laboratoire ou de petite production	Environnement de production	Production avec intégrations d'API et surveillance
Déploiement vRealize Operations Management Pack dans l'environnement VMware Cloud Director	Non	Non	Oui
Activation des mesures de machine virtuelle Cassandra dans VMware Cloud Director	Non	Non	Oui

	Medium	Large	Très grand (VVD)
Nombre approximatif d'utilisateurs ou de clients simultanés accédant à l'API sur une période de pointe de 30 minutes.	< 50	< 100	< 100
Machines virtuelles gérées	5 000	5 000	15 000

Définitions de configuration

Note Les dispositifs `primary-large` et `standby-large` pour VMware Cloud Director 9.7 et versions ultérieures ne disposent pas par défaut des 16 vCPU requis pour une configuration de cluster HA de grande taille. Si vous souhaitez disposer d'une configuration de dispositif VMware Cloud Director de grande taille, après le déploiement, vous devez remplacer manuellement le nombre de vCPU de cellule principale et en veille par 16.

	Medium	Large	Très grand (VVD)
Configuration du cluster HA	1 cellule principale + 2 cellules en veille	1 cellule principale + 2 cellules en veille + 1 cellule d'application	1 cellule principale + 2 cellules d'application en veille + 2 cellules d'application
vCPU de cellule principale ou en veille	8	16	24
vCPU de cellule d'application	S/O	8	8
RAM de cellule principale ou en veille	16 Go	24 Go	32 Go
RAM de cellule d'application	S/O	8	8
Rapport vCPU/cœur physique	1:1	1:1	1:1
Personnalisation PostgreSQL sur les cellules principale et en veille	shared_buffers = '3GB'; effective_cache_size = '9GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '8';	shared_buffers = '5GB'; effective_cache_size = '15GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '16';	shared_buffers = '7GB'; effective_cache_size = '21GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '24';

Procédure de détection de système sous-dimensionné

Dans une cellule VMware Cloud Director, l'utilisation du CPU ou de la mémoire augmente et atteint un niveau élevé, c'est-à-dire un niveau proche de la capacité. La cellule VMware Cloud Director peut également perdre la connexion à la base de données.

Procédure de détection d'un nombre de cellules insuffisant pour votre système

Dans les fichiers `vcloud-container-debug.log` et `cell-runtime.log` de l'une des cellules VMware Cloud Director, vous voyez des entrées semblables à `org.apache.tomcat.jdbc.pool.PoolExhaustedException: [pool-jetty-XXXXX] Timeout: Pool empty. Unable to fetch a connection in 20 seconds, none available`. La cellule VMware Cloud Director peut également perdre la connexion à la base de données.

Note En fonction de la configuration de la connexion à la base de données par défaut, toutes les configurations sont limitées à un maximum de 6 cellules de type principal, en veille et d'application.

Procédure de personnalisation de la taille du dispositif

Pour personnaliser la taille du dispositif VMware Cloud Director sur l'une des configurations personnalisées, après l'exécution du système de déploiement du dispositif VMware Cloud Director, vous devez suivre cette procédure sur toutes les cellules.

1. Vérifiez que vous disposez du nombre nécessaire de cellules pour la configuration sélectionnée.
2. Ajustez la mémoire et le vCPU de toutes les cellules pour qu'ils correspondent à l'une des configurations prises en charge de votre choix.

   Important La quantité de RAM et de vCPU doit être la même pour toutes les cellules principales et en veille.

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

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

5 Mettez à jour le fichier de configuration `postgresql.auto.conf` en exécutant les commandes suivantes.

Type de configuration	Description

Medium	`psql -c "ALTER SYSTEM set shared_buffers = '3GB';"`
	`psql -c "ALTER SYSTEM set effective_cache_size = '9GB';"`
	`psql -c "ALTER SYSTEM set work_mem = '8MB';"`
	`psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"`
	`psql -c "ALTER SYSTEM set max_worker_processes= '8';"`

Large	`psql -c "ALTER SYSTEM set shared_buffers = '5GB';"`
	`psql -c "ALTER SYSTEM set effective_cache_size = '15GB';"`
	`psql -c "ALTER SYSTEM set work_mem = '8MB';"`
	`psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"`
	`psql -c "ALTER SYSTEM set max_worker_processes= '16';"`

Très grand	`psql -c "ALTER SYSTEM set shared_buffers = '7GB';"`
	`psql -c "ALTER SYSTEM set effective_cache_size = '21GB';"`
	`psql -c "ALTER SYSTEM set work_mem = '8MB';"`
	`psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"`
	`psql -c "ALTER SYSTEM set max_worker_processes= '24';"`

6 Revenez à l'utilisateur **racine** en exécutant la commande `exit`.

7 Redémarrez le processus vpostgres.

```
systemctl restart vpostgres
```

8 Remplacez l'utilisateur par **postgres** à nouveau.

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

9 Pour chaque nœud en veille, copiez le fichier `postgresql.auto.conf` sur le nœud et redémarrez le processus vpostgres.

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

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

b Redémarrez le processus vpostgres.

```
systemctl restart vpostgres
```

Pour personnaliser la taille du dispositif VMware Cloud Director sur une configuration personnalisée, après l'exécution du système de déploiement du dispositif VMware Cloud Director, vous devez suivre cette procédure sur toutes les cellules.

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

2 Pour afficher et noter les informations de vCPU, exécutez la commande suivante.

```
grep -c processor /proc/cpuinfo
```

3 Pour afficher et noter les informations de RAM, exécutez la commande suivante.

La RAM signalée ci-dessous est en Ko et vous devez la convertir en Go en divisant par 1 024 000.

```
cat /proc/meminfo | grep MemTotal | cut -dk -f1 | awk '{print int($2/1024000)}'
```

4 Calculez la valeur de `shared_buffers` comme un quart de la RAM totale moins 4 Go.

`shared_buffers` = 0,25 * (*total RAM* - 4 Go)

5 Calculez la valeur de `effective_cache_size` comme trois quarts de la RAM totale moins 4 Go.

`effective_cache_size` = 0,75 * (*total RAM* - 4 Go)

6 Calculez la valeur de `max_worker_processes`, qui est le nombre de vCPU.

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

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

8 Mettez à jour le fichier de configuration `postgresql.auto.conf` en exécutant les commandes suivantes et en remplaçant les valeurs calculées.

```
psql -c "ALTER SYSTEM set shared_buffers = 'shared_buffers value';"
psql -c "ALTER SYSTEM set effective_cache_size =  'effective_cache_size value';"
psql -c "ALTER SYSTEM set work_mem = '8MB';"
psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"
psql -c "ALTER SYSTEM set max_worker_processes= 'max_worker_processes value';"
```

9 Revenez à l'utilisateur **racine** en exécutant la commande `exit`.

10 Redémarrez le processus vpostgres.

```
systemctl restart vpostgres
```

11 Remplacez l'utilisateur par **postgres** à nouveau.

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

12 Pour chaque nœud en veille, copiez le fichier `postgresql.auto.conf` sur le nœud et redémarrez le processus vpostgres.

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

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

b Redémarrez le processus vpostgres.

```
systemctl restart vpostgres
```

Conditions préalables au déploiement du dispositif VMware Cloud Director

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

- Vérifiez que vous avez accès au fichier `.ova` de VMware Cloud 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 pour VMware Cloud Director sur Linux.

  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 VMware Cloud Director

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

Déployer une instance de VMware Cloud Director Appliance à l'aide de vSphere Client

Vous pouvez déployer le dispositif VMware Cloud Director sous la forme d'un modèle OVF en utilisant vSphere Client (HTML5).

Vous devez déployer le premier membre d'un groupe de serveurs VMware Cloud Director en tant que cellule principale. Vous pouvez déployer un membre suivant d'un groupe de serveurs VMware Cloud 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 VMware Cloud Director sur Linux et les déploiements de dispositifs VMware Cloud Director dans un groupe de serveurs unique ne sont pas pris en charge.

Lors de l'ajout de dispositifs supplémentaires ou de remplacement à un cluster de base de données, le vCPU et la RAM doivent correspondre à ceux des cellules principale et en veille existantes dans le cluster.

La version du fichier OVA du dispositif en veille récemment déployé doit être la même que celle des dispositifs existants dans le cluster. Pour afficher la version des dispositifs en cours d'exécution, reportez-vous à la section À propos dans l'UI de gestion du dispositif. Le dispositif est distribué avec un nom sous la forme `VMware Cloud 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 Cloud Director-10.0.0.0-9229800_OVA10.ova`.

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 VMware Cloud Director avec VMware OVF Tool.

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

Conditions préalables

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

Procédure

1 Démarrer le déploiement du dispositif VMware Cloud 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 VMware Cloud Director et terminer le déploiement

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

Étape suivante

- Configurez l'adresse proxy de console publique, car le dispositif VMware Cloud Director utilise sa carte réseau `eth0` avec le port personnalisé 8443 pour le service de proxy de console. Reportez-vous à Personnaliser les adresses publiques pour VMware Cloud Director sous Linux.

- Pour ajouter des membres au groupe de serveurs VMware Cloud Director, répétez la procédure.
- Pour entrer la clé de licence, connectez-vous au VMware Cloud Director Service Provider Admin Portal.
- 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 VMware Cloud Director sous Linux.

Démarrer le déploiement du dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données VMware Cloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`.
Principal-grand	VMware Cloud Director 10.1.3 et versions ultérieures déploient le dispositif avec 24 Go de RAM et 8 vCPU en tant que premier membre d'un groupe de serveurs VMware Cloud Director. VMware Cloud Director 10.1 déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que premier membre d'un groupe de serveurs VMware Cloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données VMware Cloud 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 VMware Cloud 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.

Option	Description
En veille-grand	Permet de joindre une grande cellule principale dans un cluster HA de base de données. VMware Cloud Director 10.1.3 et versions ultérieures déploient le dispositif avec 24 Go de RAM et 8 vCPU en tant que deuxième ou troisième membre dans un groupe de serveurs VMware Cloud Director avec une configuration haute disponibilité de base de données. VMware Cloud Director 10.1 déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que deuxième ou troisième membre d'un groupe de serveurs VMware Cloud 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	VMware Cloud Director 10.1.3 déploie le dispositif avec 8 Go de RAM et 4 vCPU en tant que membre suivant dans un groupe de serveurs VMware Cloud Director. VMware Cloud Director 10.1 déploie le dispositif avec 8 Go de RAM et 2 vCPU en tant que membre suivant dans un groupe de serveurs VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Personnaliser le dispositif VMware Cloud Director et terminer le déploiement

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

Lorsque vous personnalisez le dispositif VMware Cloud 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 VMware Cloud 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.
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 pour VMware Cloud Director sur Linux.

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**, saisissez 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
Programme d'amélioration du produit	Active ou désactive la participation au programme d'amélioration du produit VMware.
Mot de passe de base de données « vcloud » pour l'utilisateur « vcloud »	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**. Le mot de passe doit comporter entre 6 et 128 caractères.
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 VMware Cloud Director. Réglé par défaut sur `vcd1`.
ID d'installation	L'ID à utiliser pour cette installation de VMware Cloud 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 VMware Cloud Director sur des déploiements multisites, envisagez de définir un identifiant d'installation unique pour chaque installation de VMware Cloud 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**.

Si vous souhaitez atteindre des hôtes sur un itinéraire de passerelle autre que celui par défaut, vous devrez peut-être fournir des routes statiques. 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, 172.16.200.253`**.

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**.

Paramètre	Description
Passerelle par défaut	L'adresse IP de la passerelle par défaut pour le dispositif.
Nom de domaine	Le domaine de recherche DNS, par exemple *mondomaine.com*.
Chemin de recherche du domaine	Liste de noms de domaine séparés par des virgules ou des espaces pour la recherche du nom d'hôte du dispositif, par exemple *subdomain.example.com*. **Note** Le nom de domaine que vous avez saisi dans la zone de texte Nom de domaine est le premier élément dans la liste des chemins de recherche de domaine.
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 VMware Cloud Director, puis cliquez sur **Terminer** pour démarrer le déploiement.

Étape suivante

- Mettez sous tension la nouvelle machine virtuelle.
- Modifier le fuseau horaire du dispositif VMware Cloud Director

Déploiement du dispositif VMware Cloud Director avec VMware OVF Tool

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

Vous devez déployer le premier membre d'un groupe de serveurs VMware Cloud Director en tant que cellule principale. Vous pouvez déployer un membre suivant d'un groupe de serveurs VMware Cloud 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*.

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

Lors de l'ajout de dispositifs supplémentaires ou de remplacement à un cluster de base de données, le vCPU et la RAM doivent correspondre à ceux des cellules principale et en veille existantes dans le cluster.

La version du fichier OVA du dispositif en veille récemment déployé doit être la même que celle des dispositifs existants dans le cluster. Pour afficher la version des dispositifs en cours d'exécution, reportez-vous à la section À propos dans l'UI de gestion du dispositif. Le dispositif est distribué avec un nom sous la forme `VMware Cloud 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 Cloud Director-10.0.0.0-9229800_OVA10.ova`.

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

Vous pouvez également déployer le dispositif à l'aide de vSphere Client. Reportez-vous à la section Déployer une instance de VMware Cloud Director Appliance à l'aide de vSphere Client.

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

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

Options et propriétés de commande `ovftool` pour le déploiement du dispositif VMware Cloud 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`.

Option	Valeur	Description
`--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.
`--prop:"vami.gateway.VMware_vCloud_Director`	*gateway_ip_address*	L'adresse IP de la passerelle par défaut pour le dispositif.
`--prop:"vami.netmask0.VMware_vCloud_Director`	*network_mask*	Le masque réseau ou le préfixe de l'interface `eth0`.
`--prop:"vami.netmask1.VMware_vCloud_Director`	*network_mask*	Le masque réseau ou le préfixe de l'interface `eth1`.
`--prop:"vami.searchpath.VMware_vCloud_Director`	*domain_names*	Le chemin de recherche du domaine du dispositif. Liste de noms de domaine séparés par des virgules ou des espaces.
`--prop:"vcloudapp.ceip_enabled.VMware_vCloud_Director`	`true` ou `false`	Active ou désactive la participation au Programme d'amélioration du produit VMware. La valeur par défaut est true.
`--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director`	`true` ou `false`	Active ou désactive l'accès SSH **racine** au dispositif.

Option	Valeur	Description
`--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"`		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"`	*address*	L'adresse e-mail du compte de l'**administrateur système**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director"`	*name*	Le nom du compte de l'**administrateur système**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director"`	*password*	Le mot de passe du compte de l'**administrateur système**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director"`	*username*	Le nom d'utilisateur pour l'**administrateur système**. Utilisé uniquement pour une cellule principale.
`--prop:"vcloudwiz.inst_id.VMware_vCloud_Director"`	*ID*	L'ID d'installation de VMware Cloud Director. Utilisé uniquement pour une cellule principale.

Option	Valeur	Description
`--prop:"vcloudconf.sys_name.VMware_vCloud_System_name"`	*cloud_director_name*	Le nom du dossier vCenter Server à créer pour cette installation de VMware Cloud Director.
`--prop:"vcloudnet.routes0.VMware_vCloud_Network_Address"`	*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_Network_Address"`	*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 VMware Cloud 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. ■ `primary-small` déploie le dispositif avec 12 Go de RAM et 2 vCPU en tant que premier membre dans un groupe de serveurs VMware Cloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données VMware Cloud Director. Le nom de la base de données est `vcloud` et l'utilisateur de la base de données est `vcloud`. ■ `primary-large` pour les versions 10.1.3 et ultérieures déploie le dispositif avec 24 Go de RAM et 8 vCPU en tant que premier membre d'un groupe de serveurs VMware Cloud Director. `primary-large` pour la version 10.1 déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que premier membre d'un groupe de serveurs VMware Cloud Director. La base de données intégrée dans la cellule principale est configurée en tant que base de données VMware Cloud 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 VMware Cloud Director avec une configuration haute disponibilité de base de données.

Option	Valeur	Description
		La base de données intégrée dans une cellule en veille est configurée en mode de réplication avec la base de données principale. ■ `standby-large` pour les versions 10.1.3 et ultérieures déploie le dispositif avec 24 Go de RAM et 8 vCPU en tant que deuxième ou troisième membre dans un groupe de serveurs VMware Cloud Director avec une configuration haute disponibilité de base de données. `standby-large` pour la version 10.1 déploie le dispositif avec 24 Go de RAM et 4 vCPU en tant que deuxième ou troisième membre d'un groupe de serveurs VMware Cloud 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. ■ `cell` pour les versions 10.1.3 et ultérieures déploie le dispositif avec 8 Go de RAM et 4 vCPU en tant que premier membre d'un groupe de serveurs VMware Cloud Director. `cell` pour la version 10.1 déploie le dispositif avec 8 Go de RAM et 2 vCPU en tant que membre suivant dans un groupe de serveurs VMware Cloud Director. La base de données intégrée dans une cellule

Option	Valeur	Description
		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 VMware Cloud 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 VMware Cloud Director principal

Important Avant d'exécuter la commande VMware OVF Tool, remplacez les mots de passe `vcloudapp.varoot-passwordVMware_vCloud_Director`, `vcloudconf.db_pwdVMware_vCloud_Director` et `vcloudconf.admin_pwd.VMware_vCloud_Director` par vos propres mots de passe sécurisés.

```
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"="place-secure-password-here" \
```

```
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--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"="place-secure-password-here" \
--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 VMware Cloud Director en veille

Important Avant d'exécuter la commande VMware OVF Tool, remplacez le mot de passe `vcloudapp.varoot-password.VMware_vCloud_Director` par votre propre mot de passe sécurisé.

```
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"="place-secure-password-here" \
--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
```

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

Vous pouvez déployer le dispositif VMware Cloud 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 VMware Cloud Director, VMware Cloud Director génère des certificats auto-signés et les utilise pour configurer la cellule VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Si les certificats signés que vous utilisez sur le dispositif VMware Cloud Director principal sont des certificats signés par des caractères génériques, ces certificats peuvent s'appliquer à tous les autres dispositifs du groupe de serveurs VMware Cloud Director, c'est-à-dire aux cellules en veille et aux cellules d'application VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director nécessite deux certificats SSL pour sécuriser les communications entre les clients et les serveurs. Chaque serveur VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Important Lors du déploiement, le dispositif VMware Cloud 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 VMware Cloud Director. VMware Cloud Director place une copie de `keytool` dans `/opt/vmware/vcloud-director/jre/bin/keytool`.

Procédure

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

   Lorsque vous déployez le dispositif VMware Cloud Director, VMware Cloud 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 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 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

```
service vmware-vcd restart
```

Étape suivante

- Si vous utilisez des certificats génériques, reportez-vous à Déployer le dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, consultez Remplacer un certificat auto-signé de base de données PostgreSQL intégrée et d'interface utilisateur de gestion de dispositifs VMware Cloud Director.

Importer des clés privées et des certificats SSL signés par une autorité de certification dans le dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. VMware Cloud 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 à l'aide d'un client SSH à la console du dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

```
service vmware-vcd restart
```

Étape suivante

- Si vous utilisez des certificats génériques, reportez-vous à Déployer le dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, consultez Remplacer un certificat auto-signé de base de données PostgreSQL intégrée et d'interface utilisateur de gestion de dispositifs VMware Cloud Director.

Après le déploiement du dispositif VMware Cloud Director

Après avoir créé le groupe de serveurs VMware Cloud 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.

Après la création du dispositif VMware Cloud Director, vous pouvez utiliser les fonctionnalités de mise en réseau vSphere pour ajouter une nouvelle carte réseau (NIC). Consultez les informations de Ajouter un adaptateur réseau à une machine virtuelle dans le guide *Administration d'une machine virtuelle vSphere*.

Note Si votre cluster est configuré pour le basculement automatique, après avoir déployé une ou plusieurs cellules supplémentaires, vous devez utiliser Appliance API pour réinitialiser le mode de basculement sur `Automatic`. Reportez-vous à l'API du dispositif VMware Cloud Director. Le mode de basculement par défaut des nouvelles cellules est `Manual`. Si le mode de basculement est incohérent entre les nœuds du cluster, le mode de basculement du cluster est `Indeterminate`. Le mode `Indeterminate` peut créer des états de cluster incohérents entre les nœuds et les nœuds qui suivent une ancienne cellule principale. Pour afficher le mode de basculement du cluster, reportez-vous à Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Modifier le fuseau horaire du dispositif VMware Cloud Director

Une fois que vous avez déployé le dispositif VMware Cloud Director, vous pouvez en modifier le fuseau horaire. Toutes les instances du dispositif VMware Cloud Director dans le groupe de serveurs et le stockage du serveur de transfert doivent utiliser les mêmes paramètres.

Conditions préalables

- Déployez le dispositif VMware Cloud Director. Reportez-vous à Déploiement et configuration initiale du dispositif VMware Cloud Director.
- Remplacez le fuseau horaire de stockage du serveur de transfert par le nouveau fuseau horaire du dispositif principal deVMware Cloud Director.

Procédure

1. À l'aide d'une console Web ou d'une console distante pour le nœud principal, dans la partie inférieure gauche de la fenêtre de la console, sélectionnez **Définir le fuseau horaire**.

2 Sélectionnez un emplacement, un pays et une région de fuseau horaire.

   Le nouveau fuseau horaire sélectionné s'affiche en bas à gauche de la fenêtre de la console.

3 Connectez-vous à la console du dispositif VMware Cloud Director en tant qu'utilisateur **racine**.

4 Pour vous assurer que le dispositif VMware Cloud Director utilise le nouveau fuseau horaire, redémarrez le service `vmware-vcd`.

5 Répétez l'Étape 1 à Étape 4 pour toutes les cellules en veille et d'application de votre déploiement de VMware Cloud Director.

Personnaliser les adresses publiques du dispositif VMware Cloud Director

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 le portail Web de VMware Cloud Director, l'API VMware Cloud Director et le proxy de console.

Vous devez configurer l'adresse proxy de console publique VMware Cloud Director, car le dispositif utilise une adresse IP unique avec le port personnalisé 8443 pour le service de proxy de console. Reportez-vous à 6.

Conditions préalables

Vérifiez que vous êtes connecté en tant qu'**administrateur système**. Seul un **administrateur système** peut personnaliser les points de terminaison publics.

Procédure

1 Dans la barre de navigation supérieure du Service Provider Admin Portal, sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Paramètres**, cliquez sur **Adresses publiques**.

3 Pour personnaliser les points de terminaison publics, cliquez sur **Modifier**.

4 Pour personnaliser les URL VMware Cloud Director, modifiez les points de terminaison du **portail Web**.

   a Entrez une URL publique VMware Cloud Director personnalisée pour les connexions HTTPS (sécurisées) et cliquez sur **Télécharger** pour télécharger les certificats qui établissent la chaîne d'approbation pour ce point de terminaison.

      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 cellule VMware Cloud Director avec l'alias `consoleproxy`. Les terminaisons SSL des connexions de proxy de console sur un équilibrage de charge ne sont pas prises en charge. 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 (Facultatif) Pour personnaliser les URL REST API et OpenAPI de Cloud Director, désactivez le bouton bascule **Utiliser les paramètres de portail Web**.

   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 VMware Cloud Director à l'adresse `http://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI VMware Cloud Director à l'adresse `http://vcloud.example.com/cloudapi`.

   b Entrez une URL de base HTTPS personnalisée pour l'API REST et cliquez sur **Télécharger** 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 REST API sur **`https://vcloud.example.com`**, vous pouvez accéder à l'API VMware Cloud Director à l'adresse `https://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI VMware Cloud Director 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 VMware Cloud 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.

6 Entrez une adresse proxy de console publique VMware Cloud Director personnalisée.

   Cette adresse est le nom de domaine complet (FQDN) de la carte réseau `eth0` du dispositif VMware Cloud Director, spécifiée par le nom de domaine complet ou l'adresse IP, avec le port personnalisé 8443 pour le service de proxy de la console.

   Par exemple, pour une instance de dispositif VMware Cloud Director ayant le nom de domaine complet `vcloud.example.com`, entrez **`vcloud.example.com:8443`**.

   VMware Cloud Director utilise l'adresse proxy de la console lors de l'ouverture d'une fenêtre de console distante sur une machine virtuelle.

7 Pour enregistrer les modifications, cliquez sur **Enregistrer**.

Installer et configurer une base de données Cassandra pour stocker les données de mesure historiques

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. La récupération des mesures historiques ne nécessite pas l'utilisation du logiciel de base de données facultatif.

Conditions préalables

- Vérifiez que VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Chapitre 5 Référence de l'outil de gestion des cellules.

2 (Facultatif) Si vous mettez à niveau VMware Cloud 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 VMware Cloud Director.

Installer et configurer un broker AMQP RabbitMQ

Si vous souhaitez utiliser des tâches bloquantes, des notifications ou des extensions d'API VMware Cloud Director, comme Container Service Extension (CSE), VMware Cloud Director App Launchpad ou vRealize Operations Tenant App, vous devez 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. VMware Cloud 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.

Pour VMware Cloud Director sur les installations Linux, l'utilisation d'un client MQTT peut être une alternative au broker AMQP RabbitMQ lors de la configuration de notifications. Reportez-vous à la section S'abonner à des événements et à des tâches à l'aide d'un client MQTT.

Procédure

1 Téléchargez le serveur RabbitMQ depuis https://www.rabbitmq.com/download.html.

   Reportez-vous à la section *Notes de mise à jour de VMware Cloud 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 VMware Cloud 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 VMware Cloud 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. La valeur par défaut est `5672` pour une connexion non-SSL. Le port par défaut pour SSL/TLS est `5671`.
   - Le protocole de communication est TCP.
   - L'hôte virtuel RabbitMQ. Par défaut « `/` ».

Étape suivante

Par défaut, le service AMQP de VMware Cloud 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 VMware Cloud Director, généralement situé à `$VCLOUD_HOME/jre/lib/security/cacerts`.

Pour activer SSL avec le service AMQP de VMware Cloud Director, reportez-vous à la section Configurer un broker AMQP dans le *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

Mise à niveau et migration du dispositif VMware Cloud Director

À partir de la version 9.7, le dispositif VMware Cloud Director inclut une base de données PostgreSQL intégrée avec la fonction HA (High Availability). Vous pouvez mettre à niveau le dispositif VMware Cloud Director vers une version ultérieure. Vous pouvez également migrer votre version antérieure existante de VMware Cloud Director incluant une base de données PostgreSQL externe vers un environnement VMware Cloud Director qui se compose de déploiements de dispositifs VMware Cloud Director version 10.0 ou version ultérieure.

Mise à niveau du dispositif VMware Cloud Director

Pour la mise à niveau de la version 9.7 du dispositif VMware Cloud Director vers la version 10.1, reportez-vous à la section Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour.

À partir de VMware Cloud Director 10.0, les bases de données Microsoft SQL Server ne sont pas prises en charge.

Lorsque vous mettez à niveau VMware Cloud 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 VMware Cloud Director. Pour plus d'informations, reportez-vous au tableau Chemins de mise à niveau et de migration.
- La version de VMware vSphere ® que vous utilisez actuellement.
- La version de VMware NSX® que vous utilisez actuellement.
- Tous les composants tiers qui interagissent directement avec VMware Cloud Director.

Pour plus d'informations sur la compatibilité de VMware Cloud 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 VMware Cloud Director, vous devez les mettre à niveau après la mise à niveau de VMware Cloud Director. Reportez-vous à Après la mise à niveau de VMware Cloud Director.

Après la mise à niveau d'au moins un serveur VMware Cloud Director, vous pouvez mettre à niveau la base de données VMware Cloud Director. La base de données détient des informations relatives à l'état d'exécution du serveur, notamment l'état de toutes les tâches VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.`

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux

locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Important Après la mise à niveau vers la version 10.1, VMware Cloud Director vérifie toujours les certificats pour tous les points de terminaison d'infrastructure qui y sont connectés. Cela est dû à une modification de la manière dont VMware Cloud Director gère les certificats SSL. Si vous n'importez pas vos certificats dans VMware Cloud Director avant la mise à niveau, les connexions vCenter Server et NSX peuvent afficher des erreurs de connexion infructueuses en raison de problèmes de vérification SSL. Dans ce cas, après la mise à niveau, vous avez deux options :

1. Exécutez la commande `trust-infra-certs` de l'outil de gestion des cellules pour importer automatiquement tous les certificats dans le magasin de certificats centralisé. Reportez-vous à la section Importer des certificats de point de terminaison depuis les ressources vSphere.
2. Dans l'interface utilisateur de Service Provider Admin Portal, sélectionnez chaque instance de vCenter Server et NSX, puis entrez à nouveau les informations d'identification tout en acceptant le certificat.

Migration du dispositif VMware Cloud Director

Si votre groupe de serveurs VMware Cloud Director existant se compose de déploiements de dispositifs VMware Cloud Director 9.5, vous pouvez uniquement migrer votre environnement vers une version plus récente du dispositif VMware Cloud Director. Utilisez le programme d'installation de VMware Cloud Director pour Linux pour mettre à niveau l'environnement existant uniquement dans le cadre du workflow de migration. Voir Migration vers le dispositif vCloud Director.

Si votre environnement VMware Cloud Director utilise une base de données Oracle externe ou une base de données Microsoft SQL externe, vous devez migrer vers une base de données PostgreSQL avant la mise à niveau vers VMware Cloud Director 10.1. Pour les chemins de mise à niveau, voir Mise à niveau de VMware Cloud Director sous Linux.

Chemins et workflows de mise à niveau et de migration

Environnement source	Environnement cible Dispositif VMware Cloud Director 10.1 incluant une base de données PostgreSQL intégrée
VMware Cloud Director 9.0 et 9.1 incluant une base de données Oracle externe	1 Pour VMware Cloud Director 9.0 sur Linux, mettez à niveau VMware Cloud Director vers la version 9.1. Reportez-vous à la section Mise à niveau de vCloud Director. 2 Migrez la base de données Oracle vers une base de données PostgreSQL. Reportez-vous à la section Migrer vers une base de données PostgreSQL. 3 Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director. 4 Migrez vers un dispositif VMware Cloud Director 10.1. Reportez-vous à la section Migration de VMware Cloud Director avec une base de données PostgreSQL externe vers un dispositif VMware Cloud Director.
Dispositif VMware Cloud Director 9.5 incluant une base de données PostgreSQL externe	1 Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director. 2 Migrez vers un dispositif VMware Cloud Director 10.1. Reportez-vous à la section Migration de VMware Cloud Director avec une base de données PostgreSQL externe vers un dispositif VMware Cloud Director.
VMware Cloud Director 9.0, 9.1 et 9.5 sur Linux incluant une base de données PostgreSQL externe	1 Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director. 2 Migrez vers un dispositif VMware Cloud Director 10.1. Reportez-vous à la section Migration de VMware Cloud Director avec une base de données PostgreSQL externe vers un dispositif VMware Cloud Director.
VMware Cloud Director 9.0, 9.1 et 9.5 sur Linux incluant une base de données Microsoft SQL Server externe	1 Mettez à niveau votre environnement vers VMware Cloud Director 9.7 sur Linux. Reportez-vous à la section Mise à niveau de vCloud Director. 2 Migrez vers le dispositif VMware Cloud Director 9.7. Reportez-vous à la section Migration de vCloud Director incluant une base de données Microsoft SQL externe vers un dispositif vCloud Director. 3 Mettez à niveau votre environnement vers un dispositif VMware Cloud Director 10.1. Voir Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour.

Environnement source	Environnement cible Dispositif VMware Cloud Director 10.1 incluant une base de données PostgreSQL intégrée
VMware Cloud Director 9.7 sur Linux incluant une base de données Microsoft SQL Server externe	1 Migrez vers le dispositif VMware Cloud Director 9.7. Reportez-vous à la section Migration de vCloud Director incluant une base de données Microsoft SQL externe vers un dispositif vCloud Director. 2 Mettez à niveau votre environnement vers un dispositif VMware Cloud Director 10.1. Voir Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour.
VMware Cloud Director 9.7 sur Linux incluant une base de données PostgreSQL externe	1 Migrez vers un dispositif VMware Cloud Director 9.7. Reportez-vous à la section Migration de vCloud Director incluant une base de données PostgreSQL externe vers un dispositif vCloud Director. 2 Mettez à niveau votre environnement vers un dispositif VMware Cloud Director 10.1. Voir Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour.
VMware Cloud Director 10.0 sur Linux incluant une base de données PostgreSQL externe	1 Migrez vers un dispositif VMware Cloud Director 10.0. Reportez-vous à la section Migration de vCloud Director incluant une base de données PostgreSQL externe vers un dispositif vCloud Director. 2 Mettez à niveau votre environnement vers un dispositif VMware Cloud Director 10.1. Voir Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour.
Dispositif VMware Cloud Director 9.7 et 10.0 incluant une base de données PostgreSQL intégrée	Mettez à niveau votre environnement vers un dispositif VMware Cloud Director 10.1. Voir Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour.

Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour

Vous pouvez mettre à niveau le dispositif VMware Cloud Director vers la dernière version ou appliquer des correctifs au dispositif VMware Cloud Director à l'aide d'un module de mise à jour.

Pendant la mise à niveau du dispositif VMware Cloud Director, le service VMware Cloud Director cesse de fonctionner et une interruption de service est à prévoir. L'interruption de service dépend du temps nécessaire pour mettre à niveau chaque dispositif VMware Cloud Director et pour exécuter le script de mise à niveau de la base de données VMware Cloud Director. Le nombre de cellules de travail dans le groupe de serveurs VMware Cloud Director diminue jusqu'à ce que vous arrêtiez le service VMware Cloud Director sur le dernier dispositif VMware Cloud Director. Un équilibrage de charge correctement configuré devant les points de terminaison HTTP VMware Cloud Director doit arrêter le routage du trafic vers les cellules qui sont arrêtées.

Après l'application de la mise à niveau sur chaque dispositif VMware Cloud Director et une fois la mise à niveau de la base de données terminée, vous devez redémarrer chaque dispositif VMware Cloud Director.

Conditions préalables

Prenez un snapshot du dispositif VMware Cloud Director principal.

1 Lors de la mise à niveau de la version 10.1 ou ultérieure ou de l'application de correctifs, si le basculement automatique en cas d'échec du service de base de données principal est activé, passez le mode de basculement sur `Manual` pendant la mise à niveau. Après la mise à niveau, vous pouvez définir le mode de basculement sur `Automatic`. Reportez-vous à la section Basculement automatique du dispositif VMware Cloud Director.

2 Connectez-vous à l'instance de vCenter Server sur laquelle réside le dispositif VMware Cloud Director principal de votre cluster haute disponibilité de base de données.

3 Accédez au dispositif VMware Cloud Director principal, cliquez sur lui avec le bouton droit, puis cliquez sur **Alimentation > Arrêter le SE invité**.

4 Cliquez sur le dispositif avec le bouton droit, puis cliquez sur **Snapshots > Prendre un snapshot** . Entrez un nom et, éventuellement, une description pour le snapshot, puis cliquez sur **OK**.

5 Cliquez avec le bouton droit sur le dispositif VMware Cloud Director, puis cliquez sur **Alimentation > Mettre sous tension**.

6 Vérifiez que tous les nœuds de votre configuration haute disponibilité de la base de données sont en bon état. Reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

Procédure

1 Dans un navigateur Web, connectez-vous à l'interface utilisateur de gestion de dispositif d'une instance du dispositif VMware Cloud Director pour identifier le dispositif principal, `https://`*`appliance_ip_address`*`:5480`.

Notez le nom du dispositif principal. Vous devez mettre à niveau le dispositif principal avant les cellules de veille et d'application. 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 le dispositif que vous mettez à niveau.

Note Vous devez d'abord mettre à niveau le dispositif principal.

VMware Cloud Director est distribué sous la forme d'un fichier exécutable avec un nom au format `VMware_Cloud_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_Cloud_Director_10.1.0.4424-14420378_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_Cloud_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 de la mise à niveau s'affiche sous la forme d'une `Mise à jour disponible`.

7 Arrêtez VMware Cloud Director en exécutant la commande suivante :

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

8 Appliquez la mise à niveau disponible.

```
vamicli update --install latest
```

9 Répétez 2 à 8 sur les cellules de veille et d'application restantes.

10 Depuis le dispositif principal, sauvegardez la base de données intégrée du dispositif VMware Cloud Director.

```
/opt/vmware/appliance/bin/create-db-backup
```

11 Depuis n'importe quel dispositif, exécutez l'utilitaire `upgrade` de la base de données VMware Cloud Director.

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

12 Redémarrez chaque dispositif VMware Cloud Director.

```
shutdown -r now
```

Étape suivante

- Si la mise à niveau réussit, vous pouvez supprimer le snapshot du dispositif VMware Cloud Director.
- Si la mise à niveau échoue, vous pouvez restaurer le dispositif VMware Cloud Director sur le snapshot que vous avez pris avant la mise à niveau. Reportez-vous à la section Restaurer un dispositif VMware Cloud Director en cas d'échec d'une mise à niveau.

Mettre à niveau le dispositif VMware Cloud Director à l'aide du référentiel de mise à jour de VMware

Vous pouvez utiliser le référentiel de mise à jour de VMware pour mettre à niveau le dispositif VMware Cloud Director de la version 9.7 vers la version 10.0 et versions ultérieures ou appliquer des correctifs.

Note Vous pouvez utiliser le référentiel de mise à jour de VMware uniquement pour mettre à niveau VMware Cloud Director vers la version la plus récente de VMware Cloud Director. Seule la version la plus récente est disponible dans le référentiel de mise à jour de VMware. Si vous souhaitez mettre à niveau VMware Cloud Director vers une version différente, reportez-vous à Mettre à niveau le dispositif VMware Cloud Director à l'aide d'un module de mise à jour.

Pendant la mise à niveau du dispositif VMware Cloud Director, le service VMware Cloud Director cesse de fonctionner et une interruption de service est à prévoir. L'interruption de service dépend du temps nécessaire pour mettre à niveau chaque dispositif VMware Cloud Director et pour exécuter le script de mise à niveau de la base de données VMware Cloud Director. Le nombre de cellules de travail dans le groupe de serveurs VMware Cloud Director diminue jusqu'à ce que vous arrêtiez le service VMware Cloud Director sur le dernier dispositif VMware Cloud Director. Un équilibrage de charge correctement configuré devant les points de terminaison HTTP VMware Cloud Director doit arrêter le routage du trafic vers les cellules qui sont arrêtées.

Après l'application de la mise à niveau sur chaque dispositif VMware Cloud Director et une fois la mise à niveau de la base de données terminée, vous devez redémarrer chaque dispositif VMware Cloud Director.

Conditions préalables

- Prenez un snapshot du dispositif VMware Cloud Director principal.
  a. Lors de la mise à niveau de la version 10.1 ou ultérieure ou de l'application de correctifs, si le basculement automatique en cas d'échec du service de base de données principal est activé, passez le mode de basculement sur `Manual` pendant la durée de la mise à niveau. Après la mise à niveau, vous pouvez définir le mode de basculement sur `Automatic`. Reportez-vous à la section Basculement automatique du dispositif VMware Cloud Director.
  b. Connectez-vous à l'instance de vCenter Server sur laquelle réside le dispositif VMware Cloud Director principal de votre cluster haute disponibilité de base de données.
  c. Accédez au dispositif VMware Cloud Director principal, cliquez sur lui avec le bouton droit, puis cliquez sur **Alimentation > Arrêter le SE invité**.
  d. Cliquez sur le dispositif avec le bouton droit, puis cliquez sur **Snapshots > Prendre un snapshot** . Entrez un nom et, éventuellement, une description pour le snapshot, puis cliquez sur **OK**.
  e. Cliquez avec le bouton droit sur le dispositif VMware Cloud Director, puis cliquez sur **Alimentation > Mettre sous tension**.

f Vérifiez que tous les nœuds de votre configuration haute disponibilité de la base de données sont en bon état. Reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

- Vérifiez que le dispositif VMware Cloud Director a accès à `https://vapp-updates.vmware.com`.

Procédure

1 Dans un navigateur Web, connectez-vous à l'interface utilisateur de gestion de dispositif d'une instance du dispositif VMware Cloud 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 Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif principal en tant qu'utilisateur **racine**.

3 Réinitialisez le référentiel de mise à jour pour qu'il pointe vers le référentiel de mise à jour de VMware.

```
vamicli update --repo ""
```

4 Vérifiez les mises à jour pour vous assurer que le référentiel de mise à jour de VMware dispose de la mise à niveau souhaitée.

Par défaut, la commande `vamicli` pointe vers le référentiel de mise à jour de VMware.

```
vamicli update --check
```

La version de la mise à niveau s'affiche sous la forme d'une `Mise à jour disponible`.

5 Arrêtez VMware Cloud Director en exécutant la commande suivante :

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

6 Depuis le dispositif principal, sauvegardez la base de données intégrée du dispositif VMware Cloud Director.

```
/opt/vmware/appliance/bin/create-db-backup
```

Note Vous ne devez sauvegarder le dispositif qu'une seule fois. Ne sauvegardez pas le dispositif après l'application de la mise à niveau disponible.

7 Appliquez la mise à niveau disponible.

```
vamicli update --install latest
```

8 Connectez-vous aux cellules en veille et d'application restantes, puis répétez les étapes 3, 4, 5 et 7 sur chaque dispositif.

9 Depuis n'importe quel dispositif, exécutez l'utilitaire `upgrade` de la base de données VMware Cloud Director.

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

10 Redémarrez chaque dispositif VMware Cloud Director.

```
shutdown -r now
```

Étape suivante

- Si la mise à niveau réussit, vous pouvez supprimer le snapshot du dispositif VMware Cloud Director.
- Si la mise à niveau échoue, vous pouvez restaurer le dispositif VMware Cloud Director sur le snapshot que vous avez pris avant la mise à niveau. Reportez-vous à la section Restaurer un dispositif VMware Cloud Director en cas d'échec d'une mise à niveau.
- En cas d'échec de la commande `vamicli update --install latest`, reportez-vous à Échec de l'installation de la dernière mise à jour de VMware Cloud Director.

Restaurer un dispositif VMware Cloud Director en cas d'échec d'une mise à niveau

Si la mise à niveau d'un dispositif VMware Cloud Director échoue, vous pouvez utiliser le snapshot du dispositif que vous avez pris avant la mise à niveau et restaurer le dispositif VMware Cloud Director.

Avant de commencer la restauration, utilisez VMware Cloud Director Appliance API pour noter les ID de nœud des nœuds en veille dans le cluster. Reportez-vous à la section *Référence de schéma de l'API du dispositif VMware Cloud Director* sur http://code.vmware.com.

1 Restaurez le dispositif VMware Cloud Director principal sur le snapshot que vous avez pris avant de démarrer la mise à niveau.

   Découvrez comment restaurer des snapshots de machines virtuelles à l'aide des options de restauration. Reportez-vous à Restaurer des snapshots de machines virtuelles à l'aide de la restauration dans le *Guide d'administration de machine virtuelle vSphere*.

2 Mettez sous tension la cellule du dispositif principal VMware Cloud Director.

3 Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation de chaque cellule du dispositif VMware Cloud Director. Connectez-vous en tant qu'utilisateur **racine**.

4 Arrêtez les services VMware Cloud Director sur toutes les cellules du dispositif.

```
service vmware-vcd stop
```

5 Utilisez la cellule principale de VMware Cloud Director pour annuler l'enregistrement des nœuds secondaires dans le cluster.

   a Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation de la cellule principale en tant que **racine**.

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

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

   c Exécutez la commande d'annulation de l'enregistrement d'une cellule du dispositif en veille

   Pour annuler l'enregistrement d'un nœud en veille qui n'est pas en cours d'exécution, vous devez fournir l'ID du nœud.

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

   d Répétez 5.c pour annuler l'enregistrement de l'autre cellule du dispositif en veille.

6 Dans vSphere Client, arrêtez et supprimez tous les dispositifs en veille.

   a Dans vSphere Client, accédez aux dispositifs en veille.

   b Cliquez avec le bouton droit sur un dispositif en veille et cliquez sur **Alimentation > Arrêter le SE invité**.

   c Cliquez avec le bouton droit sur le dispositif, puis cliquez sur **Supprimer du disque**.

   d Répétez les étapes 6.a à 6.c pour l'autre cellule du dispositif en veille.

7 Vérifiez que la suite d'outils `repmgr` et la base de données PostgreSQL intégrée de la cellule du dispositif VMware Cloud Director principal fonctionnent correctement.

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

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

   b Exécutez la commande pour vérifier l'état du cluster.

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

   La sortie de la console affiche des informations sur le seul nœud du cluster.

   ```
        ID |  Name    | Role    | Status         | Upstream   | Location | Connection
   string
   --------+----------+---------+----------------+------------+----------
   +-------------------------
    Node 1 | Nom du nœud | primary |
   *running   |            | default | host=adresse IP de l'hôte user=repmgr dbname=repmgr
   ```

8 Redéployez les dispositifs secondaires. Reportez-vous à la section Déployer une instance de VMware Cloud Director Appliance à l'aide de vSphere Client.

9 Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation de chaque cellule du dispositif VMware Cloud Director. Connectez-vous en tant qu'utilisateur **racine**.

10 Démarrez les services VMware Cloud Director.

```
service vmware-vcd start
```

Migration de VMware Cloud Director avec une base de données PostgreSQL externe vers un dispositif VMware Cloud Director

Si votre environnement VMware Cloud Director actuel utilise une base de données PostgreSQL externe, vous pouvez migrer vers un nouvel environnement VMware Cloud Director qui se compose de déploiements de dispositifs VMware Cloud Director. Votre environnement VMware Cloud Director actuel peut se composer d'installations de VMware Cloud Director sur des déploiements de dispositifs Linux ou VMware Cloud Director. Le nouvel environnement VMware Cloud 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 VMware Cloud Director existant.
- Création du groupe de serveurs VMware Cloud Director en déployant une ou plusieurs instances du dispositif VMware Cloud Director.
- 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 de version 9.x, mettez à niveau la base de données PostgreSQL externe vers la version 10 ou ultérieure.

2 Mettez à niveau votre environnement VMware Cloud Director vers la version 10.1.

Reportez-vous à Mise à niveau de VMware Cloud Director sous Linux.

3 Vérifiez que le redémarrage de la source de migration VMware Cloud Director a réussi.

4 Sur chaque cellule de l'environnement VMware Cloud Director mis à niveau, exécutez la commande pour arrêter le service VMware Cloud 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 décrite à l'étape 13.

7 Si vous souhaitez que le nouvel environnement VMware Cloud 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`, `proxycertificates` et `truststore` 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 VMware Cloud 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 VMware Cloud Director.

   - 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 Déploiement et configuration initiale du dispositif VMware Cloud Director.

10 Sur chaque nouvelle cellule déployée, exécutez la commande pour arrêter le service VMware Cloud 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 VMware Cloud 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 portant 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 base de données 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 VMware Cloud 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 VMware Cloud Director.

a Sauvegardez les fichiers de propriétés, de magasins d'approbation et de certificats, puis copiez et remplacez ces fichiers depuis l'emplacement de la base de données PostgreSQL externe de la source de migration dans lequel vous avez copié les fichiers à l'étape 7 a.

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

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 VMware Cloud 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 VMware Cloud Director échoue lors de la migration ou de la restauration vers le dispositif VMware Cloud Director.

d Exécutez la commande pour démarrer le service VMware Cloud 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 Modifiez la configuration de votre équilibrage de charge pour inclure toutes les nouvelles adresses IP `eth0` de dispositif dans les pools d'équilibrage de charge pour le trafic HTTP, HTTPS et TCP, et supprimez les anciennes adresses IP de la cellule Linux VMware Cloud Director de ces pools.

16 Une fois que toutes les cellules du nouveau groupe de serveurs ont terminé le processus de démarrage, vérifiez que la migration de votre environnement VMware Cloud Director a réussi.

   a Ouvrez le Service Provider Admin Portal à l'aide de l'adresse IP du réseau `eth0` d'une cellule du nouveau groupe de serveurs, `https://`*`eth0_IP_new_cell`*`/provider`.

   b Connectez-vous au Service Provider Admin Portal avec vos informations d'identification d'**administrateur système** existantes depuis la source de migration.

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

17 Après avoir procédé à la vérification de la migration de VMware Cloud Director, utilisez la Service Provider Admin Portal pour supprimer les cellules déconnectées appartenant à l'ancien environnement VMware Cloud Director.

   a Dans la barre de navigation supérieure, sous **Ressources**, sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Cellules cloud**.

   c Sélectionnez une cellule inactive et cliquez sur **Annuler l'enregistrement**.

Vous pouvez déployer le dispositif VMware Cloud Director pour ajouter des membres au groupe de serveurs de l'environnement migré.

Étape suivante

L'environnement du nouveau dispositif VMware Cloud 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 VMware Cloud 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 de VMware Cloud Director

Après avoir mis à niveau l'ensemble des serveurs VMware Cloud Director et la base de données partagée, vous pouvez mettre à niveau les instances de 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 VMware Cloud Director.

Important VMware Cloud 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.

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Important Après la mise à niveau vers la version 10.1, VMware Cloud Director vérifie toujours les certificats pour tous les points de terminaison d'infrastructure qui y sont connectés. Cela est dû à une modification de la manière dont VMware Cloud Director gère les certificats SSL. Si vous n'importez pas vos certificats dans VMware Cloud Director avant la mise à niveau, les connexions vCenter Server et NSX peuvent afficher des erreurs de connexion infructueuses en raison de problèmes de vérification SSL. Dans ce cas, après la mise à niveau, vous avez deux options :

1. Exécutez la commande `trust-infra-certs` de l'outil de gestion des cellules pour importer automatiquement tous les certificats dans le magasin de certificats centralisé. Reportez-vous à la section Importer des certificats de point de terminaison depuis les ressources vSphere.
2. Dans l'interface utilisateur de Service Provider Admin Portal, sélectionnez chaque instance de vCenter Server et NSX, puis entrez à nouveau les informations d'identification tout en acceptant le certificat.

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 VMware Cloud 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 VMware Cloud Director, que des cellules VMware Cloud 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 VMware Cloud 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 VMware Cloud Director et NSX Manager, vous devez mettre à niveau les systèmes vCenter Server et les hôtes ESXi qui sont enregistrés sur VMware Cloud 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 barre de navigation supérieure du VMware Cloud Director Service Provider Admin Portal, sous **Ressources**, sélectionnez **Ressources vSphere**.

   b Dans le panneau de gauche, cliquez sur **Instances de vCenter Server**.

   c Sélectionnez la case d'option en regard de l'instance de vCenter Server que vous souhaitez désactiver et cliquez sur **Désactiver**.

   d Cliquez sur **OK**.

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 VMware Cloud Director.

   a Dans la barre de navigation supérieure, sélectionnez **Administration**.

   b Dans le panneau de gauche, sous **Paramètres**, cliquez sur **Adresses publiques**.

   c Vérifiez toutes les adresses publiques.

4 Actualisez l'enregistrement vCenter Server avec VMware Cloud Director.

   a Dans la barre de navigation supérieure du VMware Cloud Director Service Provider Admin Portal, sous **Ressources**, sélectionnez **Ressources vSphere**.

   b Dans le panneau de gauche, cliquez sur **Instances de vCenter Server**.

   c Cochez la case d'option en regard de l'instance cible de vCenter Server et cliquez sur **Reconnecter**.

   d Cliquez sur **OK**.

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 VMware Cloud 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 VMware Cloud Director afin de mettre à niveau une passerelle Edge NSX, vous devez intervenir sur l'objet réseau VMware Cloud Director que le dispositif Edge prend en charge :
     - Une mise à niveau appropriée d'une passerelle Edge s'exécute automatiquement lorsque vous utilisez VMware Cloud Director ou VMware Cloud Director API pour réinitialiser un réseau servi par la passerelle Edge.
     - Le redéploiement d'une passerelle Edge met à niveau le dispositif NSX Edge associé.

       Note Le redéploiement n'est pris en charge que pour les passerelles Edge NSX Data Center for vSphere.

- La réinitialisation d'un réseau vApp dans le contexte du vApp met à niveau le dispositif NSX Edge associé à ce réseau. Pour réinitialiser un réseau vApp dans le contexte d'un vApp, accédez à l'onglet **Réseaux** pour le vApp, affichez ses détails de mise en réseau, cliquez sur la case d'option en regard du nom du réseau vApp, puis cliquez sur **Réinitialiser**.

Pour plus d'informations sur le redéploiement de passerelles Edge et la réinitialisation de réseaux vApp, reportez-vous au *Guide de programmation de l'API VMware Cloud Director*.

Étape suivante

Reprenez cette procédure pour les autres systèmes vCenter Server enregistrés dans votre installation VMware Cloud Director.

Administration du dispositif VMware Cloud Director

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 VMware Cloud 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 VMware Cloud 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.

Note Si votre cluster est configuré pour le basculement automatique, après avoir déployé une ou plusieurs cellules supplémentaires, vous devez utiliser Appliance API pour réinitialiser le mode de basculement sur `Automatic`. Reportez-vous à l'API du dispositif VMware Cloud Director. Le mode de basculement par défaut des nouvelles cellules est `Manual`. Si le mode de basculement est incohérent entre les nœuds du cluster, le mode de basculement du cluster est `Indeterminate`. Le mode `Indeterminate` peut créer des états de cluster incohérents entre les nœuds et les nœuds qui suivent une ancienne cellule principale. Pour afficher le mode de basculement du cluster, reportez-vous à Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

Sauvegarde et restauration de la base de données intégrée du dispositif VMware Cloud Director

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

Sauvegarder la base de données intégrée du dispositif VMware Cloud Director

Si votre environnement comprend des déploiements de dispositifs VMware Cloud Director avec des bases de données PostgreSQL intégrées, vous pouvez sauvegarder la base de données VMware Cloud 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 à l'aide d'un client SSH, à la cellule principale en tant que **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`, `proxycertificates` et `truststore` de la cellule principale.

Restauration d'un environnement de dispositif VMware Cloud 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 VMware Cloud 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.

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 VMware Cloud Director.
- Déployez une cellule de base de données principale et deux cellules de base de données de secours. Reportez-vous à la section Déploiement et configuration initiale du dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director 9.7.0.1 et versions ultérieures.

```
cp certificates /opt/vmware/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 VMware Cloud 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 VMware Cloud Director échoue lors de la migration ou de la restauration vers le dispositif VMware Cloud Director.

e Exécutez la commande pour démarrer le service VMware Cloud 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 Déploiement et configuration initiale du dispositif VMware Cloud 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 VMware Cloud Director a réussi.

a Ouvrez le VMware Cloud Director Service Provider Admin Portal à l'aide de l'adresse IP du réseau `eth0` d'une cellule du nouveau groupe de serveurs, `https://`*`et0_IP_new_cell`*`/provider`.

b Connectez-vous à la Service Provider Admin Portal 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 Service Provider Admin Portal pour supprimer les cellules déconnectées appartenant à l'ancien environnement VMware Cloud Director.

a Dans la barre de navigation supérieure, sous **Ressources**, sélectionnez **Ressources de Cloud**.

b Dans le panneau de gauche, cliquez sur **Cellules cloud**.

c Sélectionnez une cellule inactive et cliquez sur **Annuler l'enregistrement**.

9 Si le mode de basculement avant la restauration était `Automatic`, vous devez le redéfinir sur `Automatic` à l'aide de VMware Cloud Director Appliance API.

Modification du mode de basculement du dispositif VMware Cloud Director

Par défaut, le dispositif VMware Cloud Director est en mode de basculement manuel et, si le service de base de données principal échoue, vous devez initier l'action de basculement. Vous pouvez définir le mode de basculement sur automatique à l'aide de l'API du dispositif .

À partir de VMware Cloud Director 10.1, si le service de base de données principale échoue, vous pouvez activer VMware Cloud Director pour effectuer un basculement automatique vers un nouveau service de base de données principale. Reportez-vous à la section Basculement automatique du dispositif VMware Cloud Director.

Le mode de basculement est défini sur `automatic` ou `manual` à l'aide de l'API du dispositif VMware Cloud Director. Reportez-vous à la section *Mode de basculement* de la Référence du schéma de l'API du dispositif VMware Cloud Director.

Pour les clusters configurés avec basculement automatique, après le déploiement d'une ou de plusieurs cellules supplémentaires, vous devez utiliser l'API du dispositif pour réinitialiser le mode de basculement du cluster sur `automatic`. Si vous ne réinitialisez pas le mode de basculement du cluster, le mode de basculement sur les nœuds devient incohérent.

Configurer l'accès externe à la base de données VMware Cloud Director

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

Lors d'une migration vers le dispositif VMware Cloud 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 VMware Cloud Director intégrée.

Procédure

1. Connectez-vous, directement ou à l'aide d'un client SSH, à la cellule principale en tant que **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 VMware Cloud 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.

Conditions préalables

Procédure

1 Si vous souhaitez apporter des modifications temporaires à la propriété OVF (par exemple, à des fins de test), modifiez la propriété dans VMware Cloud Director.

   a Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif VMware Cloud 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`**.

Modification des paramètres DNS du dispositif VMware Cloud Director

Après le déploiement, vous pouvez modifier le ou les serveurs DNS du dispositif VMware Cloud 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.

Conditions préalables

Procédure

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

   a Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif VMware Cloud 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 VMware Cloud Director

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

Conditions préalables

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 VMware Cloud Director.

   a Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif VMware Cloud 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 VMware Cloud 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 du dispositif VMware Cloud Director

Le dispositif VMware Cloud 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 VMware Cloud Director.

Renouveler les certificats du dispositif VMware Cloud Director

Lorsque vous déployez le dispositif VMware Cloud 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 VMware Cloud Director individuellement.

Le dispositif VMware Cloud Director utilise deux ensembles de certificats SSL. Le service VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director en tant qu'utilisateur **racine**.
2. Pour arrêter les services VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

```
service vmware-vcd start
```

Résultats

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

Le nouveau certificat PostgreSQL est importé dans le magasin d'approbations VMware Cloud Director sur les autres cellules VMware Cloud 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.

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

Par défaut, la base de données PostgreSQL intégrée et l'interface utilisateur de gestion des dispositifs VMware Cloud 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 VMware Cloud Director, il génère des certificats auto-signés avec une période de validité de 365 jours. Le dispositif VMware Cloud Director utilise deux ensembles de certificats SSL. Le service VMware Cloud 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 VMware Cloud 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 VMware Cloud Director sur les autres cellules VMware Cloud Director lors de la prochaine exécution de la fonction `appliance-sync`. L'opération peut prendre jusqu'à 60 secondes.

Augmenter la capacité de la base de données PostgreSQL intégrée sur un dispositif VMware Cloud Director

Si vous ne disposez pas d'un espace suffisant sur le disque de base de données PostgreSQL d'un dispositif VMware Cloud Director, vous pouvez augmenter la capacité de la base de données PostgreSQL intégrée.

La base de données PostgreSQL réside sur le disque dur 3. Sa taille par défaut est de 80 Go. La procédure peut être effectuée lorsque les dispositifs sont opérationnels.

Important Vous devez augmenter la capacité des dispositifs en veille existants avant d'augmenter la capacité du dispositif principal.

La taille de disque de la base de données PostgreSQL sur chaque dispositif en veille doit être équivalente à celle du disque de la base de données PostgreSQL sur le dispositif principal.

Conditions préalables

- Si votre environnement VMware Cloud Director comporte des nœuds en veille, identifiez les nœuds en veille et le nœud principal, puis commencez la procédure depuis un nœud en veille. Pour plus d'informations sur l'identification des rôles des nœuds, reportez-vous à Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.
- Si votre environnement VMware Cloud Director se compose uniquement d'un nœud principal, exécutez la procédure sur le nœud principal.

Procédure

1. Connectez-vous à vSphere Client pour augmenter la capacité du disque dur 3 à la taille souhaitée.

   La taille de disque de la base de données PostgreSQL sur chaque dispositif en veille doit être aussi importante que le disque de la base de données PostgreSQL sur le dispositif principal.

   a. Sélectionnez la machine virtuelle du dispositif que vous souhaitez modifier.

   b. Sélectionnez **Actions > Modifier les paramètres**.

   c. Augmentez la taille de **Disque dur 3** et cliquez sur **OK**.

   L'avancement de la tâche de reconfiguration s'affiche dans le volet **Tâches récentes**.

2. Appliquez les modifications au système d'exploitation du nœud du dispositif.

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

   b. Pour appliquer la modification du redimensionnement du disque dur au système d'exploitation, exécutez le script suivant.

   ```
   /opt/vmware/appliance/bin/db_diskresize.sh
   ```

3. Si votre environnement ne comporte qu'un seul dispositif principal, répétez la procédure pour chacun des nœuds disposant d'une base de données.

Modifier les configurations PostgreSQL dans le dispositif VMware Cloud Director

Vous pouvez modifier les configurations PostgreSQL du dispositif VMware Cloud 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 le fonctionnement du cluster nécessite un remplacement périodique du fichier et les modifications ne sont pas permanentes.

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 valeur du='paramètre';"
   ```

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@<adresse-nœud-en veille>:/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.

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

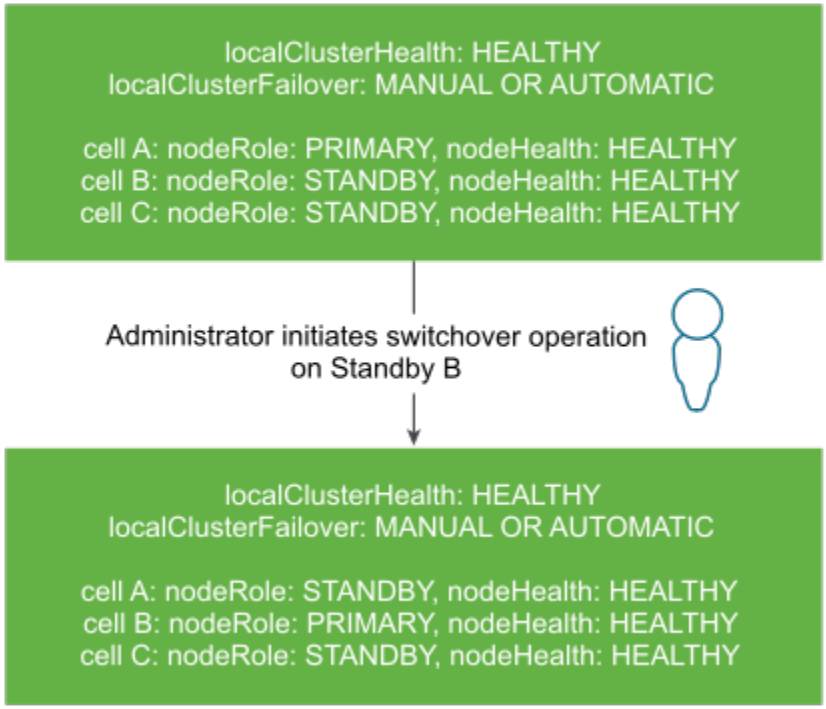
L'annulation de l'enregistrement du nœud supprime l'enregistrement du nœud en veille dans la table de métadonnées interne de la suite d'outils repmgr.

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 l'interface utilisateur de gestion du dispositif VMware Cloud Director pour changer les rôles des cellules d'un cluster haute disponibilité de base de données et promouvoir une cellule différente en tant que cellule principale.

Vous pouvez basculer les rôles de la cellule principale et de la cellule en veille à l'aide de l'interface utilisateur de gestion des dispositifs VMware Cloud Director ou de l'API du dispositif VMware Cloud Director. Cette procédure décrit les étapes de la procédure de basculement à l'aide de l'interface utilisateur de gestion.

Figure 3-3. Basculement entre la cellule principale et la cellule en veille



Conditions préalables

- Vérifiez que tous les nœuds du cluster sont sains et en ligne. Reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

Procédure

1. Suspendez les activités sur toutes les cellules VMware Cloud Director faisant partie du groupe de serveurs ou placez les cellules en mode de maintenance.

   Le basculement entraîne la non-disponibilité de la base de données VMware Cloud Director pendant 30 à 60 secondes. Pour éviter les défaillances de tâches inattendues, vous devez suspendre l'activité sur toutes les cellules du cluster.

2. Connectez-vous en tant qu'utilisateur **racine** à l'interface utilisateur de gestion de dispositif à l'adresse `https://primary_eth1_ip_address:5480`.

3. Dans le panneau de gauche, sélectionnez **Disponibilité de la base de données intégrée**.

   Vous pouvez afficher les noms des cellules, leurs rôles, leur état, le nom de la cellule que suivent les cellules en veille.

4. Vérifiez que la santé du cluster est `Healthy`.

5. Cliquez sur le bouton **Basculer** pour la cellule que vous souhaitez promouvoir comme cellule principale et confirmez le basculement.

6. Lorsque la tâche de basculement se termine, redémarrez le planificateur ou désactivez le mode de maintenance pour les cellules du cluster.

S'abonner à des événements et à des tâches à l'aide d'un client MQTT

Vous pouvez utiliser un client MQTT pour vous abonner à des messages concernant des événements et des tâches VMware Cloud Director.

MQTT est un protocole de transport de messagerie léger et binaire. VMware Cloud Director utilise MQTT pour publier des informations sur les événements et les tâches auxquels vous pouvez vous abonner à l'aide d'un client MQTT. Les messages MQTT transitent par un Broker MQTT qui peut également stocker des messages si les clients ne sont pas en ligne.

Conditions préalables

- Vérifiez que vous disposez d'un client MQTT qui prend en charge WebSocket.
- Vérifiez que vous pouvez ajouter des en-têtes à une demande mise à niveau par WebSocket.

Procédure

1. Connectez-vous à VMware Cloud Director à l'aide du point de terminaison OpenAPI.
2. Pour établir une connexion WebSocket, définissez la propriété Sec-WebSocket-Protocol sur `mqtt`, configurez le client pour qu'il se connecte au chemin d'accès `/messaging/mqtt`, ajoutez un en-tête d'autorisation et suivez le flux de connexion MQTT standard.

   Vous recevez le jeton JWT de la demande de connexion standard à VMware Cloud Director. Vous pouvez laisser le nom d'utilisateur et le mot de passe vides.

   ```
   Sec-WebSocket-Protocol: mqtt
   ```

   ```
   Authorization: Bearer {JWT_token}
   ```

3. Une fois que la connexion a été établie, abonnez-vous aux rubriques via le client MQTT.

   ```
   publish/{user_org_id}/{user_id}
   ```

   ```
   publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
   ```

   Les **administrateurs d'organisation** peuvent utiliser des caractères génériques pour accéder à toutes les rubriques de l'organisation.

   ```
   publish/{user_org_id}/*
   ```

   Les **administrateurs système** peuvent utiliser des caractères génériques pour accéder à toutes les rubriques.

   ```
   publish/*/*
   ```

Surveillance de la santé du cluster de base de données du dispositif VMware Cloud Director

Vous pouvez surveiller votre cluster de dispositifs VMware Cloud Director à l'aide de l'interface utilisateur de gestion du dispositif VMware Cloud Director Appliance, d'Appliance API ou de la suite d'outils open source repmgr.

Vous pouvez également utiliser l'interface utilisateur de gestion des dispositifs VMware Cloud Director pour afficher le mode de basculement du dispositif. Le mode de basculement indique si VMware Cloud Director déclenche automatiquement un basculement de base de données si la base de données principale échoue ou si **l'administrateur système** doit initier le basculement manuellement.

Si le mode de basculement est incohérent entre les nœuds, il est `Indeterminate`. Le mode `Indeterminate` peut créer des états de cluster incohérents entre les nœuds et les nœuds qui suivent une ancienne cellule principale. Vous devez diagnostiquer le problème et y remédier manuellement.

Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director

Vous pouvez surveiller l'état du cluster à l'aide de l'interface utilisateur de gestion des dispositifs VMware Cloud Director.

Vous pouvez afficher les noms des cellules d'un cluster, les rôles des cellules, l'état de la cellule, le nom de la cellule que suivent les cellules en veille et le mode de basculement du cluster à l'aide de l'interface utilisateur de gestion du dispositif VMware Cloud Director Appliance ou de VMware Cloud Director Appliance API. Cette procédure décrit les étapes de surveillance du cluster de dispositifs dans l'interface utilisateur de gestion.

Procédure

1. Connectez-vous en tant qu'utilisateur **racine** à l'interface utilisateur de gestion de dispositif à l'adresse `https://primary_eth1_ip_address:5480`.
2. Dans le panneau de gauche, sélectionnez **Disponibilité de la base de données intégrée**.

   Vous pouvez afficher les noms des cellules, leurs rôles, leur état, le nom de la cellule que suivent les cellules en veille.

3 Affichez la santé du cluster.

État de santé du cluster	Description
Sain	Le cluster est dans un état sain. La cellule principale et les deux cellules en veille sont en ligne et opérationnelles. L'interface utilisateur et l'API de VMware Cloud Director sont opérationnelles.
Dégradé	Le cluster est dans un état dégradé. La cellule principale et l'une des cellules en veille sont en ligne et opérationnelles, mais l'autre cellule en veille ne fonctionne pas. La base de données principale est opérationnelle dans cet état, mais s'il existe une autre panne de base de données de l'une des deux cellules opérationnelles, la cellule principale devient non fonctionnelle. La cellule en veille non fonctionnelle doit être remplacée par une nouvelle cellule en veille opérationnelle dès que possible pour restaurer le cluster à un état `Healthy`. L'interface utilisateur et l'API de VMware Cloud Director sont opérationnelles.
No_Active_Primary	Il n'y a pas de base de données principale opérationnelle. S'il y a deux cellules en veille opérationnelles, l'une d'entre elles doit être promue pour devenir la nouvelle cellule principale. Si l'environnement ne dispose pas de deux cellules en veille opérationnelles, vous devez diagnostiquer le problème et résoudre la situation manuellement. L'interface utilisateur et l'API de VMware Cloud Director ne sont pas disponibles.
Read_Only_Primary	Il y a une base de données principale en ligne, mais elle est `Read_Only`, car l'environnement ne dispose pas d'une cellule en veille opérationnelle. Deux nouvelles cellules en veille doivent être déployées. L'interface utilisateur et l'API de VMware Cloud Director ne sont pas disponibles.
Critical_Problem	Le cluster est dans un état incohérent. Par exemple, plusieurs cellules principales sont en ligne ou une cellule en veille ne suit pas la bonne cellule principale. Vous devez diagnostiquer le problème et y remédier manuellement. Cet état peut affecter la disponibilité de l'interface utilisateur et de l'API de VMware Cloud Director.

4 Affichez le mode de basculement du dispositif.

Mode de basculement	Description
Automatique	Si une panne de la base de données principale se produit, VMware Cloud Director déclenche automatiquement un basculement de base de données.
Manuelle	Si une panne de la base de données principale se produit, vous devez initier un basculement de base de données à l'aide de l'interface utilisateur de gestion des dispositifs VMware Cloud Director ou de l'API de basculement.
Indéterminé	Le mode de basculement n'est pas cohérent sur tous les nœuds du cluster. Vous devez diagnostiquer le problème et y remédier. À l'aide de l'API du dispositif VMware Cloud Director, réinitialisez le `FailoverMode` sur `Manual` ou sur `Automatic`. Reportez-vous aux informations sur le *mode de basculement* dans la rubrique *Référence de schéma de l'API du dispositif VMware Cloud Director*.

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 du nœud principal fournit des informations sur le nœud, la version de PostgreSQL et les détails de la réplication. Par exemple :

```
Node "bos1-vcloud-static-161-5":
        PostgreSQL version: 10.9
        Total data size: 81 MB
        Conninfo: host=172.18.36.193 user=repmgr dbname=repmgr connect_timeout=2
        Role: primary
        WAL archiving: off
        Archive command: (none)
        Replication connections: 2 (of maximal 10)
        Replication slots: 0 physical (of maximal 10; 0 missing)
        Replication lag: n/a
```

La sortie système d'un nœud en veille fournit des informations sur le nœud, la version de PostgreSQL, les détails de la réplication et un nœud en amont. Par exemple :

```
Node "bos1-vcloud-static-161-49":
    PostgreSQL version: 10.9
    Total data size: 83 MB
    Conninfo: host=172.18.36.191 user=repmgr dbname=repmgr connect_timeout=2
    Role: standby
    WAL archiving: off
    Archive command: (none)
    Replication connections: 0 (of maximal 10)
    Replication slots: 0 physical (of maximal 10; 0 missing)
    Upstream node: bos1-vcloud-static-161-48 (ID: 683)
    Replication lag: 0 seconds
    Last received LSN: 2/D863B4E0
    Last replayed LSN: 2/D863B4E0
```

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.

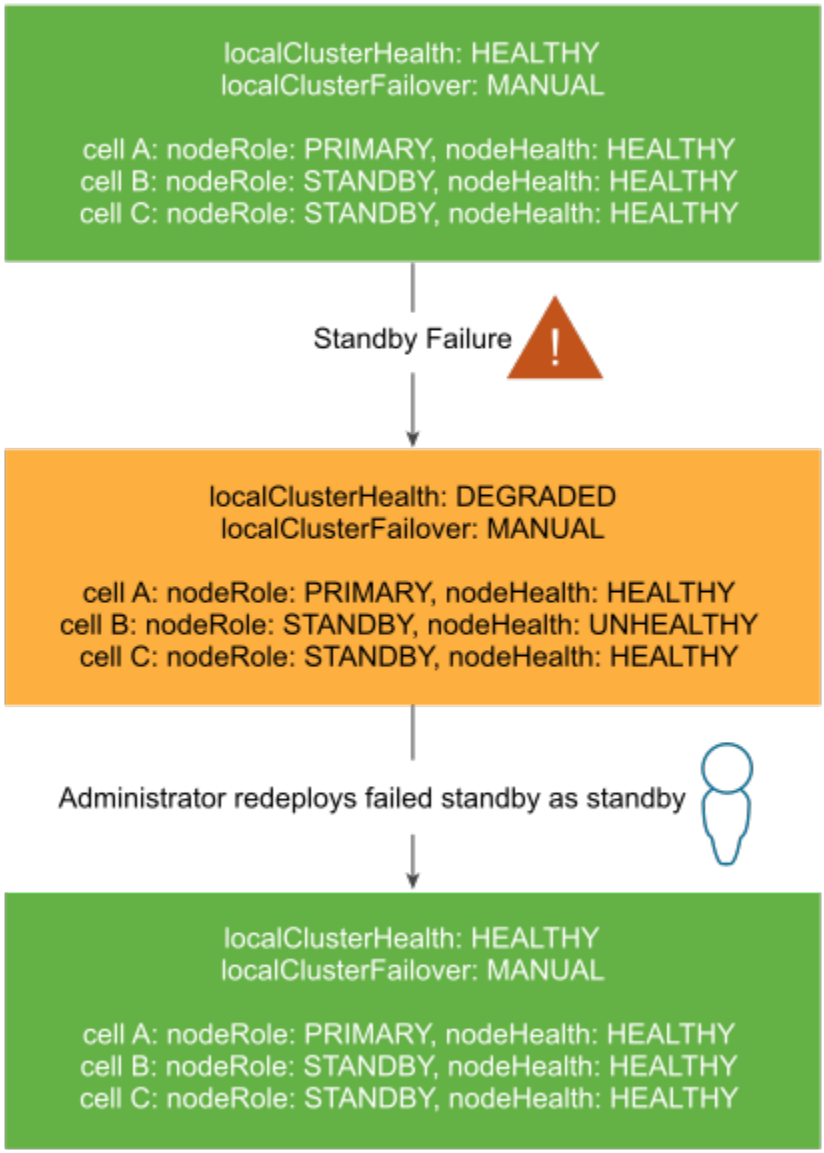
Option	Action
Exécutez une requête sur le nœud principal.	`select* from pg_stat_replication;`
Exécutez une requête sur un nœud en veille.	`select* from pg_stat_wal_receiver;`

Récupération de cluster de base de données de dispositif VMware Cloud Director

En cas de défaillance de la base de données ou de l'un des nœuds VMware Cloud Director, vous pouvez récupérer votre cluster de base de données.

Si une cellule du cluster haute disponibilité de la base de données échoue, l'état de santé du cluster indique la nature de l'échec et comment vous pouvez résoudre le problème. Par exemple, la santé du cluster `Degraded` indique un échec de cellule en veille. Un administrateur système doit redéployer la cellule ayant échoué.

Figure 3-4. Récupérer d'une panne de cellule en veille



Si une cellule principale du cluster haute disponibilité de la base de données échoue, la santé du cluster peut devenir `No_Active_Primary`, ce qui indique qu'un administrateur système doit réparer la cellule principale ayant échoué.

Récupérer après une panne de cellule principale dans un cluster haute disponibilité

Si la cellule principale ne fonctionne pas correctement, pour récupérer la base de données VMware Cloud Director, l'une des cellules en veille doit devenir la nouvelle cellule principale et vous devez déployer une nouvelle cellule en veille. En fonction du mode de panne, le dispositif VMware Cloud Director promeut automatiquement une cellule en veille comme nouvelle cellule principale ou vous devez la promouvoir manuellement.

En fonction du mode de basculement du dispositif VMware Cloud Director, il existe deux workflows différents pour la récupération à la suite d'une panne de cellule principale. Vous pouvez utiliser ces workflows pour réutiliser les adresses IP et le nom d'hôte de la cellule principale en échec lorsque vous déployez la nouvelle cellule en veille.

Workflow de récupération pour le mode de basculement manuel

Si la cellule principale se trouve dans l'état `Not reachable` ou `Failed`, et que les deux cellules en veille sont dans l'état `Running`, vous pouvez effectuer une récupération après la panne à l'aide de l'interface utilisateur dispositif HTML5 du dispositif et de l'API du dispositif VMware Cloud Director.

Pour afficher l'état des cellules dans le cluster, reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

1 À l'aide de l'outil de gestion des cellules, si possible, arrêtez le processus VMware Cloud Director. Depuis la cellule principale en échec, exécutez la commande suivante

```
/opt/vmware/vcloud-director/bin/cell-management-tool  -u <sysadmin user> cell --shutdown
```

2 Mettez hors tension la machine virtuelle principale en échec.

3 Promouvez une cellule en veille pour qu'elle devienne le nouveau nœud principal.

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

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

   L'interface utilisateur de gestion affiche deux cellules avec le rôle `principal`. L'instance principale d'origine a l'état `échec` et la nouvelle instance principale a l'état `en cours d'exécution`. La santé du cluster est `Dégradé`.

4 À partir de n'importe quelle cellule autre que le dispositif principal en échec, à l'aide de la méthode API `Unregister` du dispositif, supprimez le dispositif principal en échec du cluster haute disponibilité repmgr. Reportez-vous à la documentation de VMware Cloud Director Appliance API.

5 Supprimez le dispositif principal ayant échoué du groupe de serveurs VMware Cloud Director.

   a Connectez-vous en tant qu'**administrateur** au Service Provider Admin Portal.

   b Dans la barre de navigation supérieure, sous **Ressources**, sélectionnez **Ressources de Cloud**.

   c Dans le panneau de gauche, cliquez sur **Cellules cloud**.

   d Sélectionnez la cellule inactive et cliquez sur **Annuler l'enregistrement**.

6 Si vous souhaitez réutiliser l'adresse IP et le nom d'hôte du dispositif principal en échec, assurez-vous que le dispositif principal en échec reste hors tension ou utilisez vSphere Client pour le supprimer.

7 Déployez un nouveau dispositif en veille. Vous pouvez Démarrer le déploiement du dispositif VMware Cloud Director ou Déploiement du dispositif VMware Cloud Director avec VMware OVF Tool.

   Après le déploiement du nouveau dispositif en veille, la santé du cluster doit être `Sain`.

Récupération du mode de basculement automatique

Si le dispositif principal est dans l'état `Failed`, VMware Cloud Director promeut automatiquement une cellule en veille en tant que nouveau dispositif principal en cours d'exécution, mais le cluster est dans l'état `Dégradé`, car une seule cellule en veille est en cours d'exécution. Vous pouvez récupérer de l'échec à l'aide de l'interface utilisateur HTML5 et de VMware Cloud Director Appliance API.

Pour afficher l'état des cellules dans le cluster, reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

1 Si possible, à l'aide de l'outil de gestion des cellules, arrêtez le processus VMware Cloud Director. Depuis la cellule principale en échec, exécutez la commande suivante

```
/opt/vmware/vcloud-director/bin/cell-management-tool  -u <sysadmin user> cell --shutdown
```

2 Mettez hors tension la machine virtuelle principale en échec.

   L'interface utilisateur de gestion affiche deux cellules avec le rôle `principal`. L'instance principale d'origine a l'état `échec` et la nouvelle instance principale a l'état `en cours d'exécution`. La santé du cluster est `Dégradé`.

3 À partir de n'importe quelle cellule autre que le dispositif principal en échec, à l'aide de la méthode API `Unregister` du dispositif, supprimez le dispositif principal en échec du cluster haute disponibilité repmgr. Reportez-vous à la documentation de VMware Cloud Director Appliance API.

4 Supprimez le dispositif principal ayant échoué du groupe de serveurs VMware Cloud Director.

   a Connectez-vous en tant qu'**administrateur** au Service Provider Admin Portal.

   b Dans la barre de navigation supérieure, sous **Ressources**, sélectionnez **Ressources de Cloud**.

   c Dans le panneau de gauche, cliquez sur **Cellules cloud**.

   d Sélectionnez la cellule inactive et cliquez sur **Annuler l'enregistrement**.

5 Si vous souhaitez réutiliser l'adresse IP et le nom d'hôte du dispositif principal en échec, assurez-vous que le dispositif principal en échec est hors tension ou utilisez vSphere Client pour le supprimer.

6 Déployez un nouveau dispositif en veille. Vous pouvez Démarrer le déploiement du dispositif VMware Cloud Director ou Déploiement du dispositif VMware Cloud Director avec VMware OVF Tool. Après le déploiement du nouveau dispositif en veille, la santé du cluster doit être `Sain`.

7 À partir de n'importe quelle cellule autre que la cellule principale en échec, utilisez la méthode de l'API `Failover` du dispositif pour réinitialiser le mode de basculement du cluster sur `Automatic`. Reportez-vous à la documentation de VMware Cloud Director Appliance API.

Récupérer après une panne de cellule en veille dans un cluster haute disponibilité

Si une cellule en veille ne fonctionne pas correctement, vous pouvez récupérer après l'échec en déployant une nouvelle cellule en veille.

Si l'une des cellules en veille est dans l'état `Not reachable` ou `Failed`, vous pouvez déployer une nouvelle cellule. Pour afficher l'état des cellules dans le cluster, reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

Vous pouvez utiliser ce workflow pour réutiliser les adresses IP et le nom d'hôte du dispositif en veille en échec lorsque vous déployez un nouveau dispositif en veille.

1 Si possible, utilisez l'outil de gestion des cellules pour arrêter le processus VMware Cloud Director. Depuis la cellule en veille en échec, exécutez la commande suivante.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

2 Mettez hors tension la machine virtuelle en veille en échec.

3 Annulez l'enregistrement de la cellule en veille ayant échoué du cluster haute disponibilité repmgr. Reportez-vous à la section Annuler l'enregistrement d'un nœud en veille ayant échoué ou inaccessible dans un cluster haute disponibilité de base de données.

4 Utilisez le Service Provider Admin Portal pour supprimer le dispositif en veille ayant échoué du groupe de serveurs VMware Cloud Director.

   a Dans la barre de navigation supérieure, sous **Ressources**, sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Cellules cloud**.

   c Sélectionnez une cellule inactive et cliquez sur **Annuler l'enregistrement**.

5 Si vous souhaitez réutiliser l'adresse IP et le nom DNS de la cellule en veille en échec, vous devez vous assurer que le dispositif en veille en échec reste hors tension ou le supprimer.

6 Déployez un nouveau dispositif en veille. Vous pouvez Démarrer le déploiement du dispositif VMware Cloud Director ou Déploiement du dispositif VMware Cloud Director avec VMware OVF Tool.

   Après le déploiement du nouveau dispositif en veille, la santé du cluster doit être `Sain`.

7 Pour réinitialiser le mode de basculement du cluster sur `Automatic`, à partir de n'importe quelle cellule autre que la cellule en veille en échec, utilisez la méthode de l'API `Failover` du dispositif. Reportez-vous à la documentation de VMware Cloud Director Appliance API.

   Pour plus d'informations sur le mode de basculement automatique, consultez Basculement automatique du dispositif VMware Cloud Director.

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. Reportez-vous à Vérifier l'état de connectivité 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. Vous pouvez utiliser l'API du dispositif VMware Cloud Director pour noter l'ID de nœud du nœud principal du cluster. Reportez-vous à la section *Référence de schéma de l'API du dispositif VMware Cloud Director* sur http://code.vmware.com.

- 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. Pour plus d'informations sur l'état des cellules et le nom de la cellule que les cellules en veille suivent, reportez-vous à la section Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

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. (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.

Dépannage du dispositif

Si le déploiement du dispositif VMware Cloud 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 VMware Cloud Director. Pour plus d'informations sur la collecte d'informations de diagnostic pour VMware Cloud 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.

Examiner les fichiers journaux dans le dispositif VMware Cloud Director

Après avoir déployé le dispositif VMware Cloud 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 à l'aide d'un client SSH à la console du dispositif VMware Cloud 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 VMware Cloud Director ne parvient pas à démarrer après le déploiement du dispositif

Vous avez correctement déployé le dispositif VMware Cloud Director, mais les services VMware Cloud 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 VMware Cloud 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 VMware Cloud 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`.

Note Si votre cluster est configuré pour le basculement automatique, après avoir déployé une ou plusieurs cellules supplémentaires, vous devez utiliser Appliance API pour réinitialiser le mode de basculement sur `Automatic`. Reportez-vous à l'API du dispositif VMware Cloud Director. Le mode de basculement par défaut des nouvelles cellules est `Manual`. Si le mode de basculement est incohérent entre les nœuds du cluster, le mode de basculement du cluster est `Indeterminate`. Le mode `Indeterminate` peut créer des états de cluster incohérents entre les nœuds et les nœuds qui suivent une ancienne cellule principale. Pour afficher le mode de basculement du cluster, reportez-vous à Afficher la santé et le mode de basculement du cluster du dispositif VMware Cloud Director.

Solution

1. Connectez-vous directement ou à l'aide d'un client SSH à la console du dispositif VMware Cloud 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 VMware Cloud Director échoue lors de la migration ou de la restauration vers le dispositif VMware Cloud Director

Lorsque vous migrez ou restaurez vers un dispositif VMware Cloud Director, l'exécution de la commande `configure` peut échouer.

Problème

Pendant la procédure de migration ou de restauration de VMware Cloud Director vers un nouvel environnement de dispositif VMware Cloud Director, vous exécutez la commande `configure` pour reconfigurer le service VMware Cloud 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 VMware Cloud Director

Vous pouvez examiner les fichiers journaux pour rechercher des erreurs et des avertissements lorsque vous appliquez des correctifs au dispositif VMware Cloud 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 VMware Cloud 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 VMware Cloud Director

Lorsque vous vérifiez la présence de mises à jour au dispositif VMware Cloud Director, l'exécution de la commande `vamicli update --check` peut échouer.

Problème

Pendant la procédure d'application d'un correctif au dispositif VMware Cloud 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 VMware Cloud Director

Lorsque vous installez les dernières mises à jour au dispositif VMware Cloud Director, l'exécution de la commande `vamicli update --install latest` peut échouer.

Problème

Pendant la procédure d'application d'un correctif au dispositif VMware Cloud 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
```

Vérifier l'état des services VMware Cloud Director

Vous pouvez utiliser l'interface utilisateur de gestion du dispositif VMware Cloud Director pour afficher l'état des services VMware Cloud Director pour la cellule dans laquelle vous êtes connecté.

Procédure

1 Connectez-vous en tant qu'utilisateur **racine** à l'interface utilisateur de gestion de dispositif à l'adresse `https://primary_eth1_ip_address:5480`.

2 Pour afficher l'état des services, dans le panneau de gauche, sélectionnez **Services**.

Si le dispositif VMware Cloud Director fonctionne correctement, les services `vmware-vcd` et `vpostgres` sont en cours d'exécution.

Étape suivante

Si vous devez vérifier l'état du service `repmgrd` à des fins de débogage, vous devez utiliser l'API du dispositif VMware Cloud Director.

Installation, mise à niveau et administration de VMware Cloud Director sous Linux

4

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

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

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

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

Ce chapitre contient les rubriques suivantes :

Planification de la configuration

vSphere fournit des capacités de stockage, de calcul et de mise en réseau à VMware Cloud Director. Avant de commencer l'installation, évaluez la capacité vSphere et VMware Cloud 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 VMware Cloud Director à chaque système vCenter Server devant être accessible dans votre Cloud.
- Assurez-vous que tous les serveurs Linux VMware Cloud Director cibles sont conformes à la configuration minimale requise en termes de mémoire et de stockage détaillée dans *Notes de mise à jour de VMware Cloud Director*.
- Si vous prévoyez d'installer VMware Cloud Director sur Linux, configurez la base de données VMware Cloud Director comme décrit dans Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.

Préparation de l'installation de VMware Cloud Director

Avant d'installer VMware Cloud Director sur un serveur Linux, vous devez préparer votre environnement.

Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux

Les cellules de VMware Cloud Director utilisent une base de données pour stocker les informations partagées. Avant d'installer VMware Cloud Director sur Linux, vous devez installer et configurer une instance de base de données PostgreSQL, et créer le compte d'utilisateur de base de données VMware Cloud Director.

Les bases de données PostgreSQL doivent répondre à des exigences de configuration spécifiques pour les utiliser avec VMware Cloud Director.

Vous devez créer un schéma de base de données dédié distinct que VMware Cloud Director pourra utiliser. VMware Cloud Director ne peut pas partager un schéma de la base de données avec un autre produit VMware.

VMware Cloud Director prend en charge les connexions SSL à la 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 VMware Cloud Director. Reportez-vous à Référence de configuration sans surveillance et Effectuer des configurations supplémentaires sur la base de données PostgreSQL externe.

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

Conditions préalables

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

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 VMware Cloud 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 VMware Cloud Director, vous pouvez configurer la base de données PostgreSQL pour exiger des connexions SSL à partir des cellules VMware Cloud 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.

Préparation du stockage du serveur de transfert pour VMware Cloud Director sur Linux

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 VMware Cloud Director.

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.

Exigences pour la configuration du serveur NFS

Il existe des exigences spécifiques pour la configuration du serveur NFS, afin que VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 la ligne suivante 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 VMware Cloud 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 VMware Cloud Director vers une version ultérieure

Lors de la mise à niveau d'un groupe de serveurs VMware Cloud Director, vous exécutez le fichier d'installation de la version mise à niveau pour mettre à niveau tous les membres du groupe de serveurs VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director

Si vous planifiez l'installation de VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Important Cette procédure ne s'applique que dans le cas d'une nouvelle installation de VMware Cloud Director. Si vous mettez à niveau une installation de VMware Cloud Director existante, consultez Mise à niveau de VMware Cloud Director sous Linux.

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 VMware Cloud Director dans votre installation de VMware Cloud Director.

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

   VMware Cloud 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 VMware Cloud Director

Si vous planifiez l'installation de VMware Cloud Director pour utiliser les ressources réseau de NSX-T Data Center, vous devez installer et configurer NSX-T Data Center.

Important Pour configurer les objets et les outils NSX-T Data Center, utilisez l'interface utilisateur de stratégie simplifiée et les API de stratégie qui correspondent à l'interface utilisateur simplifiée. Pour plus d'informations, consultez la présentation de NSX-T Manager à la section *Guide d'administration de NSX-T Data Center* .

Pour obtenir les informations les plus récentes sur la compatibilité entre VMware Cloud Director et d'autres produits VMware, reportez-vous aux Matrices d'interopérabilité des produits VMware.

Pour plus d'informations sur les conditions requises en matière de réseau, consultez Configuration réseau requise pour VMware Cloud Director.

Cette procédure ne s'applique que dans le cas d'une nouvelle installation de VMware Cloud Director. Si vous mettez à niveau une installation de VMware Cloud Director existante, consultez Mise à niveau de VMware Cloud Director sous Linux.

Conditions préalables

Familiarisez-vous avec NSX-T Data Center.

Procédure

1. Déployez et configurez les dispositifs virtuels NSX-T Manager.

   Pour plus d'informations sur le déploiement de NSX-T Manager, consultez la section *Guide d'installation de NSX-T Data Center* .

2. Créez des zones de transport en fonction de vos exigences de mise en réseau.

   Pour plus d'informations sur la création de zones de transport, consultez la section *Guide d'installation de NSX-T Data Center* .

   Note

3. Déployez et configurez des nœuds Edge et un cluster Edge.

   Pour plus d'informations sur la création de NSX Edge, consultez la section *Guide d'installation de NSX-T Data Center* .

4. Configurez les nœuds de transport de l'hôte ESXi.

   Pour plus d'informations sur la configuration du nœud de transport d'un hôte géré, consultez la section *Guide d'installation de NSX-T Data Center* .

5. Créez une passerelle de niveau 0.

   Pour plus d'informations sur la création de passerelles de niveau 0, consultez la section *Guide d'administration de NSX-T Data Center* .

Étape suivante

Après l'installation de VMware Cloud Director, vous pouvez :

1 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 la section *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

2 Créer un pool de réseaux reposant sur une zone de transport NSX-T Data Center.

   Pour plus d'informations sur la création d'un pool de réseaux dépendant d'une zone de transport NSX-T Data Center, reportez-vous à la section *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

3 Importer la passerelle de niveau 0 en tant que réseau externe.

   Pour plus d'informations sur l'ajout d'un réseau externe dépendant d'un routeur logique de niveau 0 NSX-T Data Center, reportez-vous à la section *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

Installer VMware Cloud Director sous Linux

Vous pouvez créer un groupe de serveurs VMware Cloud Director en installant le logiciel VMware Cloud 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 VMware Cloud Director existante, consultez Mise à niveau de VMware Cloud Director sous Linux.

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

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Conditions préalables

- Vérifiez que les serveurs cible pour votre groupe de serveurs respectent les Chapitre 2 Configuration matérielle et logicielle requise pour installer VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. Reportez-vous à Préparation du stockage du serveur de transfert pour VMware Cloud Director sur Linux.
- Vérifiez que vous avez créé une base de données VMware Cloud Director et que tous les serveurs du groupe peuvent y accéder. Reportez-vous à la section Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux. Vérifiez que le service de base de données démarre lorsque vous redémarrez le serveur de base de données.
- Vérifiez que tous les serveurs VMware Cloud 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 VMware Cloud Director.
- Vérifiez que tous les serveurs VMware Cloud 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 VMware Cloud Director.
- Si vous envisagez d'importer des utilisateurs ou des groupes depuis un service LDAP, vérifiez que chaque serveur VMware Cloud 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 VMware Cloud Director et les systèmes vCenter Server.

Procédure

1 Installez VMware Cloud 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 VMware Cloud Director en exécutant le programme d'installation VMware Cloud Director sur le premier serveur Linux cible.

2 Création et gestion de certificats SSL pour VMware Cloud Director sous Linux

VMware Cloud Director utilise SSL pour sécuriser les communications entre les clients et les serveurs. Chaque serveur VMware Cloud 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.

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

Après avoir installé VMware Cloud 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.

4 Installez VMware Cloud Director sur un membre supplémentaire d'un groupe de serveurs

   Vous pouvez ajouter des serveurs à un groupe de serveurs VMware Cloud 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.

Étape suivante

Utilisez la commande system-setup de l'outil de gestion de cellules pour initialiser la base de données d'un groupe de serveurs avec un compte d'administrateur système et les informations associées. Reportez-vous à la section Configurer une installation de VMware Cloud Director .

Installez VMware Cloud 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 VMware Cloud Director en exécutant le programme d'installation VMware Cloud Director sur le premier serveur Linux cible.

VMware Cloud 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 VMware Cloud Director.

Le programme d'installation de VMware Cloud Director vérifie que le serveur cible répond à toutes les conditions requises de la plate-forme et installe le logiciel VMware Cloud 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 **execute**. 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 VMware Cloud 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 VMware Cloud 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.

Création et gestion de certificats SSL pour VMware Cloud Director sous Linux

VMware Cloud Director utilise SSL pour sécuriser les communications entre les clients et les serveurs. Chaque serveur VMware Cloud 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.

Avant de créer des certificats SSL pour VMware Cloud Director sur Linux

Lorsque vous installez VMware Cloud 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 VMware Cloud Director sous Linux. Le dispositif VMware Cloud Director crée des certificats SSL auto-signés lors de son premier démarrage.

Procédure

1 Connectez-vous au serveur VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director sous Linux.

Créer des certificats SSL auto-signés pour VMware Cloud Director sous Linux

Les certificats auto-signés constituent un moyen pratique de configurer SSL pour VMware Cloud Director dans des environnements où les considérations de confiance ne sont pas primordiales.

Chaque serveur VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director nécessite deux certificats SSL pour sécuriser les communications entre les clients et les serveurs. Chaque serveur VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Remplacement des certificats pour les points de terminaison HTTPS et de proxy de console.

Procédure

1. Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation du serveur VMware Cloud 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 VMware Cloud 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 VMware Cloud Director du groupe de serveurs.

Étape suivante

- Si vous n'avez pas encore configuré votre instance de VMware Cloud Director, exécutez le script `configure` pour importer le keystore des certificats dans VMware Cloud 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 VMware Cloud 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 HTTPS et de proxy de console.

Créer un keystore de certificats SSL signé par une autorité de certification avec des clés privées importées pour VMware Cloud 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 VMware Cloud Director.

Conditions préalables

- Reportez-vous à la section Avant de créer des certificats SSL pour VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Remplacement des certificats pour les points de terminaison HTTPS 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 VMware Cloud Director dans votre environnement.

Étape suivante

- Si vous n'avez pas encore configuré votre instance de VMware Cloud Director, exécutez le script `configure` pour importer le keystore des certificats dans VMware Cloud 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 VMware Cloud 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 HTTPS et de proxy de console.

Configuration des connexions au réseau et à la base de données

Après avoir installé VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 HTTPS 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 Chapitre 5 Référence de l'outil de gestion des cellules.

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 VMware Cloud Director est installé. Cette valeur est généralement `/opt/vmware/vcloud-director`.

Procédure

1. Connectez-vous au serveur VMware Cloud 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 une URL qui vous permet de vous connecter à l'assistant **Configuration de VMware Cloud Director** après le démarrage du service VMware Cloud Director.

c Il propose de démarrer la cellule VMware Cloud Director.

3 (Facultatif) Notez l'URL de l'assistant **Configuration de VMware Cloud Director** et entrez **`y`** pour démarrer le service VMware Cloud 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 4-1. Informations requises lors de la configuration d'un réseau interactif et d'une base de données

Informations requises	Description
Adresse IP pour le service HTTPS	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 HTTPS et le service de proxy de la console, vous devez exécuter le script de configuration en mode sans surveillance.

Tableau 4-1. Informations requises lors de la configuration d'un réseau interactif et d'une base de données (suite)

Informations requises	Description
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 VMware Cloud Director sur Linux.
Mot de passe de clé privée pour le certificat SSL HTTPS	Reportez-vous à Avant de créer des certificats SSL pour VMware Cloud 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 VMware Cloud Director sur Linux.
Activer la journalisation d'audit à distance à un hôte syslog	Les services de chaque cellule VMware Cloud Director consignent des messages d'audit dans la base de données VMware Cloud Director qui sont conservés pendant 90 jours. Pour conserver les messages d'audit au-delà de cette période, vous pouvez configurer les services VMware Cloud Director pour qu'ils envoient les messages d'audit à l'utilitaire `syslog` en plus de la base de données VMware Cloud 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.
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	La valeur est définie par défaut sur 5432.
Nom de la base de données	La valeur est définie par défaut sur vcloud.
Nom d'utilisateur de la base de données	Reportez-vous à Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.

Tableau 4-1. Informations requises lors de la configuration d'un réseau interactif et d'une base de données (suite)

Informations requises	Description
Mot de passe de la base de données	Reportez-vous à Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.
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 Chapitre 5 Référence de l'outil de gestion des cellules. 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 4-2. 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 VMware Cloud 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 VMware Cloud Director.

Tableau 4-2. Options et arguments de l'utilitaire de configuration (suite)

Option	Argument	Description
`--database-ssl`	`true` ou `false`	Vous pouvez configurer la base de données PostgreSQL pour exiger une connexion SSL correctement signée depuis VMware Cloud Director. 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 VMware Cloud Director l'hôte de la base de données	Reportez-vous à la section Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.
`--database-name` (`-dbname`)	Nom de service de la base de données	Reportez-vous à la section Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.
`--database-password` (`-dbpassword`)	Mot de passe de l'utilisateur de la base de données. Il peut être nul.	Reportez-vous à la section Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.
`--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 la section Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.
`--database-type` (`-dbtype`)	Type de base de données. Le type pris en charge est `postgres`.	Facultatif. Le type de base de données sera défini sur `postgres` par défaut. Reportez-vous à la section Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.
`--database-user` (`-dbuser`)	Nom d'utilisateur de l'utilisateur de la base de données.	Reportez-vous à la section Configurer une base de données PostgreSQL externe pour VMware Cloud Director sous Linux.

Tableau 4-2. Options et arguments de l'utilitaire de configuration (suite)

Option	Argument	Description
`--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 Chapitre 5 Référence de l'outil de gestion des cellules.
`--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 VMware Cloud Director. Par exemple, *10.17.118.159*.
`--primary-port-http`	Entier dans la plage comprise entre 0 et 65535	Numéro de port à utiliser pour les connexions HTTP (non sécurisées) auVMware Cloud 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 VMware Cloud 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` .

Tableau 4-2. Options et arguments de l'utilitaire de configuration (suite)

Option	Argument	Description
`--syslog-host` (`-loghost`)	Adresse IP ou nom de domaine complet de l'hôte du serveur syslog	Les services de chaque cellule VMware Cloud Director consignent des messages d'audit dans la base de données VMware Cloud Director qui sont conservés pendant 90 jours. Pour conserver les messages d'audit au-delà de cette période, vous pouvez configurer les services VMware Cloud Director pour qu'ils envoient les messages d'audit à l'utilitaire `syslog` en plus de la base de données VMware Cloud 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.
`--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 VMware Cloud Director avec deux adresses IP différentes pour le service HTTPS 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 postgres -dbhost 10.150.10.78 -dbname postgresql-db-name -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 VMware Cloud Director avec une adresse IP unique à deux ports distincts pour le service HTTPS 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 postgres -dbhost 10.150.10.78 -dbname postgresql-db-
name \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

Protection et réutilisation du fichier de réponses

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

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

Important L'outil de gestion de cellules inclut des sous-commandes que vous pouvez utiliser pour apporter des modifications aux détails de connexion au réseau et à la base de données que vous avez spécifiés lors de la configuration de la première cellule VMware Cloud Director. 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. Reportez-vous à la section « Référence de l'outil de gestion de cellules » dans le *Guide de l'administrateur de VMware Cloud Director*.

Procédure

1 Protégez le fichier de réponses.

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

2 Réutilisez le fichier de réponses.

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

Note Vous devez installer le logiciel VMware Cloud 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 VMware Cloud Director sur un membre supplémentaire d'un groupe de serveurs

Vous pouvez ajouter des serveurs à un groupe de serveurs VMware Cloud 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 VMware Cloud Director sur Linux et les déploiements de dispositifs VMware Cloud 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 VMware Cloud 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 **execute**. 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 un utilisateur racine.

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 VMware Cloud Director.

9 (Facultatif) Entrez **y** pour démarrer le service VMware Cloud 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 VMware Cloud Director s'exécutent sur tous les serveurs, vous devez initialiser la base de données VMware Cloud Director avec une clé de licence, un compte d'administrateur système et les informations associées. Vous pouvez initialiser la base de données à l'aide de l'outil de gestion des cellules avec la sous-commande `system-setup`. Reportez-vous au Configurer une installation de VMware Cloud Director .

Après l'installation de VMware Cloud Director

Après avoir créé le groupe de serveurs VMware Cloud 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.

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Personnaliser les adresses publiques pour VMware Cloud Director sous Linux

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 le portail Web de VMware Cloud Director, l'API VMware Cloud Director et le proxy de console.

Conditions préalables

Vérifiez que vous êtes connecté en tant qu'**administrateur système**. Seul un **administrateur système** peut personnaliser les points de terminaison publics.

Procédure

1. Dans la barre de navigation supérieure du Service Provider Admin Portal, sélectionnez **Administration**.
2. Dans le volet de gauche, sous **Paramètres**, cliquez sur **Adresses publiques**.
3. Pour personnaliser les points de terminaison publics, cliquez sur **Modifier**.

4 Pour personnaliser les URL VMware Cloud Director, modifiez les points de terminaison du **portail Web**.

   a Entrez une URL publique VMware Cloud Director personnalisée pour les connexions HTTP (non sécurisées).

   b Entrez une URL publique VMware Cloud Director personnalisée pour les connexions HTTPS (sécurisées) et cliquez sur **Télécharger** pour télécharger les certificats qui établissent la chaîne d'approbation pour ce point de terminaison.

      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 cellule VMware Cloud Director avec l'alias `consoleproxy`. Les terminaisons SSL des connexions de proxy de console sur un équilibrage de charge ne sont pas prises en charge. 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 (Facultatif) Pour personnaliser les URL REST API et OpenAPI de Cloud Director, désactivez le bouton bascule **Utiliser les paramètres de portail Web**.

   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 VMware Cloud Director à l'adresse `http://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI VMware Cloud Director à l'adresse `http://vcloud.example.com/cloudapi`.

   b Entrez une URL de base HTTPS personnalisée pour l'API REST et cliquez sur **Télécharger** 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 REST API sur **`https://vcloud.example.com`**, vous pouvez accéder à l'API VMware Cloud Director à l'adresse `https://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI VMware Cloud Director 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 VMware Cloud 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.

6 Entrez une adresse proxy de console publique VMware Cloud Director personnalisée.

   Cette adresse est le nom de domaine complet (FQDN) du serveur VMware Cloud Director ou de l'équilibrage de charge avec le numéro de port. Le port par défaut est 443.

Important Le dispositif VMware Cloud Director utilise sa carte réseau `eth0` avec le port personnalisé 8443 pour le service de proxy de console.

Par exemple, pour une instance de dispositif VMware Cloud Director ayant le nom de domaine complet `vcloud.example.com`, entrez **`vcloud.example.com:8443`**.

VMware Cloud Director utilise l'adresse proxy de la console lors de l'ouverture d'une fenêtre de console distante sur une machine virtuelle.

7 Pour enregistrer les modifications, cliquez sur **Enregistrer**.

Installer et configurer une base de données Cassandra pour stocker les données de mesure historiques

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. La récupération des mesures historiques ne nécessite pas l'utilisation du logiciel de base de données facultatif.

Conditions préalables

- Vérifiez que VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Chapitre 5 Référence de l'outil de gestion des cellules.

2. (Facultatif) Si vous mettez à niveau VMware Cloud 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 VMware Cloud Director.

Effectuer des configurations supplémentaires sur la base de données PostgreSQL externe

Après avoir créé le groupe de serveurs VMware Cloud Director, vous pouvez configurer la base de données PostgreSQL externe pour exiger des connexions SSL à partir des cellules VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, exécutez la commande d'importation du certificat de la base de données dans le truststore VMware Cloud 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 VMware Cloud 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 Chapitre 5 Référence de l'outil de gestion des cellules.

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 VMware Cloud 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.

Installer et configurer un broker AMQP RabbitMQ

Si vous souhaitez utiliser des tâches bloquantes, des notifications ou des extensions d'API VMware Cloud Director, comme Container Service Extension (CSE), VMware Cloud Director App Launchpad ou vRealize Operations Tenant App, vous devez 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. VMware Cloud 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.

Pour VMware Cloud Director sur les installations Linux, l'utilisation d'un client MQTT peut être une alternative au broker AMQP RabbitMQ lors de la configuration de notifications. Reportez-vous à la section S'abonner à des événements et à des tâches à l'aide d'un client MQTT.

Procédure

1. Téléchargez le serveur RabbitMQ depuis https://www.rabbitmq.com/download.html.

   Reportez-vous à la section *Notes de mise à jour de VMware Cloud 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 VMware Cloud 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 VMware Cloud 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. La valeur par défaut est `5672` pour une connexion non-SSL. Le port par défaut pour SSL/TLS est `5671`.
   - Le protocole de communication est TCP.
   - L'hôte virtuel RabbitMQ. Par défaut « `/` ».

Étape suivante

Par défaut, le service AMQP de VMware Cloud 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 VMware Cloud Director, généralement situé à `$VCLOUD_HOME/jre/lib/security/cacerts`.

Pour activer SSL avec le service AMQP de VMware Cloud Director, reportez-vous à la section Configurer un broker AMQP dans le *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*.

S'abonner à des événements et à des tâches à l'aide d'un client MQTT

Vous pouvez utiliser un client MQTT pour vous abonner à des messages concernant des événements et des tâches VMware Cloud Director.

MQTT est un protocole de transport de messagerie léger et binaire. VMware Cloud Director utilise MQTT pour publier des informations sur les événements et les tâches auxquels vous pouvez vous abonner à l'aide d'un client MQTT. Les messages MQTT transitent par un Broker MQTT qui peut également stocker des messages si les clients ne sont pas en ligne.

Conditions préalables

- Vérifiez que vous disposez d'un client MQTT qui prend en charge WebSocket.
- Vérifiez que vous pouvez ajouter des en-têtes à une demande mise à niveau par WebSocket.

Procédure

1. Connectez-vous à VMware Cloud Director à l'aide du point de terminaison OpenAPI.
2. Pour établir une connexion WebSocket, définissez la propriété Sec-WebSocket-Protocol sur `mqtt`, configurez le client pour qu'il se connecte au chemin d'accès `/messaging/mqtt`, ajoutez un en-tête d'autorisation et suivez le flux de connexion MQTT standard.

   Vous recevez le jeton JWT de la demande de connexion standard à VMware Cloud Director. Vous pouvez laisser le nom d'utilisateur et le mot de passe vides.

   ```
   Sec-WebSocket-Protocol: mqtt
   ```

   ```
   Authorization: Bearer {JWT_token}
   ```

3. Une fois que la connexion a été établie, abonnez-vous aux rubriques via le client MQTT.

   ```
   publish/{user_org_id}/{user_id}
   ```

   ```
   publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
   ```

Les **administrateurs d'organisation** peuvent utiliser des caractères génériques pour accéder à toutes les rubriques de l'organisation.

```
publish/{user_org_id}/*
```

Les **administrateurs système** peuvent utiliser des caractères génériques pour accéder à toutes les rubriques.

```
publish/*/*
```

Mise à niveau de VMware Cloud Director sous Linux

Pour mettre à niveau VMware Cloud Director vers une nouvelle version, arrêtez les services VMware Cloud Director sur toutes les cellules du groupe de serveurs, installez la nouvelle version sur chaque serveur, mettez à niveau la base de données VMware Cloud Director et redémarrez les cellules VMware Cloud Director.

Si votre groupe de serveurs VMware Cloud Director existant comprend des installations de VMware Cloud Director sur Linux, vous pouvez utiliser le programme d'installation de VMware Cloud Director pour Linux pour mettre à niveau votre environnement.

Pour les installations de VMware Cloud Director sur Linux, vous pouvez effectuer une mise à niveau orchestrée ou procéder à une mise à niveau manuelle de VMware Cloud Director. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud 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 VMware Cloud Director 9.5 :

- Les bases de données Oracle ne sont plus prises en charge. Si votre installation existante de VMware Cloud Director utilise une base de données Oracle, reportez-vous au tableau Chemins et workflows de mise à niveau.
- 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. Vous pouvez placer les hôtes ESXi en mode de maintenance à l'aide de vSphere Client.
- VMware Cloud 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.

À partir de VMware Cloud Director 10.0, les bases de données Microsoft SQL Server ne sont pas prises en charge.

Lorsque vous mettez à niveau VMware Cloud 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 VMware Cloud Director. Pour plus d'informations, reportez-vous au tableau Chemins de mise à niveau et de migration.
- La version de VMware vSphere ® que vous utilisez actuellement.
- La version de VMware NSX® que vous utilisez actuellement.
- Tous les composants tiers qui interagissent directement avec VMware Cloud Director.

Pour plus d'informations sur la compatibilité de VMware Cloud 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 VMware Cloud Director, vous devez les mettre à niveau après la mise à niveau de VMware Cloud Director. Reportez-vous à Après la mise à niveau de VMware Cloud Director.

Après la mise à niveau d'au moins un serveur VMware Cloud Director, vous pouvez mettre à niveau la base de données VMware Cloud Director. La base de données détient des informations relatives à l'état d'exécution du serveur, notamment l'état de toutes les tâches VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.`

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux

locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Important Après la mise à niveau vers la version 10.1, VMware Cloud Director vérifie toujours les certificats pour tous les points de terminaison d'infrastructure qui y sont connectés. Cela est dû à une modification de la manière dont VMware Cloud Director gère les certificats SSL. Si vous n'importez pas vos certificats dans VMware Cloud Director avant la mise à niveau, les connexions vCenter Server et NSX peuvent afficher des erreurs de connexion infructueuses en raison de problèmes de vérification SSL. Dans ce cas, après la mise à niveau, vous avez deux options :

1. Exécutez la commande `trust-infra-certs` de l'outil de gestion des cellules pour importer automatiquement tous les certificats dans le magasin de certificats centralisé. Reportez-vous à la section Importer des certificats de point de terminaison depuis les ressources vSphere.
2. Dans l'interface utilisateur de Service Provider Admin Portal, sélectionnez chaque instance de vCenter Server et NSX, puis entrez à nouveau les informations d'identification tout en acceptant le certificat.

Chemins et workflows de mise à niveau

	Environnement cible
Environnement source	**VMware Cloud Director 10.1 sur Linux incluant une base de données PostgreSQL externe**
VMware Cloud Director 9.0 et 9.1 incluant une base de données Oracle externe	1 Pour VMware Cloud Director 9.0 sur Linux, mettez à niveau VMware Cloud Director vers la version 9.1. Reportez-vous à la section Mise à niveau de vCloud Director. 2 Migrez la base de données Oracle vers une base de données PostgreSQL. Reportez-vous à la section Migrer vers une base de données PostgreSQL. 3 Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director.
Dispositif VMware Cloud Director 9.5 incluant une base de données PostgreSQL externe	Non pris en charge
VMware Cloud Director 9.0, 9.1 et 9.5 sur Linux incluant une base de données PostgreSQL externe	Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director.

Environnement source	Environnement cible VMware Cloud Director 10.1 sur Linux incluant une base de données PostgreSQL externe
VMware Cloud Director 9.0, 9.1 et 9.5 sur Linux incluant une base de données Microsoft SQL Server externe	1 Mettez à niveau votre environnement vers VMware Cloud Director 9.7 sur Linux. Reportez-vous à la section Mise à niveau de vCloud Director. 2 Migrez la base de données Microsoft SQL Server vers une base de données PostgreSQL. Reportez-vous à la section Migrer vers une base de données PostgreSQL. 3 Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director.
VMware Cloud Director 9.7 sur Linux incluant une base de données Microsoft SQL Server externe	1 Migrez la base de données Microsoft SQL Server vers une base de données PostgreSQL. Reportez-vous à la section Migrer vers une base de données PostgreSQL. 2 Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director.
VMware Cloud Director 9.7 et 10.0 sous Linux avec une base de données PostgreSQL externe	Mettez à niveau votre environnement vers VMware Cloud Director 10.1 sur Linux. Reportez-vous à la section Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director ou Mettre à niveau manuellement une Installation VMware Cloud Director.
Dispositif VMware Cloud Director 9.7 et 10.0 incluant une base de données PostgreSQL intégrée	Non pris en charge

Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud 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 VMware Cloud Director avec l'option `--private-key-path`.

Vous pouvez utiliser le programme d'installation de VMware Cloud Director pour Linux pour mettre à niveau un groupe de serveurs VMware Cloud Director composé des installations de VMware Cloud Director sur un système d'exploitation Linux pris en charge. Si votre groupe de serveurs VMware Cloud Director se compose des déploiements de dispositifs VMware Cloud Director 9.5, vous utilisez le programme d'installation de VMware Cloud Director pour Linux pour mettre à niveau votre environnement existant uniquement dans le cadre du workflow de migration. Reportez-vous à la section Mise à niveau et migration du dispositif VMware Cloud Director.

VMware Cloud 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 VMware Cloud Director.

Lorsque vous exécutez le programme d'installation VMware Cloud 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 VMware Cloud Director, les composants vSphere et les composants NSX sont compatibles avec la nouvelle version de VMware Cloud Director.

  Important Si votre installation VMware Cloud Director existante utilise une base de données Oracle ou une base de données Microsoft SQL Server, vérifiez que vous avez migré vers une base de données PostgreSQL avant la mise à niveau. Pour connaître les chemins de mise à niveau possibles, reportez-vous à la section Mise à niveau de VMware Cloud Director sous Linux.

- 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 VMware Cloud 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 VMware Cloud Director pour servir d'identité sous laquelle les processus de VMware Cloud Director s'exécutent. L'utilisateur de `vcloud` n'a aucun mot de passe.

- Vérifiez que tous les hôtes ESXi sont activés. À partir de VMware Cloud 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 pour VMware Cloud Director sur Linux.
- Si votre installation de VMware Cloud 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 **execute**. 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 VMware Cloud 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 VMware Cloud Director et vous invite à confirmer la mise à niveau.

Si le programme d'installation détecte une version de VMware Cloud 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 VMware Cloud Director.

3 Il met à jour le logiciel VMware Cloud Director sur la cellule actuelle.

4 Il met à niveau la base de données VMware Cloud Director.

5 Il met à niveau le logiciel VMware Cloud Director sur chacune des cellules restantes, puis redémarre les services VMware Cloud Director sur la cellule.

6 Redémarre les services VMware Cloud Director sur la cellule actuelle.

Étape suivante

Démarrez les services VMware Cloud 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 VMware Cloud Director

Vous pouvez mettre à niveau une seule cellule en exécutant le programme d'installation VMware Cloud 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 VMware Cloud Director pour Linux pour mettre à niveau un groupe de serveurs VMware Cloud Director composé des installations de VMware Cloud Director sur un système d'exploitation Linux pris en charge. Si votre groupe de serveurs VMware Cloud Director se compose des déploiements de dispositifs VMware Cloud Director 9.5, vous utilisez le programme d'installation de VMware Cloud Director pour Linux pour mettre à niveau votre environnement existant uniquement dans le cadre du workflow de migration. Reportez-vous à la section Mise à niveau et migration du dispositif VMware Cloud Director.

Pour une installation VMware Cloud Director à plusieurs cellules, au lieu mettre à niveau manuellement chaque cellule et la base de données en séquence, vous pouvez effectuer une mise à niveau orchestrée de l'installation VMware Cloud Director. Reportez-vous à Effectuer une mise à niveau orchestrée d'une Installation VMware Cloud Director.

Conditions préalables

- Vérifiez que votre base de données VMware Cloud Director, les composants vSphere et les composants NSX sont compatibles avec la nouvelle version de VMware Cloud Director.

  Important Si votre installation VMware Cloud Director existante utilise une base de données Oracle ou une base de données Microsoft SQL Server, vérifiez que vous avez migré vers une base de données PostgreSQL avant la mise à niveau. Pour connaître les chemins de mise à niveau possibles, reportez-vous à la section Mise à niveau de VMware Cloud Director sous Linux.

- Vérifiez que vous disposez des informations d'identification de super utilisateur pour les serveurs dans le groupe de serveurs VMware Cloud 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 VMware Cloud Director vers laquelle vous effectuez la mise à niveau.

- Vérifiez que tous les hôtes ESXi sont activés. À partir de VMware Cloud Director 9.5, les hôtes ESXi désactivés ne sont pas pris en charge.

Procédure

1 Mise à niveau d'une cellule VMware Cloud Director

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

2 Mise à niveau de la base de données VMware Cloud Director

   À partir d'un serveur VMware Cloud Director mis à niveau, vous exécutez un outil qui met à niveau la base de données VMware Cloud Director. Vous ne devez pas redémarrer n'importe quel serveur VMware Cloud 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 VMware Cloud Director dans le groupe de serveurs et la base de données, vous pouvez démarrer les services VMware Cloud Director sur toutes les cellules.
- Mettre à niveau chaque instance de NSX Manager associée à un système vCenter Server relié
- Après la mise à niveau de chaque instance de NSX Manager, vous pouvez mettre à niveau les systèmes vCenter Server, les hôtes et les dispositifs Edge NSX. Reportez-vous à Mettre à niveau les systèmes vCenter Server, les hôtes ESXi et les dispositifs NSX Edge .

Mise à niveau d'une cellule VMware Cloud Director

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

VMware Cloud 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 VMware Cloud Director.

Pour une installation VMware Cloud Director à plusieurs cellule, vous devez exécuter le programme d'installation VMware Cloud Director sur chaque membre du groupe de serveurs VMware Cloud 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 **execute**. 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

c Une fois que tous les travaux VMware Cloud Director actifs sur la cellule sont terminés, arrêtez les services VMware Cloud Director sur le serveur et met à niveau le logiciel VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Répétez cette procédure sur chaque cellule VMware Cloud Director du groupe de serveurs.

Important Ne démarrez pas les services VMware Cloud 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 VMware Cloud Director

À partir d'un serveur VMware Cloud Director mis à niveau, vous exécutez un outil qui met à niveau la base de données VMware Cloud Director. Vous ne devez pas redémarrer n'importe quel serveur VMware Cloud 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 VMware Cloud 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 VMware Cloud 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. Une fois la base de données mise à niveau, les cellules VMware Cloud 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 pour 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 VMware Cloud Director du groupe de serveurs sont arrêtées. Les cellules mises à niveau sont arrêtées pendant la mise à niveau. S'il existe des serveurs VMware Cloud 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 Chapitre 5 Référence de l'outil de gestion des cellules.
- Consultez la rubrique Référence de l'utilitaire de mise à niveau de la base de données.

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 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 VMware Cloud 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 VMware Cloud Director mis à niveau.

Vous pouvez mettre à niveau les autres VMware Cloud Director membres du serveur de groupe et démarrer leurs services. Reportez-vous à Mise à niveau d'une cellule VMware Cloud 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.

L'emplacement de l'utilitaire `upgrade` est `/opt/vmware/vcloud-director/bin/`.

Tableau 4-3. Arguments et options de l'utilitaire de mise à niveau de base de données

Option	Argument	Description
`--backup-completed`	aucune	Indique que vous avez effectué une sauvegarde de VMware Cloud 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.	Si un utilisateur sous ce nom d'utilisateur existe déjà dans l'organisation du système, la mise à niveau échoue. Par défaut : `phone-home-system-account`

Tableau 4-3. Arguments et options de l'utilitaire de mise à niveau de base de données (suite)

Option	Argument	Description
`--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 des cellules pour rejoindre ou quitter le Programme d'amélioration du produit VMware à tout moment. Reportez-vous à la section Chapitre 5 Référence de l'outil de gestion des cellules.
`--installer-path`	Chemin d'accès complet au fichier d'installation de VMware Cloud Director. Le fichier d'installation et le répertoire dans lequel il est stocké doivent être accessibles par l'utilisateur vcloud.vcloud.	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` .

Tableau 4-3. Arguments et options de l'utilitaire de mise à niveau de base de données (suite)

Option	Argument	Description
`--multisite-user`	Nom d'utilisateur du compte système multi-site.	Ce compte est utilisé par la fonctionnalité multi-site de VMware Cloud Director . Si un utilisateur sous ce nom d'utilisateur existe déjà dans l'organisation du système, la mise à niveau échoue. Par défaut : `multisite-system-account`
`--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 VMware Cloud Director pour plus d'informations sur ce workflow de mise à niveau.
`--unattended-upgrade`	aucune	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 VMware Cloud Director pour servir d'identité sous laquelle les processus de VMware Cloud Director s'exécutent. L'utilisateur de `vcloud` n'a aucun mot de passe.

Après la mise à niveau de VMware Cloud Director

Après avoir mis à niveau l'ensemble des serveurs VMware Cloud Director et la base de données partagée, vous pouvez mettre à niveau les instances de 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 VMware Cloud Director.

Important VMware Cloud 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.

À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une connexion SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste bloquée d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent l'API VMware Cloud Director pour les tests de connexion. Configurez la liste bloquée après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste bloquée de connexion test.

Important Après la mise à niveau vers la version 10.1, VMware Cloud Director vérifie toujours les certificats pour tous les points de terminaison d'infrastructure qui y sont connectés. Cela est dû à une modification de la manière dont VMware Cloud Director gère les certificats SSL. Si vous n'importez pas vos certificats dans VMware Cloud Director avant la mise à niveau, les connexions vCenter Server et NSX peuvent afficher des erreurs de connexion infructueuses en raison de problèmes de vérification SSL. Dans ce cas, après la mise à niveau, vous avez deux options :

1. Exécutez la commande `trust-infra-certs` de l'outil de gestion des cellules pour importer automatiquement tous les certificats dans le magasin de certificats centralisé. Reportez-vous à la section Importer des certificats de point de terminaison depuis les ressources vSphere.
2. Dans l'interface utilisateur de Service Provider Admin Portal, sélectionnez chaque instance de vCenter Server et NSX, puis entrez à nouveau les informations d'identification tout en acceptant le certificat.

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 VMware Cloud 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 VMware Cloud Director, que des cellules VMware Cloud 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 VMware Cloud 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 VMware Cloud Director et NSX Manager, vous devez mettre à niveau les systèmes vCenter Server et les hôtes ESXi qui sont enregistrés sur VMware Cloud 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 barre de navigation supérieure du VMware Cloud Director Service Provider Admin Portal, sous **Ressources**, sélectionnez **Ressources vSphere**.

   b Dans le panneau de gauche, cliquez sur **Instances de vCenter Server**.

   c Sélectionnez la case d'option en regard de l'instance de vCenter Server que vous souhaitez désactiver et cliquez sur **Désactiver**.

   d Cliquez sur **OK**.

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 VMware Cloud Director.

   a Dans la barre de navigation supérieure, sélectionnez **Administration**.

   b Dans le panneau de gauche, sous **Paramètres**, cliquez sur **Adresses publiques**.

   c Vérifiez toutes les adresses publiques.

4 Actualisez l'enregistrement vCenter Server avec VMware Cloud Director.

   a Dans la barre de navigation supérieure du VMware Cloud Director Service Provider Admin Portal, sous **Ressources**, sélectionnez **Ressources vSphere**.

   b Dans le panneau de gauche, cliquez sur **Instances de vCenter Server**.

c Cochez la case d'option en regard de l'instance cible de vCenter Server et cliquez sur **Reconnecter**.

d Cliquez sur **OK**.

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 VMware Cloud 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 VMware Cloud Director afin de mettre à niveau une passerelle Edge NSX, vous devez intervenir sur l'objet réseau VMware Cloud Director que le dispositif Edge prend en charge :
  - Une mise à niveau appropriée d'une passerelle Edge s'exécute automatiquement lorsque vous utilisez VMware Cloud Director ou VMware Cloud Director API pour réinitialiser un réseau servi par la passerelle Edge.
  - Le redéploiement d'une passerelle Edge met à niveau le dispositif NSX Edge associé.

    Note Le redéploiement n'est pris en charge que pour les passerelles Edge NSX Data Center for vSphere.

  - La réinitialisation d'un réseau vApp dans le contexte du vApp met à niveau le dispositif NSX Edge associé à ce réseau. Pour réinitialiser un réseau vApp dans le contexte d'un vApp, accédez à l'onglet **Réseaux** pour le vApp, affichez ses détails de mise en réseau, cliquez sur la case d'option en regard du nom du réseau vApp, puis cliquez sur **Réinitialiser**.

Pour plus d'informations sur le redéploiement de passerelles Edge et la réinitialisation de réseaux vApp, reportez-vous au *Guide de programmation de l'API VMware Cloud Director*.

Étape suivante

Reprenez cette procédure pour les autres systèmes vCenter Server enregistrés dans votre installation VMware Cloud Director.

Référence de l'outil de gestion des cellules

5

L'outil de gestion de cellules est un utilitaire de ligne de commande que vous pouvez utiliser pour gérer une cellule ou une base de données VMware Cloud Director. Des informations d'identification de superutilisateur ou d'administrateur système sont requises pour la plupart des opérations.

L'outil de gestion des cellules est installé dans `/opt/vmware/vcloud-director/bin/`. Vous pouvez l'utiliser pour exécuter une commande ou l'exécuter comme un shell interactif.

Liste des commandes disponibles

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

```
./cell-management-tool -h
```

Utilisation du mode Shell

Vous pouvez exécuter l'outil de gestion de cellules comme shell interactif en l'invoquant sans argument, comme indiqué ci-dessous.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool
Cell Management Tool v8.14.0.4146350 Type "help" for available subcommands. cmt>
```

En mode Shell, vous pouvez taper n'importe quelle commande de l'outil de gestion de cellules à l'invite `cmt>`, comme dans cet exemple.

```
cmt>cell -h
usage: cell [options] -a,--application-states display the state of each application on
the cell [DEPRECATED - use the cell-application command instead] -h,--help print this
message -i,--pid <arg> the process id of the cell [REQUIRED if username is not specified]
-m,--maintenance <arg> gracefully enter maintenance mode on the cell -p,--password <arg>
administrator password [OPTIONAL] -q,--quiesce <arg> quiesce activity on the cell -s,--
shutdown gracefully shutdown the cell -t,--status display activity on the cell -tt,--
status-verbose display a verbose description of activity on the cell -u,--username <arg>
administrator username [REQUIRED if pid is not specified] Note: You will be prompted for
administrator password if not entered in command line. cmt>
```

La commande revient à l'invite `cmt>` en fin d'exécution. Pour quitter le mode Shell, tapez **`exit`** à l'invite `cmt>`.

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

Cet exemple exécute une commande non interactive qui répertorie les commandes disponibles de l'outil de gestion shell.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Available commands: cell -
Manipulates the Cell and core components certificates - Reconfigures the SSL certificates for
the cell . . . For command specific help: cell-management-tool <commandName> -h
```

- Configurer une installation de VMware Cloud Director

  Utilisez la commande `system-setup` de l'outil de gestion de cellules pour initialiser la base de données d'un groupe de serveurs avec un compte d'administrateur système et les informations associées.

- Désactiver l'accès du fournisseur de services au point de terminaison d'API hérité

  À partir de VMware Cloud Director 10.0, vous pouvez utiliser des points de terminaison de connexion de VMware Cloud Director OpenAPI distincts pour l'accès du fournisseur de services et du locataire à VMware Cloud Director.

- Gestion d'une cellule

  Avec la sous-commande `cell` de l'outil de gestion des cellules, vous pouvez suspendre le planificateur des tâches afin d'empêcher le démarrage de nouvelles tâches, vérifier l'état des tâches actives, contrôler le mode de maintenance d'une cellule et arrêter correctement la cellule.

- Gestion d'applications de cellule

  Utilisez la commande `cell-application` de l'outil de gestion de cellule pour contrôler l'ensemble des applications que la cellule exécute au démarrage.

- Modifier les propriétés de connexion de la base de données

  Vous pouvez mettre à jour les propriétés de connexion de la base de dconfiguration script or perform an unattended configuration where you set onnées VMware Cloud Director à l'aide de la sous-commande `reconfigure-database` de l'outil de gestion de cellules.

- Détection et réparation des données corrompues du planificateur

  VMware Cloud Director utilise le Planificateur de tâches Quartz pour coordonner les opérations asynchrones (tâches) en cours d'exécution sur le système. Si la base de données du planificateur Quartz se corrompt, vous risquez de ne pas être en mesure de suspendre le système correctement. Utilisez la commande `fix-scheduler-data` de l'outil de gestion de cellules pour analyser la base de données en recherchant les données corrompues du planificateur et les réparer si nécessaire.

- Génération de certificats auto-signés pour les points de terminaison HTTPS et de proxy de console

  Utilisez la commande `generate-certs` de l'outil de gestion des cellules pour générer des certificats SSL auto-signés pour les points de terminaison HTTPS et de proxy de console.
- Remplacement des certificats pour les points de terminaison HTTPS et de proxy de console

  Utilisez la commande `certificates` de l'outil de gestion de cellules pour remplacer les certificats SSL pour les points de terminaison HTTPS et de proxy de console.
- Importation de certificats SSL à partir de services externes

  Utilisez la commande `import-trusted-certificates` de l'outil de gestion des cellules pour importer des certificats à utiliser pour établir des connexions sécurisées à des services externes, tels qu'AMQP et la base de données VMware Cloud Director.
- Importer des certificats de points de terminaison à partir de ressources vSphere

  Après la mise à niveau, utilisez la commande `trust-infra-certs` de l'outil de gestion des cellules pour collecter et importer des certificats depuis les ressources vSphere de votre environnement vers la base de données VMware Cloud Director.
- Configurer une liste bloquée de connexion test

  Après l'installation ou la mise à niveau, utilisez la commande `manage-test-connection-blacklist` de l'outil de gestion des cellules pour bloquer l'accès aux hôtes internes avant de fournir aux locataires un accès au réseau VMware Cloud Director.
- Gestion de la liste des chiffrements SSL autorisés

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

  Pour configurer l'ensemble de protocoles SSL que la cellule propose d'utiliser lors du processus d'établissement de liaison SSL, utilisez la commande `ssl-protocols` de l'outil de gestion des cellules.
- Configuration de la collecte de mesures

  Utilisez la commande `configure-metrics` de l'outil de gestion de cellules pour configurer l'ensemble de mesures à collecter.
- Configuration d'une base de données de mesures Cassandra

  Utilisez la commande `cassandra` de l'outil de gestion des cellules pour connecter la cellule à une base de données de mesures en option.
- Restauration du mot de passe de l'administrateur système

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

- Mettre à jour l'état d'échec d'une tâche

  Utilisez la commande `fail-tasks` de l'outil de gestion des cellules pour mettre à jour l'état d'achèvement associé aux tâches que vous exécutiez lorsque la cellule a été volontairement arrêtée. Vous ne pouvez pas utiliser la commande `fail-tasks` si les cellules n'ont pas toutes été arrêtées.

- Configurer le traitement des messages d'audit

  Utilisez la commande `configure-audit-syslog` de l'outil de gestion de cellules pour configurer l'enregistrement des messages d'audit par le système.

- Configuration des modèles d'e-mail

  Pour gérer les modèles que le système utilise lors de la création d'alertes par e-mail, vous pouvez utiliser la commande `manage-email` de l'outil de gestion des cellules.

- Rechercher des machines virtuelles orphelines

  Utilisez la commande `find-orphan-vms` de l'outil de gestion de cellules pour rechercher des références à des machines virtuelles présentes dans la base de données vCenter mais pas dans la base de données VMware Cloud Director.

- Rejoindre ou quitter le programme d'amélioration du produit VMware

  Pour rejoindre ou quitter le Programme d'amélioration du produit (CEIP) VMware, vous pouvez utiliser la sous-commande `configure-ceip` de l'outil de gestion des cellules.

- Mise à jour des paramètres de configuration des applications

  Avec la sous-commande `manage-config` de l'outil de gestion des cellules, vous pouvez mettre à jour les paramètres de configuration de différentes applications, tels que les limitations de catalogue.

- Configuration de la limite de synchronisation du catalogue

  Lorsque vous disposez de nombreux éléments du catalogue publiés ou auxquels d'autres organisations sont abonnées, pour éviter de surcharger le système pendant les synchronisations du catalogue, vous pouvez configurer une limite de synchronisation du catalogue. Vous pouvez utiliser la sous-commande `manage-config` de l'outil de gestion des cellules pour configurer une limite de synchronisation du catalogue en limitant le nombre d'éléments de bibliothèque qui peuvent être synchronisés en même temps.

- Résoudre les problèmes d'échec d'accès à l'interface utilisateur de VMware Cloud Director

  Pour afficher et mettre à jour les adresses IP et les entrées DNS valides pour les cellules VMware Cloud Director dans votre environnement VMware Cloud Director, vous pouvez utiliser la sous-commande `manage-config` de l'outil de gestion des cellules.

- Débogage de la découverte de machines virtuelles vCenter

  La sous-commande `debug-auto-import` de l'outil de gestion des cellules vous permet de déterminer la raison pour laquelle le mécanisme de découverte des vApp ignore une ou plusieurs machines virtuelles vCenter.

- Régénération des adresses MAC pour les réseaux étirés multisites

  Si vous associez deux sites VMware Cloud Director qui sont configurés avec le même ID d'installation, vous pouvez rencontrer des conflits d'adresses MAC dans les réseaux étirés entre ces sites. Pour éviter de tels conflits, vous devez régénérer les adresses MAC d'un des sites en se basant sur une valeur initiale personnalisée qui est différente de l'ID d'installation.
- Mettre à jour les adresses IP de la base de données sur des cellules VMware Cloud Director

  Pour mettre à jour les adresses IP des cellules VMware Cloud Director dans un cluster haute disponibilité d'une base de données, vous pouvez utiliser l'outil de gestion des cellules.

Configurer une installation de VMware Cloud Director

Utilisez la commande `system-setup` de l'outil de gestion de cellules pour initialiser la base de données d'un groupe de serveurs avec un compte d'administrateur système et les informations associées.

Après que vous avez configuré tous les serveurs dans le groupe de serveurs VMware Cloud Director et les avez connectés à la base de données, vous pouvez créer le compte d'administrateur système initial et initialiser la base de données VMware Cloud Director avec les informations associées à l'aide d'une ligne de commande du format suivant :

```
cell-management-tool system-setup  options
```

Vous ne pouvez pas exécuter cette commande sur un système qui a déjà été configuré. Toutes les options à l'exception de `--unattended` et de `--password` doivent être spécifiées.

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

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--email`	Adresse e-mail de l'administrateur système que vous créez.	L'adresse e-mail de l'administrateur système est stockée dans la base de données VMware Cloud Director.
`--full-name`	Nom complet de l'administrateur système que vous créez.	Le nom complet de l'administrateur système est stocké dans la base de données VMware Cloud Director.

Tableau 5-1. Options et arguments de l'outil de gestion des cellules, sous-commande `system-setup` (suite)

Option	Argument	Description
`--installation-id`	Entier compris entre 1 et 63	ID d'installation pour cette installation de VMware Cloud Director. Le système utilise l'ID d'installation lors de la génération d'adresses MAC pour des cartes réseau virtuelles. **Note** Si vous prévoyez de créer des réseaux étirés dans les installations de VMware Cloud Director sur un déploiement multisite, envisagez de définir un ID d'installation unique pour chaque installation de VMware Cloud Director.
`--password`	Mot de passe de l'administrateur système que vous créez. Requis lorsque vous utilisez l'option `--unattended` . Si vous n'utilisez pas l'option `--unattended` , la commande vous demande ce mot de passe si vous ne le fournissez pas sur la ligne de commande.	L'administrateur système fournit le mot passe lors de l'authentification dans VMware Cloud Director.
`--serial-number`	Le numéro de série (clé de licence) de cette installation.	Facultatif. Doit être un numéro de série VMware Cloud Director valide.
`--system-name`	Nom à utiliser pour le dossier VMware Cloud Director de vCenter Server.	Cette installation de VMware Cloud Director est représentée par un dossier sous ce nom dans chaque instance de vCenter Server dans laquelle elle s'enregistre.
`--unattended`	Aucun	Facultatif. La commande ne demande pas d'autres informations lorsqu'elle est invoquée avec cette option.
`--user`	Nom d'utilisateur de l'administrateur système que vous créez.	L'administrateur système fournit ce nom d'utilisateur lors de l'authentification dans VMware Cloud Director.

Exemple : Spécifier les paramètres système de VMware Cloud Director

Une commande comme celle-ci spécifie tous les paramètres système d'une nouvelle installation de VMware Cloud Director. Comme les arguments `--unattended` et `--password` ne sont pas spécifiés, la commande vous demande de fournir et de confirmer le mot passe pour créer l'administrateur système.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool system-setup \ --user
admin --full-name "VCD System Administrator" --email vcd-admin@example.com --system-name VCD
--installation-id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

Désactiver l'accès du fournisseur de services au point de terminaison d'API hérité

À partir de VMware Cloud Director 10.0, vous pouvez utiliser des points de terminaison de connexion de VMware Cloud Director OpenAPI distincts pour l'accès du fournisseur de services et du locataire à VMware Cloud Director.

Vous pouvez utiliser deux nouveaux points de terminaison OpenAPI pour augmenter la sécurité en limitant l'accès à VMware Cloud Director.

- `/cloudapi/1.0.0/sessions/provider` - Point de terminaison OpenAPI pour la connexion du fournisseur de services. Les locataires ne peuvent pas accéder à VMware Cloud Director à l'aide de ce point de terminaison.
- `/cloudapi/1.0.0/sessions/` - Point de terminaison OpenAPI pour la connexion du locataire. Les fournisseurs de services ne peuvent pas accéder à VMware Cloud Director à l'aide de ce point de terminaison.

Par défaut, les administrateurs de fournisseurs et les utilisateurs d'organisation peuvent accéder à VMware Cloud Director en se connectant au point de terminaison d'API `/api/sessions`.

En utilisant la sous-commande `manage-config` de l'outil de gestion des cellules, vous pouvez désactiver l'accès du fournisseur de services au point de terminaison de l'API `/api/sessions` et limiter ainsi la connexion du fournisseur au point de terminaison OpenAPI `/cloudapi/1.0.0/sessions/provider` auquel seuls les fournisseurs de services ont accès.

Note Lorsque vous désactivez l'accès du fournisseur de services au point de terminaison de l'API `/api/sessions`, les demandes de fournisseur de services qui fournissent uniquement un jeton SAML dans l'en-tête d'autorisation échoueront pour tous les points de terminaison d'API hérités.

Procédure

1. Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur **`racine`** au système d'exploitation de toute cellule VMware Cloud Director.
2. Pour bloquer l'accès du fournisseur au point de terminaison d'API `/api/sessions`, utilisez l'outil de gestion des cellules et exécutez la commande suivante :

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v true
```

Résultats

Le point de terminaison d'API `/api/sessions` n'est plus accessible par les fournisseurs de services. Les fournisseurs de services peuvent utiliser le nouveau point de terminaison OpenAPI `/cloudapi/1.0.0/sessions/provider` pour accéder à VMware Cloud Director. Les locataires peuvent accéder à VMware Cloud Director en utilisant le point de terminaison d'API `/api/sessions` et le nouveau point de terminaison OpenAPI `/cloudapi/1.0.0/sessions/`.

Étape suivante

Pour permettre au fournisseur d'accéder au point de terminaison d'API `/api/sessions`, exécutez la commande suivante :

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

Gestion d'une cellule

Avec la sous-commande `cell` de l'outil de gestion des cellules, vous pouvez suspendre le planificateur des tâches afin d'empêcher le démarrage de nouvelles tâches, vérifier l'état des tâches actives, contrôler le mode de maintenance d'une cellule et arrêter correctement la cellule.

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

```
cell-management-toolcell-usysadmin-username -p sysadmin-passwordoption
```

où *sysadmin-username* et *sysadmin-password* sont le nom d'utilisateur et le mot de passe de l'**administrateur système**.

Note Pour des raisons de sécurité, vous pouvez omettre le mot de passe. Dans ce cas, la commande vous invite à entrer le mot de passe sans l'afficher sur l'écran.

Au lieu de fournir les informations d'identification de l'**administrateur système**, vous pouvez utiliser l'option `--pid` et fournir l'ID de processus du processus de cellule. Pour rechercher l'ID de processus de la cellule, utilisez une commande semblable à celle-ci :

```
cat /var/run/vmware-vcd-cell.pid
```

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

Option	Argument	Description
`--help` (`-h`)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--pid` (`-i`)	ID de processus du processus de cellule	Vous pouvez utiliser cette option plutôt que `-username`
`--maintenance` (`-m`)	`true` ou `false`	Définit la cellule en mode de maintenance. L'argument `true` suspend l'activité sur la cellule et place la cellule en mode de maintenance. L'argument `false` fait sortir la cellule du mode de maintenance.
`--password` (`-p`)	Mot de passe de l'VMware Cloud Director**administrateur système**	Facultatif si l'option `-username` est utilisée. Si vous omettez cette option, la commande vous invite à entrer le mot de passe sans l'afficher sur l'écran.
`--quiesce` (`-q`)	`true` ou `false`	Met en veille l'activité sur la cellule. L'argument `true` suspend le planificateur. L'argument `false` redémarre le planificateur.
`--shutdown` (`-s`)	Aucun	Arrête correctement les services VMware Cloud Director sur le serveur.
`--status` (`-t`)	Aucun	Affiche des informations sur le nombre de tâches exécutées sur la cellule et l'état de la cellule.

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

Option	Argument	Description
`--status-verbose` (`-tt`)	Aucun	Affiche des informations détaillées sur le nombre de tâches exécutées sur la cellule et l'état de la cellule.
`--username` (`-u`)	Nom d'utilisateur de l'VMware Cloud Director**administrateur système**.	Vous pouvez utiliser cette option plutôt que `-pid`

Gestion d'applications de cellule

Utilisez la commande `cell-application` de l'outil de gestion de cellule pour contrôler l'ensemble des applications que la cellule exécute au démarrage.

Un système VMware Cloud Director exécute un certain nombre d'applications qui fournissent des services que les clients VMware Cloud Director nécessitent. La cellule démarre un sous-ensemble de ces applications par défaut. Tous les membres de ce sous-ensemble sont généralement requis pour prendre en charge une installation de VMware Cloud Director .

Pour afficher ou modifier la liste d'applications qui s'exécutent au démarrage de la cellule, utilisez une ligne de commande de la forme suivante :

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

sysadmin-username

Nom d'utilisateur d'un administrateur système VMware Cloud Director.

sysadmin-password

Mot de passe de l'administrateur système VMware Cloud Director. Vous devez indiquer le mot de passe s'il contient des caractères spéciaux.

Note Vous pouvez fournir le mot de passe de l'administrateur système VMware Cloud Director sur la ligne de commande `cell-management-tool`, mais il est plus sûr d'omettre le mot de passe. La commande `cell-management-tool` vous invitera alors à saisir le mot de passe, qui ne s'affiche pas à l'écran au fur et à mesure que vous tapez.

Au lieu de fournir les informations d'identification de l'administrateur système, vous pouvez utiliser l'option `--pid` et fournir l'ID de processus du processus de cellule. Pour rechercher l'ID de processus de la cellule, utilisez une commande semblable à celle-ci :

```
cat /var/run/vmware-vcd-cell.pid
```

commande

Sous-commande `cell-application`.

Tableau 5-3. Options et arguments de l'outil de gestion des cellules, sous-commande `cell-application`

Commande	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--application-states`	Aucun	Répertorier les applications de cellule et leur état actuel.
`--disable`	ID d'application	Empêcher cette application de cellule de s'exécuter au démarrage de la cellule.
`--enable`	ID d'application	Autoriser cette application de cellule à s'exécuter au démarrage de la cellule.
`--pid` (-i)	ID de processus du processus de cellule	Vous pouvez utiliser cette option plutôt que `-u` ou `-u` et `-p`.
`--list`	Aucun	Répertorier toutes les applications de cellule et indiquer si elles sont activées pour s'exécuter au démarrage de la cellule.
`--password` (-p)	Mot de passe de l'administrateur VMware Cloud Director	Facultatif. La commande demandera le mot de passe si vous ne le fournissez pas sur la ligne de commande.
`--set`	Liste d'ID d'application séparés par des points-virgules.	Spécifier l'ensemble des applications de cellule qui s'exécutent au démarrage de la cellule. Cette commande remplace l'ensemble existant d'applications de cellule qui démarrent au démarrage de la cellule. Utiliser `--enable` ou `--disable` pour modifier l'état de démarrage d'une application spécifique.
`--username` (-u)	Nom d'utilisateur de l'administrateur VMware Cloud Director.	Requis si `--pid` non spécifié

Exemple : Liste des applications de cellule et leur état de démarrage

La ligne de commande suivante `cell-management-tool` requière les informations d'identification du système et renvoie la liste des applications de cellule et leur état de démarrage.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell-application --list
Please enter the administrator password:

 name                    id              enabled
description

 Networking              com.vmware.vc... true     Exposes NSX api endpoints directly from vCD.
 Console Proxy           com.vmware.vc... true     Proxies VM console data connection...
 Cloud Proxy             com.vmware.vc... true     Proxies TCP connections from a tenant site.
 Compute Service Broker  com.vmware.vc... true     Allows registering with a service
```

```
control...
 Maintenance Application  com.vmware.vc... false    Indicates to users the cell is
undergo ...
 Core Cell Application    com.vmware.vc... true     Main cell application, Flex UI and REST
API.
```

Modifier les propriétés de connexion de la base de données

Vous pouvez mettre à jour les propriétés de connexion de la base de dconfiguration script or perform an unattended configuration where you set onnées VMware Cloud Director à l'aide de la sous-commande `reconfigure-database` de l'outil de gestion de cellules.

Lors de l'installation de VMware Cloud Director ou du processus de déploiement du dispositif VMware Cloud Director, vous configurez les propriétés de type de base de données et de connexion de base de données. Reportez-vous à Installer VMware Cloud Director sous Linux et à Déploiement et configuration initiale du dispositif VMware Cloud Director.

Après avoir configuré la base de données VMware Cloud Director, vous pouvez mettre à jour les connexions de base de données à l'aide de la sous-commande `reconfigure-database`. Vous pouvez déplacer la base de données VMware Cloud Director existante vers un nouvel hôte, changer le nom d'utilisateur et le mot de passe de la base de données, ou activer une connexion SSL à une base de données PostgreSQL.

```
cell-management-tool reconfigure-database  options
```

Important Les modifications que vous apportez en exécutant la commande `reconfigure-database` sont écrites dans le fichier de configuration globale `global.properties` et le fichier de réponse `responses.properties` de la cellule. Avant d'exécuter la commande, vérifiez la présence du fichier de réponse dans `/opt/vmware/vcloud-director/etc/responses.properties` et son accessibilité en écriture. Pour plus d'informations sur la protection et la réutilisation du fichier de réponses, reportez-vous à Installer VMware Cloud Director sous Linux.

Si vous n'utilisez pas l'option `--pid`, vous devez redémarrer la cellule pour appliquer les modifications.

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

Option	Argument	Description
`--help` (`-h`)	aucune	Fournit un résumé des options disponibles dans cette catégorie.
`--database-host` (`-dbhost`)	Adresse IP ou nom de domaine complet de VMware Cloud Director l'hôte de la base de données	Met à jour la valeur de la propriété `database.jdbcUrl`. **Important** La commande ne valide que le format de la valeur.

Tableau 5-4. Options et arguments de l'outil de gestion des cellules, sous-commande `reconfigure-database` (suite)

Option	Argument	Description
`--database-instance` (`-dbinstance`)	Instance de la base de données SQL Server.	Facultatif. Utilisée si le type de base de données est `sqlserver`. **Important** Si vous incluez cette option, vous devez fournir la même valeur que celle que vous avez spécifiée lors de la configuration initiale de la base de données.
`--database-name` (`-dbname`)	Nom de service de la base de données.	Met à jour la valeur de la propriété `database.jdbcUrl`.
`--database-password` (`-dbpassword`)	Mot de passe de l'utilisateur de la base de données.	Met à jour la valeur de la propriété `database.password`. Le mot de passe que vous fournissez est chiffré avant d'être stocké sous la forme d'une valeur de propriété.
`--database-port` (`-dbport`)	Numéro de port utilisé par le service de base de données sur l'hôte de la base de données.	Met à jour la valeur de la propriété `database.jdbcUrl`. **Important** La commande ne valide que le format de la valeur.
`--database-type` (`-dbtype`)	Type de base de données. Un des types suivants : ■ `sqlserver` ■ `postgres`	Met à jour la valeur de la propriété `database.jdbcUrl`.
`--database-user` (`-dbuser`)	Nom d'utilisateur de l'utilisateur de la base de données.	Met à jour la valeur de la propriété `database.user`.
`--database-ssl`	`true` ou `false`	Utilisée si le type de base de données est `postgres`. Configure la base de données PostgreSQL pour qu'elle exige une connexion SSL depuis VMware Cloud Director.
`--pid` (`-i`)	ID de processus de la cellule.	Facultatif. Exécute une reconfiguration à chaud sur une cellule VMware Cloud Director en cours d'exécution. Ne nécessite pas de redémarrage de la cellule. Si l'option est utilisée avec `--private-key-path`, vous pouvez exécuter la commande sur des cellules locales et distantes immédiatement.

Tableau 5-4. Options et arguments de l'outil de gestion des cellules, sous-commande `reconfigure-database` (suite)

Option	Argument	Description
`--private-key-path`	Chemin d'accès à la clé privée de la cellule.	Facultatif. Toutes les cellules du groupe de serveurs s'arrêtent normalement, mettent à jour leurs propriétés de base de données et redémarrent. **Important** Toutes les cellules doivent autoriser les connexions SSH à partir du super utilisateur sans mot de passe.
`--remote-sudo-user`	Un nom d'utilisateur avec les droits sudo.	S'utilise avec l'option `--private-key-path` lorsque l'utilisateur distant est différent de **racine**. Pour le dispositif, vous pouvez utiliser cette option pour l'utilisateur **postgres** ; par exemple, **`--remote-sudo-user=postgres`**.

Lorsque vous utilisez les options `--database-host` et `--database-port`, la commande valide le format des arguments, mais ne teste pas la combinaison de l'hôte et du port pour l'accessibilité réseau ou la présence d'une base de données en cours d'exécution du type spécifié.

Si vous utilisez l'option `--private-key-path` , toutes les cellules doivent être configurées pour autoriser les connexions SSH depuis le super utilisateur sans mot de passe. Par exemple, 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 VMware Cloud Director pour servir d'identité sous laquelle les processus de VMware Cloud Director s'exécutent. L'utilisateur de `vcloud` n'a aucun mot de passe.

Exemple : Modifier le nom d'utilisateur et le mot de passe de la base de données VMware Cloud Director

Pour changer le nom d'utilisateur et le mot de passe de la base de données VMware Cloud Director, si vous conservez toutes les autres propriétés de connexion telles qu'elles ont été initialement configurées, vous pouvez exécuter la commande suivante :

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \
-dbuser vcd-dba -dbpassword P@55w0rd
```

Exemple : Mettre à jour l'adresse IP de la base de données VMware Cloud Director par une reconfiguration à chaud sur toutes les cellules

Si vous êtes un utilisateur non-racine disposant de droits sudo, pour changer l'adresse IP de la base de données VMware Cloud Director immédiatement sur toutes les cellules, vous pouvez exécuter la commande suivante :

```
[sudo@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \ --
dbhost db_ip_address -i $(service vmware-vcd pid cell) --private-key-path=path_to_private-key
\ --remote-sudo-user=non-root-user
```

Détection et réparation des données corrompues du planificateur

VMware Cloud Director utilise le Planificateur de tâches Quartz pour coordonner les opérations asynchrones (tâches) en cours d'exécution sur le système. Si la base de données du planificateur Quartz se corrompt, vous risquez de ne pas être en mesure de suspendre le système correctement. Utilisez la commande `fix-scheduler-data` de l'outil de gestion de cellules pour analyser la base de données en recherchant les données corrompues du planificateur et les réparer si nécessaire.

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

```
cell-management-toolfix-scheduler-dataoptions
```

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

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

Génération de certificats auto-signés pour les points de terminaison HTTPS et de proxy de console

Utilisez la commande `generate-certs` de l'outil de gestion des cellules pour générer des certificats SSL auto-signés pour les points de terminaison HTTPS et de proxy de console.

Chaque groupe de serveurs VMware Cloud Director doit prendre en charge deux points de terminaison SSL : un pour le service HTTPS et un autre pour le service de proxy de console. Le point de terminaison du service HTTPS prend en charge le VMware Cloud Director Service Provider Admin Portal, le VMware Cloud Director Tenant Portal et VMware Cloud Director API. Le point de terminaison de proxy de console distante prend en charge les connexions VMRC aux vApp et aux machines virtuelles.

La commande `generate-certs` de l'outil de gestion des cellules automatise la procédure Créer des certificats SSL auto-signés pour VMware Cloud Director sous Linux.

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

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

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

Option	Argument	Description
`--help` (-h)	aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--expiration` (-x)	*days-until-expiration*	Nombre de jours avant l'expiration des certificats. Réglé par défaut sur 365.

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

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

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

Exemple : Création de certificats auto-signés

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

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

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

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

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

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

Remplacement des certificats pour les points de terminaison HTTPS et de proxy de console

Utilisez la commande `certificates` de l'outil de gestion de cellules pour remplacer les certificats SSL pour les points de terminaison HTTPS et de proxy de console.

La commande `certificates` de l'outil de gestion des cellules automatise le processus de remplacement des certificats existants par de nouveaux certificats, qui sont stockés dans un keystore JCEKS. Utilisez la commande `certificates` pour remplacer les certificats auto-signés par des certificats signés ou pour remplacer les certificats arrivant à expiration par de nouveaux certificats. Pour créer un keystore JCEKS contenant des certificats signés, consultez Créer des certificats SSL auto-signés pour VMware Cloud Director sous Linux.

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

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

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

Option	Argument	Description
`--help` (-h)	aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--config` (-c)	Chemin d'accès complet vers le fichier `global.properties` de la cellule	Réglé par défaut sur `$VCLOUD_HOME/etc/global.properties`.
`--httpks` (-j)	aucune	Remplacez le fichier keystore nommé `certificates` utilisé par le point de terminaison http.

Tableau 5-7. Options et arguments de l'outil de gestion des cellules, sous-commande `certificates` (suite)

Option	Argument	Description
`--consoleproxyks` (-p)	aucune	Remplacez le fichier keystore nommé `proxycertificates` utilisé par le point de terminaison http de proxy de la console.
`--responses` (-r)	Chemin d'accès complet vers le fichier `responses.properties` de la cellule	Réglé par défaut sur `$VCLOUD_HOME/etc/responses.properties`.
`--keystore` (-k)	*keystore-pathname*	Chemin d'accès complet vers un keystore JCEKS contenant les certificats signés. Version abrégée `-s` déconseillée remplacée par `-k`.
`--keystore-password` (-w)	*keystore-password*	Mot de passe du keystore JCEKS référencé par l'option `--keystore`. Remplace les options `-kspassword` et `--keystorepwd` déconseillées.

Exemple : Remplacement des certificats

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

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

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

Importation de certificats SSL à partir de services externes

Utilisez la commande `import-trusted-certificates` de l'outil de gestion des cellules pour importer des certificats à utiliser pour établir des connexions sécurisées à des services externes, tels qu'AMQP et la base de données VMware Cloud Director.

Avant de pouvoir établir une connexion sécurisée à un service externe, VMware Cloud Director doit établir une chaîne de confiance valide pour ce service en important des certificats du service dans son propre truststore. Pour importer des certificats de confiance dans le truststore de la cellule, utilisez une commande au format suivant :

```
cell-management-toolimport-trusted-certificatesoptions
```

Tableau 5-8. Options et arguments de l'outil de gestion des cellules, sous-commande `import-trusted-certificates`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--destination`	nom du chemin d'accès	Nom de la route d'accès complet au truststore de destination. La valeur par défaut est `opt/vmware/vcloud-director/etc/certificates` si aucun chemin d'accès n'est fourni dans la ligne de commande.
`--destination-password`	chaîne	Mot de passe pour le truststore de destination. Si aucune valeur n'est spécifiée dans la ligne de commande, la valeur de `vcloud.ssl.truststore.password` est utilisée par défaut.
`--destination-type`	type de keystore	Type de keystore du truststore de destination. Il peut s'agir de JKS ou JCEKS. La valeur par défaut est JCEKS.
`--force`	Aucun	Remplace les certificats existants dans le truststore de destination.
`--source`	nom du chemin d'accès	Nom de la route d'accès complet au fichier PEM source.

Exemple : Importation de certificats approuvés

Cet exemple importe les certificats à partir de `/tmp/demo.pem` vers le keystore local VMware Cloud Director dans `/opt/vmware/vcloud-director/etc/certificates`. VMware Cloud Director stocke le mot de passe du keystore dans un format chiffré que la commande `import-trusted-certificates` déchiffre.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

Importer des certificats de points de terminaison à partir de ressources vSphere

Après la mise à niveau, utilisez la commande `trust-infra-certs` de l'outil de gestion des cellules pour collecter et importer des certificats depuis les ressources vSphere de votre environnement vers la base de données VMware Cloud Director.

La commande `trust-infra-certs` de l'outil de gestion des cellules collecte automatiquement les certificats SSL à partir des ressources vSphere de votre environnement et les importe dans la base de données VMware Cloud Director.

Conditions préalables

Vérifiez que les instances de vCenter Server et NSX Manager pour lesquelles vous souhaitez importer des points de terminaison sont en cours d'exécution.

Procédure

1. Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur racine à la cellule VMware Cloud Director.
2. Exécutez la commande au format suivant.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs options
```

Tableau 5-9. Options et arguments de l'outil de gestion des cellules, sous-commande `trust-infra-certs`

Option	Argument	Description
`--help (-h)`	Aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--vsphere`	Aucune	Vous invite à approuver les certificats de toutes les instances de vCenter Server, de NSX Data Center for vSphere et de NSX-T Data Center enregistrées dans cette installation.
`--trust`	Aucune	Facultatif. Ajoute des certificats au magasin d'approbations de VMware Cloud Director.
`--inspect`	Facultatif. Chemin d'accès.	Facultatif. Affiche les certificats dans un fichier.
`--unattended`	Aucune	Facultatif. La commande ne demande pas d'autres informations lorsqu'elle est invoquée avec cette option. Tous les certificats d'infrastructure sont automatiquement approuvés.

Exemple : approuver et importer tous les certificats à partir de points de terminaison de ressources vSphere

Pour approuver et importer les certificats à partir de vos points de terminaison de ressources vSphere sans être invité à entrer d'autres informations, exécutez la commande avec les options suivantes.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs --vsphere --unattended
```

Configurer une liste bloquée de connexion test

Après l'installation ou la mise à niveau, utilisez la commande `manage-test-connection-blacklist` de l'outil de gestion des cellules pour bloquer l'accès aux hôtes internes avant de fournir aux locataires un accès au réseau VMware Cloud Director.

À partir de VMware Cloud Director 10.1, les fournisseurs de services et les locataires peuvent utiliser l'API VMware Cloud Director pour tester les connexions à des serveurs distants et vérifier l'identité du serveur dans le cadre d'une connexion à SSL.

Pour protéger le réseau interne dans lequel une instance de VMware Cloud Director est déployée contre les attaques malveillantes, les fournisseurs de systèmes peuvent configurer une liste bloquée des hôtes internes inaccessibles aux locataires.

Ainsi, si un pirate ayant un accès locataire tente d'utiliser l'API de test de connexion VMware Cloud Director pour mapper le réseau sur lequel VMware Cloud Director est installé, il ne pourra pas se connecter aux hôtes internes sur la liste bloquée.

Après l'installation ou la mise à niveau et avant de fournir aux locataires l'accès au réseau VMware Cloud Director, utilisez la commande `manage-test-connection-blacklist` de l'outil de gestion des cellules pour bloquer l'accès des locataires aux hôtes internes.

Procédure

1. Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur racine à la cellule VMware Cloud Director.
2. Exécutez la commande pour ajouter une entrée à la liste bloquée.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool manage-test-connection-blacklist
   option
   ```

   Tableau 5-10. Options et arguments de l'outil de gestion des cellules, sous-commande `manage-test-connection-blacklist`

Option	Argument	Description
`--help (-h)`	Aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--add-ip`	Adresse IPv4 ou IPv6	Ajoute une adresse IP à la liste bloquée.

Tableau 5-10. Options et arguments de l'outil de gestion des cellules, sous-commande `manage-test-connection-blacklist` (suite)

Option	Argument	Description
`--add-name`	Sous-domaine ou nom de domaine complet pour un hôte	Ajoute un sous-domaine ou un nom de domaine à la liste bloquée.
`--add-range`	Plage d'adresses IPv4 ou IPv6 au format CIDR ou séparées par des tirets.	Ajoute une plage d'adresses IP à la liste bloquée.
`--list`	Aucune	Répertorie toutes les entrées existantes avec l'accès refusé.

Gestion de la liste des chiffrements SSL autorisés

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

Note La commande `ciphers` ne s'applique qu'à l'ensemble de certificats que VMware Cloud Director utilise pour les communications HTTPS et de proxy de console, et non aux certificats que le dispositif VMware Cloud Director utilise pour son interface utilisateur de gestion de dispositif et son API.

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

1. Créez de nouveaux certificats qui n'utilisent aucun des chiffrements rejetés. Vous pouvez utiliser `cell-management-tool ciphers -a` comme indiqué dans l'exemple ci-dessous pour répertorier tous les chiffrements autorisés dans la configuration par défaut.
2. Utilisez la commande `cell-management-tool certificates` pour remplacer les certificats existants de la cellule par les nouveaux.

3 Utilisez la commande `cell-management-tool ciphers` pour reconfigurer la liste des chiffrements autorisés afin d'exclure tous les chiffrements non utilisés par les nouveaux certificats. L'exclusion de ces chiffrements facilite la mise en place d'une connexion SSL sur la cellule, du fait que le nombre de chiffrements offerts lors de l'établissement de liaison est réduit au minimum pratique.

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

Pour gérer la liste des chiffrements SSL autorisés, utilisez une ligne de commande au format suivant.

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

Tableau 5-11. Options et arguments de l'outil de gestion des cellules, sous-commande `ciphers`

Option	Argument	Description
`--help` (-h)	Aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--all-allowed` (-a)	Aucune	Répertoriez tous les chiffrements pris en charge par VMware Cloud Director.
`--compatible-reset` (-c)	Aucune	Réinitialiser la liste par défaut des chiffrements autorisés et autoriser les chiffrements utilisés par les certificats de cette cellule.
`--disallow` (-d)	Liste de noms de chiffrement séparés par des virgules.	Rejeter les chiffrements de la liste séparée par des virgules spécifiée. Chaque fois que vous exécutez cette option, vous devez inclure la liste complète des chiffrements que vous souhaitez désactiver, car l'exécution de l'option remplace le paramètre précédent. **Important** L'exécution de l'option sans valeur active tous les chiffrements. Pour afficher tous les chiffrements possibles, exécutez l'option `-a`. **Important** Vous devez redémarrer la cellule après l'exécution de **`ciphers --disallow`**.

Tableau 5-11. Options et arguments de l'outil de gestion des cellules, sous-commande `ciphers` (suite)

Option	Argument	Description
`--list` (-l)	Aucune	Répertorie l'ensemble des chiffrements autorisés en cours d'utilisation.
`--reset` (-r)	Aucune	Réinitialiser la liste par défaut des chiffrements autorisés. Si les certificats de cette cellule utilisent des chiffrements rejetés, vous ne pourrez pas établir de connexion SSL à la cellule tant que vous n'aurez pas installé de nouveaux certificats qui contiennent un chiffrement autorisé. **Important** Vous devez redémarrer la cellule après l'exécution de **`ciphers --reset`**.

Exemple : Rejeter deux chiffrements

VMware Cloud Director inclut une liste préconfigurée de chiffrements activés.

Cet exemple montre comment activer des chiffrements supplémentaires à partir de la liste des chiffrements autorisés et comment interdire les chiffrements que vous ne souhaitez pas utiliser.

1 Obtenez la liste des chiffrements activés par défaut.

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

La sortie de la commande renvoie la liste des chiffrements activés.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

2 Obtenez une liste de tous les chiffrements que la cellule peut offrir lors d'une négociation SSL.

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

La sortie de la commande renvoie la liste des chiffrements autorisés.

```
# ./cell-management-tool ciphers -a
Product default ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
```

```
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
```

3 Spécifiez les chiffrements à désactiver.

Si vous exécutez la commande et que vous ne désactivez pas explicitement un chiffrement, il devient activé.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool ciphers -d
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
```

4 Exécutez la commande pour vérifier la liste des chiffrements activés. Tout chiffrement absent de la liste est désactivé.

```
root@bos1-vcd-static-211-90 [ /opt/vmware/vcloud-director/bin ]# ./cell-management-tool
ciphers -l
```

La sortie renvoie une liste de tous les chiffrements qui sont maintenant activés.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
```

```
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
```

Gérer la liste des protocoles SSL autorisés

Pour configurer l'ensemble de protocoles SSL que la cellule propose d'utiliser lors du processus d'établissement de liaison SSL, utilisez la commande `ssl-protocols` de l'outil de gestion des cellules.

Lorsqu'un client effectue une connexion SSL sur une cellule VMware Cloud Director, la cellule propose d'utiliser uniquement les protocoles qui sont configurés sur sa liste de protocoles SSL autorisés. Plusieurs protocoles, y compris TLSv1, SSLv3 et SSLv2Hello, ne figurent pas dans la liste par défaut, car ils sont connus pour avoir de graves problèmes de sécurité.

Procédure

1 Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation de la cellule VMware Cloud Director en tant qu'utilisateur **racine**.

2 Exécutez la commande pour gérer la liste des protocoles SSL autorisés.

```
cell-management-tool ssl-protocols options
```

Tableau 5-12. Options et arguments de l'outil de gestion des cellules, sous-commande `ssl-protocols`

Option	Argument	Description
`--help` (-h)	Aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--all-allowed` (-a)	Aucune	Répertoriez tous les protocoles SSL pris en charge par VMware Cloud Director.

Tableau 5-12. Options et arguments de l'outil de gestion des cellules, sous-commande `ssl-protocols` (suite)

Option	Argument	Description
`--disallow` (-d)	Liste de noms de protocoles SSL séparés par une virgule.	Reconfigurez la liste des protocoles SSL non autorisés sur les protocoles spécifiés dans la liste. Chaque fois que vous exécutez cette option, vous devez inclure la liste complète des protocoles SSL que vous souhaitez désactiver, car l'exécution de l'option remplace le paramètre précédent. **Important** L'exécution de l'option sans valeur active tous les protocoles SSL. Pour afficher tous les protocoles SSL possibles, exécutez l'option `-a`. **Important** Vous devez redémarrer la cellule après l'exécution de **`ssl-protocols --disallow`**.
`--list` (-l)	Aucune	Répertorie l'ensemble des protocoles SSL autorisés en cours d'utilisation.
`--reset` (-r)	Aucune	Réinitialisez la liste des protocoles SSL configurés sur les paramètres d'usine par défaut. **Important** Vous devez redémarrer la cellule après l'exécution de **`ssl-protocols --reset`**.

Exemple : Répertoriez les protocoles SSL autorisés et configurés, et reconfigurez la liste des protocoles SSL non autorisés

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

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

    * TLSv1.2
    * TLSv1.1
    * TLSv1
    * SSLv3
    * SSLv2Hello
```

En général, cette liste est un sur-ensemble de protocoles SSL que la cellule est configurée pour prendre en charge. Pour répertorier ces protocoles SSL, utilisez l'option `--list` (-l).

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

    * TLSv1.2
    * TLSv1.1
```

Pour reconfigurer la liste des protocoles SSL non autorisés, utilisez l'option `--disallow` (`-d`). Cette option nécessite une liste des sous-ensembles (séparés par une virgule) des protocoles autorisés produite par `ssl-protocols -a`.

Cet exemple met à jour la liste des protocoles SSL autorisés pour inclure TLSv1. Les versions de vCenter Serverantérieures à la version 5.5 Update 3e nécessitent TLSv1.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d
SSLv3,SSLv2Hello
```

Vous devez redémarrer la cellule après avoir exécuté cette commande.

Configuration de la collecte de mesures

Utilisez la commande `configure-metrics` de l'outil de gestion de cellules pour configurer l'ensemble de mesures à collecter.

VMware Cloud Director peut collecter des mesures qui fournissent des informations actuelles et historiques sur les performances et la consommation de ressources de la machine virtuelle. Utilisez cette sous-commande pour configurer les mesures collectées par VMware Cloud Director. Utilisez la sous-commande `cell-management-tool cassandra` pour configurer une base de données Apache Cassandra utilisable comme référentiel de mesures VMware Cloud Director. Reportez-vous à Configuration d'une base de données de mesures Cassandra.

Pour configurer les mesures collectées par VMware Cloud Director, utilisez une ligne de commande au format suivant :

```
cell-management-tool configure-metrics --metrics-config pathname
```

Tableau 5-13. Options et arguments de l'outil de gestion des cellules, sous-commande `configure-metrics`

Commande	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--repository-host` (Obsolète)	Nom d'hôte ou adresse IP de l'hôte KairosDB	Obsolète. Utilisez l'option `--cluster-nodes` de la sous-commande `cell-management-tool cassandra` pour configurer une base de données Apache Cassandra utilisable comme référentiel de mesures VMware Cloud Director.
`--repository-port` (Obsolète)	Port de KairosDB à utiliser.	Obsolète. Utilisez l'option `--port` de la sous-commande `cell-management-tool cassandra` pour configurer une base de données Apache Cassandra utilisable comme référentiel de mesures VMware Cloud Director.
`--metrics-confg`	nom du chemin d'accès	Chemin d'accès au fichier de configuration de mesures

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

Cet exemple configure la collecte de mesures telle que spécifiée dans le fichier `/tmp/metrics.groovy`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

Le service de collecte de mesures VMware Cloud Director implémente un sous-ensemble des mesures collectées par vSphere Performance Manager. Consultez la documentation de vSphere Performance Manager pour obtenir plus d'informations sur les noms de mesure et les paramètres de collecte. Le fichier `metrics-config` cite un ou plusieurs noms de mesure et fournit des paramètres de collecte pour chaque mesure citée. Par exemple :

```
configuration {
    metric("cpu.usage.average")
    metric("cpu.usagemhz.average")
    metric("cpu.usage.maximum")
    metric("disk.used.latest") {
        currentInterval=300
        historicInterval=300
        entity="VM"
        instance=""
        minReportingInterval=1800
```

```
        aggregator="AVERAGE"
    }
}
```

Les noms de mesure suivants sont pris en charge.

Tableau 5-14. Noms de mesure

Nom de mesure	Description
`cpu.usage.average`	Vue de l'hôte de l'activité moyenne du CPU de cette machine virtuelle en tant que pourcentage du total disponible. Inclut tous les cœurs dans tous les sockets.
`cpu.usagemhz.average`	Vue de l'hôte de l'activité moyenne du CPU de cette machine virtuelle en tant que mesure brute. Inclut tous les cœurs dans tous les sockets.
`cpu.usage.maximum`	Vue de l'hôte de l'activité maximale du CPU de cette machine virtuelle en tant que pourcentage du total disponible. Inclut tous les cœurs dans tous les sockets.
`mem.usage.average`	Mémoire utilisée par cette machine virtuelle en tant que pourcentage de la mémoire totale configurée.
`disk.provisioned.latest`	Espace de stockage alloué à ce disque dur virtuel dans le centre de données virtuel d'organisation conteneur.
`disk.used.latest`	Stockage utilisé par tous les disques durs virtuels.
`disk.read.average`	Taux de lecture moyen pour tous les disques durs virtuels.
`disk.write.average`	Taux d'écriture moyen pour tous les disques durs virtuels.

Note Lorsqu'une machine virtuelle a plusieurs disques, les mesures sont indiquées comme un agrégat de tous les disques. Les mesures de CPU sont un agrégat de tous les cœurs et sockets.

Pour chaque mesure nommée, vous pouvez spécifier les paramètres de collecte suivants.

Tableau 5-15. Paramètres de collecte des mesures

Nom du paramètre	Valeur	Description
`currentInterval`	Nombre entier de secondes.	Intervalle en secondes à utiliser lors d'une demande des dernières valeurs de mesure disponibles (pour les requêtes de mesures actuelles). La valeur 20 est utilisée par défaut. Les valeurs supérieures à 20 ne sont prises en charge que pour les mesures de niveau 1 telles que définies par vSphere Performance Manager.
`historicInterval`	Nombre entier de secondes.	Intervalle en secondes à utiliser lors de l'interrogation des valeurs de mesure historique. Défini par défaut sur 20 s'il n'est pas spécifié. Les valeurs supérieures à 20 ne sont prises en charge que pour les mesures de niveau 1 telles que définies par vSphere Performance Manager.

Tableau 5-15. Paramètres de collecte des mesures (suite)

Nom du paramètre	Valeur	Description
`entity`	`HOST` ou `VM`	Le type d'objet VC pour lequel la mesure est disponible devient VM par défaut si cette valeur n'est pas spécifiée. Certaines mesures ne sont pas disponibles pour toutes les entités.
`instance`	Identifiant de l'instance `PerfMetricId` de vSphere Performance Manager.	Indique s'il convient de récupérer les données d'instances individuelles d'une mesure (par exemple, cœurs individuels de CPU), un agrégat de toutes les instances ou les deux. La valeur `"*"` collecte toutes les mesures, instances et données d'agrégat. Une chaîne vide, `""` collecte uniquement les données d'agrégat. Une chaîne spécifique comme `"DISKFILE"` collecte des données uniquement pour l'instance correspondante. Défini par défaut sur `"*"` s'il n'est pas spécifié.
`minReportingInterval`	Nombre entier de secondes.	Spécifie un intervalle d'agrégation par défaut à utiliser dans un rapport de données chronologiques. Fournit un contrôle plus poussé sur la granularité des rapports lorsque la granularité de l'intervalle de collecte est insuffisante. 0 est utilisé par défaut (pas d'intervalle de rapport dédié)
`aggregator`	`AVERAGE`, `MINIMUM`, `MAXIMUM` ou `SUMMATION`	Type d'agrégation à effectuer pendant l'intervalle `minReportingInterval`. Défini par défaut sur `AVERAGE` s'il n'est pas spécifié.

Configuration d'une base de données de mesures Cassandra

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

VMware Cloud Director peut collecter des mesures qui fournissent des informations actuelles et historiques sur les performances et la consommation de ressources de la machine virtuelle. Utilisez cette sous-commande pour configurer une base de données Apache Cassandra comme un référentiel de mesures VMware Cloud Director. Utilisez la sous-commande `cell-management-tool configure-metrics` pour configurer l'ensemble de mesures à collecter. Reportez-vous à la section Configuration de la collecte de mesures.

Les données des mesures historiques sont stockées dans une base de données Apache Cassandra. Pour plus d'informations sur la configuration du logiciel de base de données facultatif pour stocker et récupérer des mesures de performances, reportez-vous au Installer et configurer une base de données Cassandra pour stocker les données de mesure historiques

Pour créer une connexion entre VMware Cloud Director et une base de données Apache Cassandra, utilisez une ligne de commande au format suivant :

```
cell-management-tool cassandra options
```

Tableau 5-16. Options et arguments de l'outil de gestion des cellules, sous-commande `cassandra`

Commande	Argument	Description
`--help` (-h)	aucune	Fournit un résumé des options disponibles pour cette commande.
`--add-rollup`	Aucun	Met à jour le schéma de mesures afin d'inclure des mesures cumulées. Reportez-vous à la section Installer et configurer une base de données Cassandra pour stocker les données de mesure historiques.
`--cluster-nodes`	*adresse* [, *adresse* ...]	Liste séparée par des virgules de nœuds de clusters Cassandra à utiliser pour les mesures VMware Cloud Director.
`--clean`	Aucun	Supprimez les paramètres de configuration Cassandra de la base de données VMware Cloud Director.
`--configure`	Aucun	Configurez VMware Cloud Director pour une utilisation avec un cluster Cassandra existant.
`--dump`	Aucun	Videz la configuration de connexion actuelle.
`--keyspace`	chaîne	Définissez le nom d'espace de clés de VMware Cloud Director dans Cassandra sur *chaîne*. Réglé par défaut sur `vcloud_metrics`.
`--offline`	Aucun	Configurez Cassandra pour une utilisation par VMware Cloud Director, mais ne testez pas la configuration par une connexion à VMware Cloud Director.
`--password`	chaîne	Mot de passe d'utilisateur de base de données Cassandra
`--port`	nombre entier	Port de connexion à chaque nœud de clusters. Réglé par défaut sur 9042.
`--ttl`	Nombre entier	Conserver les données de mesures pendant *nombre entier* jours. Définissez *nombre entier* sur `0` afin de conserver les données de mesures de façon permanente.

Tableau 5-16. Options et arguments de l'outil de gestion des cellules, sous-commande `cassandra` (suite)

Commande	Argument	Description
`--update-schema`	Aucun	Initialise le schéma Cassandra pour conserver les données de mesure VMware Cloud Director.
`--username`	chaîne	Nom de l'utilisateur de la base de données Cassandra.

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

Utilisez une commande semblable à celle-ci, où *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
```

Vous devez redémarrer la cellule après l'exécution de cette commande.

Restauration du mot de passe de l'administrateur système

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

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

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

```
cell-management-toolrecover-passwordoptions
```

Tableau 5-17. Options et arguments de l'outil de gestion des cellules, sous-commande `recover-password`

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

Mettre à jour l'état d'échec d'une tâche

Utilisez la commande `fail-tasks` de l'outil de gestion des cellules pour mettre à jour l'état d'achèvement associé aux tâches que vous exécutiez lorsque la cellule a été volontairement arrêtée. Vous ne pouvez pas utiliser la commande `fail-tasks` si les cellules n'ont pas toutes été arrêtées.

Lorsque vous mettez une cellule en veille avec la commande `cell-management-tool -q`, les tâches en cours d'exécution doivent se terminer proprement en quelques minutes. Si des tâches continuent à s'exécuter sur une cellule qui a été mise au repos, le superutilisateur peut arrêter la cellule, ce qui contraint toutes les tâches restantes à se mettre en échec. Après un arrêt ayant contraint les tâches qui s'exécutaient à échouer, le superutilisateur peut exécuter `cell-management-tool fail-tasks` pour mettre à jour l'état d'achèvement de ces tâches. Ce type de mise à jour de l'état d'achèvement d'une tâche est facultatif, mais il contribue à maintenir l'intégrité des journaux système en identifiant clairement les pannes dues à une action administrative.

Pour générer la liste des tâches qui continuent à s'exécuter sur une cellule mise au repos, utilisez une ligne de commande ayant le format suivant :

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

Tableau 5-18. Options et arguments de l'outil de gestion des cellules, sous-commande `fail-tasks`

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

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

Cet exemple montre la mise à jour de l'état d'achèvement d'une tâche associé à une tâche qui était encore en cours d'exécution lorsque la cellule a été arrêtée.

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

Tapez **y** pour mettre la tâche à jour avec un état d'achèvement de type **Échec d'arrêt administratif**. Tapez **n** pour permettre à la tâche de continuer de s'exécuter.

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

Configurer le traitement des messages d'audit

Utilisez la commande `configure-audit-syslog` de l'outil de gestion de cellules pour configurer l'enregistrement des messages d'audit par le système.

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

Le script de configuration du système vous permet de spécifier le mode de traitement des messages d'audit. Reportez-vous à « Configuration des connexions au réseau et à la base de données » dans le *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*. Les options d'enregistrement que vous spécifiez pendant la configuration du système sont conservées dans deux fichiers : `global.properties` et `responses.properties`. Vous pouvez modifier la configuration de l'enregistrement des messages d'audit dans les deux fichiers avec une ligne de commande de l'outil de gestion de cellules de la forme suivante :

```
cell-management-tool configure-audit-syslog  options
```

Toutes les modifications que vous apportez avec cette sous-commande de l'outil de gestion de cellules sont conservées dans les fichiers `global.properties` et `responses.properties` de la cellule. Les modifications ne sont appliquées qu'après redémarrage de la cellule.

Tableau 5-19. Options et arguments de l'outil de gestion des cellules, sous-commande `configure-audit-syslog`

Option	Argument	Description
`--help` (-h)	aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--disable` (-d)	aucune	Désactiver l'enregistrement des événements d'audit dans `syslog`. Consigner les événements d'audit uniquement dans la base de données VMware Cloud Director. Cette option annule la définition des valeurs des propriétés `audit.syslog.host` et `audit.syslog.port` dans `global.properties` et `responses.properties`.
`--syslog-host` (-loghost)	Adresse IP ou nom de domaine complet de l'hôte du serveur syslog	Cette option définit la valeur de la propriété `audit.syslog.host` sur l'adresse ou le nom de domaine complet spécifié.
`--syslog-port` (-logport)	entier dans la plage comprise entre 0 et 65535	Cette option définit la valeur de la propriété `audit.syslog.port` sur l'entier spécifié.

Lorsque vous spécifiez une valeur pour `--syslog-host`, `--syslog-port` ou les deux, la commande confirme que la valeur spécifiée a le format approprié, mais ne teste pas la combinaison de l'hôte et du port pour l'accessibilité réseau ou la présence d'un service `syslog` en cours d'exécution.

Exemple : modifier le nom d'hôte du serveur Syslog

Important Les modifications que vous apportez en utilisant cette commande sont écrites dans le fichier de configuration globale et dans le fichier de réponses. Avant d'utiliser cette commande, veillez à ce que le fichier de réponses soit en places (dans `/opt/vmware/vcloud-director/etc/responses.properties`) et accessible en écriture. Reportez-vous à la section « Protection et réutilisation du fichier de réponses » dans le *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*.

Pour modifier l'hôte auquel les messages syslog sont envoyés, utilisez une commande semblable à celle-ci :

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool configure-audit-syslog
-loghost syslog.example.com
Using default port 514
```

Cet exemple part du principe que le nouvel hôte écoute les messages syslog sur le port par défaut.

La commande met à jour `global.properties` et `responses.properties`, mais les modifications ne sont appliquées que lorsque vous redémarrez la cellule.

Configuration des modèles d'e-mail

Pour gérer les modèles que le système utilise lors de la création d'alertes par e-mail, vous pouvez utiliser la commande `manage-email` de l'outil de gestion des cellules.

Par défaut, le système envoie des alertes par e-mail qui signalent à des administrateurs système des événements et des conditions susceptibles de nécessiter leur intervention. La liste des destinataires de l'e-mail peut être mise à jour à l'aide de VMware Cloud Director API ou de la console Web. Vous pouvez remplacer le contenu par défaut de l'e-mail pour chaque type d'alerte en utilisant une commande de l'outil de gestion de cellules au format suivant :

```
cell-management-tool manage-email  options
```

Tableau 5-20. Options et arguments de l'outil de gestion des cellules, sous-commande `manage-email`

Option	Argument	Description
`--help`	Aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--delete`	nom du modèle	Nom du modèle à supprimer.
`--lookup`	nom du modèle	Cet argument est facultatif. Si vous ne le fournissez pas, la commande renvoie la liste de tous les noms de modèles.
`--locale`	les paramètres régionaux du modèle	Par défaut, cette commande fonctionne sur les modèles définis avec les paramètres régionaux en-US. Pour spécifier des paramètres régionaux différents, utilisez cette option.
`--set-template`	nom de chemin vers un fichier contenant un modèle d'e-mail mis à jour	Ce fichier doit être accessible sur l'hôte local et lisible par l'utilisateur vcloud.vcloud. Par exemple, /tmp/my-email-template.txt

Il existe différents noms de modèles autorisés que vous pouvez utiliser pour différentes notifications par e-mail.

Tableau 5-21. Noms des notifications par e-mail VMware Cloud Director

Nom	Description	Lorsque l'e-mail est envoyé	Destinataires
VAPP_UNDEPLOY_NOTIFICATION_SUBJECT VAPP_UNDEPLOY_NOTIFICATION_BODY	Alerte lorsque le bail d'exécution du vApp est sur le point d'expirer. Lorsque le bail expire, VMware Cloud Director interrompt ou met hors tension le vApp.	Avant l'expiration du bail d'exécution d'un vApp, en fonction de la durée d'alerte configurée pour le déploiement et le bail de stockage.	Le propriétaire du vApp ou, si le propriétaire est un **administrateur système**, l'**administrateur d'organisation** reçoit la notification.
VAPP_STORAGE_NOTIFICATION_SUBJECT VAPP_STORAGE_NOTIFICATION_BODY	Alerte lorsque le bail de stockage du vApp est sur le point d'expirer. Lorsque le bail expire, VMware Cloud Director supprime le vApp.	Avant l'expiration du bail de stockage d'un vApp, en fonction de la durée d'alerte configurée pour le déploiement et le bail de stockage.	Le propriétaire du vApp ou, si le propriétaire est un **administrateur système**, l'**administrateur d'organisation** reçoit la notification.
VAPP_STORAGE_NOTIFICATION_FAILURE_SUBJECT VAPP_STORAGE_NOTIFICATION_BODY	Alerte lorsque le bail de stockage du vApp est sur le point d'expirer. Lorsque le bail expire, VMware Cloud Director marque le vApp comme ayant expiré.	Avant l'expiration du bail de stockage d'un vApp, en fonction de la durée d'alerte configurée pour le déploiement et le bail de stockage.	Le propriétaire du vApp ou, si le propriétaire est un **administrateur système**, l'**administrateur d'organisation** reçoit la notification.
VAPPTEMPLATE_STORAGE_NOTIFICATION_SUBJECT VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY	Alerte lorsque le bail de stockage du modèle de vApp est sur le point d'expirer. Lorsque le bail expire, VMware Cloud Director supprime le modèle de vApp.	Avant l'expiration du bail de stockage d'un modèle de vApp, en fonction de la durée d'alerte configurée pour le déploiement et le bail de stockage.	Le propriétaire du modèle de vApp ou, si le propriétaire est un **administrateur système**, l'**administrateur d'organisation**, reçoit la notification.
VAPPTEMPLATE_STORAGE_NOTIFICATION_FAILURE_SUBJECT VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY	Alerte lorsque le bail de stockage du modèle de vApp est sur le point d'expirer. Lorsque le bail expire, VMware Cloud Director marque le modèle de vApp comme ayant expiré.	Avant l'expiration du bail de stockage d'un modèle de vApp, en fonction de la durée d'alerte configurée pour le déploiement et le bail de stockage.	Le propriétaire du modèle de vApp ou, si le propriétaire est un **administrateur système**, l'**administrateur d'organisation** reçoit la notification.
DISK_STORAGE_ALERT	Alerte de stockage sur disque (alerte rouge)	Lorsque l'espace disque de la banque de données est faible et qu'il atteint le seuil rouge.	**Administrateurs système**
DISK_STORAGE_ALERT_VDCS	Alerte de stockage sur disque envoyée aux VDC fournisseurs. L'e-mail contient la liste des VDC fournisseurs utilisant la banque de données qui présente une alerte rouge en raison d'un espace disque faible.	Lorsque l'espace disque de la banque de données est faible et qu'il atteint le seuil rouge.	**Administrateurs système**

Tableau 5-21. Noms des notifications par e-mail VMware Cloud Director (suite)

Nom	Description	Lorsque l'e-mail est envoyé	Destinataires
VM_HW_UPGRADE_INVALID_POWER_STATE VM_UPDATE_NESTED_HV_INVALID_POWER_STATE	Notification sur l'état d'alimentation d'une machine virtuelle. Pour mettre à niveau le matériel virtuel, vous devez mettre la machine virtuelle hors tension.	Lorsqu'un utilisateur tente de mettre à niveau la version du matériel d'une machine virtuelle.	Le propriétaire de la machine virtuelle ou, si le propriétaire est un **administrateur système**, l'**administrateur d'organisation** reçoit la notification.
FEDERATION_CERTIFICATE_SUCCESS_EXPIRY FEDERATION_CERTIFICATE_SUCCESS_EXPIRY	Notification d'expiration du certificat de fédération envoyée à tous les **administrateurs d'organisation** lorsqu'un certificat d'un serveur SSO externe est sur le point d'expirer. Il invite les **administrateurs d'organisation** à télécharger un nouveau certificat depuis le serveur SSO et à mettre à jour VMware Cloud Director.	Un certificat de fédération expire dans les 7 jours à partir de la date actuelle.	**Administrateurs de l'organisation**
IPSEC_VPN_TUNNEL_ERROR IPSEC_VPN_TUNNEL_ERROR_SUMMARY	Erreur de tunnel VPN (alerte rouge)	Lorsque le tunnel VPN n'est pas opérationnel.	**Administrateurs système**
IPSEC_VPN_TUNNEL_ENABLED IPSEC_VPN_TUNNEL_ENABLED _SUMMARY	Tunnel VPN activé (alerte verte)	Lorsque le tunnel VPN fonctionne à nouveau après ne pas avoir été opérationnel.	**Administrateurs système**

Tableau 5-22. Modèles d'e-mail non personnalisables

Notification	Lorsque l'e-mail est envoyé	Destinataires
Alerte par e-mail en cas de système vCenter Server reconnecté	Lorsqu'un système vCenter Server est reconnecté.	**Administrateurs système**
Alerte par e-mail en cas de déconnexion du système vCenter Server. L'e-mail indique si une erreur ou une demande utilisateur a entraîné la déconnexion du système vCenter Server.	Lorsqu'un système vCenter Server est déconnecté.	**Administrateurs système**
Alerte par e-mail en cas de perte de la connexion AMQP. Alerte informant que VMware Cloud Director est déconnecté du serveur AMQP.	Lorsque RabbitMQ cesse de fonctionner.	**Administrateurs système**
Alerte par e-mail en cas de connexion interrompue à la base de données	Lorsque VMware Cloud Director est déconnecté de la base de données.	**Administrateurs système**

Tableau 5-22. Modèles d'e-mail non personnalisables (suite)

Notification	Lorsque l'e-mail est envoyé	Destinataires
Alerte par e-mail en cas de restauration de la connexion à la base de données	Lorsque VMware Cloud Director est reconnecté à la base de données.	**Administrateurs système**
Alerte par e-mail en cas de déconnexion de l'hôte du commutateur	Un hôte est déconnecté des commutateurs disponibles.	**Administrateurs système**
Alerte par e-mail en cas de déconnexion de l'hôte du commutateur virtuel distribué	Un hôte est déconnecté des commutateurs virtuels distribués disponibles.	**Administrateurs système**
Alerte par e-mail en cas d'erreur LDAP	Pendant la synchronisation avec LDAP.	**Administrateurs système**
Alerte par e-mail lors de la synchronisation des utilisateurs LDAP	Lors du changement de nom d'un utilisateur LDAP.	**Administrateurs système**
Alerte par e-mail en cas de changement d'état des associations de sites	Les sites ont récemment perdu la connexion, ont récupéré la connexion ou sont toujours inactifs.	**Administrateurs système**

Exemple : Mettre à jour un modèle d'e-mail

La commande suivante remplace le contenu actuel du modèle d'e-mail DISK_STORAGE_ALERT par le contenu que vous avez créé dans un fichier nommé `/tmp/DISK_STORAGE_ALERT_VDCS-new.txt`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-email --set-
template DISK_STORAGE_ALERT_VDCS /tmp/DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s):
$pvdcsList
"
Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from
$productName The $datastore is used by the followingProvider VDC(s): $pvdcsList
"

VCD Email notification details:
 name                     : DISK_STORAGE_ALERT_VDCS
 description              : Alert when used disk storage exceeds threshold
 config key               : email.template.DISK_STORAGE_ALERT_VDCS.en-US
 template placeholders    : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcsList]
 template content         : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcsList
```

Rechercher des machines virtuelles orphelines

Utilisez la commande `find-orphan-vms` de l'outil de gestion de cellules pour rechercher des références à des machines virtuelles présentes dans la base de données vCenter mais pas dans la base de données VMware Cloud Director.

Les machines virtuelles référencées dans la base de données vCenter mais pas dans la base de données VMware Cloud Director sont considérées comme des machines virtuelles orphelines, car VMware Cloud Director ne peut pas y accéder même si elles peuvent consommer des ressources de calcul et de stockage. Ce type d'inadéquation de référence peut survenir pour diverses raisons, notamment des volumes élevés de charge de travail, des erreurs de base de données et des actions administratives. La commande `find-orphan-vms` permet à un administrateur de répertorier ces machines virtuelles afin qu'elles puissent être retirées de VMware Cloud Director ou y être réimportées. Cette commande permet la spécification d'un autre magasin d'approbations, pouvant être requis si vous travaillez avec des installations VMware Cloud Director ou vCenter qui utilisent des certificats auto-signés.

Utilisez une commande du format suivant :

```
cell-management-toolfind-orphan-vms options
```

Tableau 5-23. Options et arguments de l'outil de gestion des cellules, sous-commande `find-orphan-vms`

Option	Argument	Description
`--help` (-h)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--enableVerifyHostname`	Aucun	Activer la partie de vérification du nom d'hôte de la négociation SSL.
`--host`	Obligatoire	Adresse IP ou nom de domaine complet de l'installation VMware Cloud Director dans laquelle rechercher des machines virtuelles orphelines.
`--output-file`	nom de chemin ou –	Nom de chemin complet du fichier dans lequel la liste des machines virtuelles orphelines doit être écrite. Spécifiez le nom de chemin – pour écrire la liste vers la sortie standard.
`--password` (-p)	Obligatoire	Mot de passe de l'administrateur système VMware Cloud Director.
`--port`	Port HTTPS de VMware Cloud Director.	Spécifiez cette option uniquement si vous ne souhaitez pas que cette commande utilise le port HTTPS par défaut de VMware Cloud Director.

Tableau 5-23. Options et arguments de l'outil de gestion des cellules, sous-commande `find-orphan-vms` (suite)

Option	Argument	Description
`--trustStore`	Nom de chemin complet vers un fichier de magasin d'approbations Java.	Spécifiez cette option uniquement si vous ne souhaitez pas que cette commande utilise le fichier de magasin d'approbations VMware Cloud Director par défaut.
`--trustStorePassword`	Mot de passe du `--trustStore` spécifié	Requis uniquement si vous utilisez `--trustStore` pour spécifier un autre fichier de magasin d'approbations.
`--trustStoreType`	Le type du `--trustStore` spécifié (PKCS12, JCEKS, ...)	Requis uniquement si vous utilisez `--trustStore` pour spécifier un autre fichier de magasin d'approbations.
`--user` (-u)	Obligatoire	Nom d'utilisateur de l'administrateur système VMware Cloud Director
`--vc-name`	Obligatoire	Nom de l'instance de vCenter dans laquelle rechercher des machines virtuelles orphelines.
`--vc-password`	Obligatoire	Mot de passe de l'administrateur vCenter.
`--vc-user`	Obligatoire	Nom d'utilisateur de l'administrateur vCenter.

Exemple : Rechercher des machines virtuelles orphelines

Cet exemple interroge une seule instance de vCenter Server. Comme `--output-file` est spécifié sous la forme -, les résultats sont renvoyés sur la sortie standard.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vms \
 --host 10.20.30.40 -u vcadmin -vc-name vcenter1 -vc-password P@55w0rd --vc-user admin --
output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc<->resource pool mappings associated with VC: 10.20.30.40 (https://
10.20.30.40:443)
Querying all vdc<->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...)
[moref: "resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test
```

```
VMs", parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test
VMs", parent moref : "group-v30533")
```

Rejoindre ou quitter le programme d'amélioration du produit VMware

Pour rejoindre ou quitter le Programme d'amélioration du produit (CEIP) VMware, vous pouvez utiliser la sous-commande `configure-ceip` de l'outil de gestion des cellules.

Ce produit participe au Programme d'amélioration du produit VMware du (« CEIP »). 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.

```
cell-management-tool
configure-ceip
options
```

Si vous préférez ne pas participer au Programme d'amélioration du produit VMware pour ce produit, exécutez cette commande avec l'option `--disable`.

Tableau 5-24. Options et arguments de l'outil de gestion des cellules, sous-commande `configure-ceip`

Option	Argument	Description
`--help` (`-h`)	Aucun	Fournit un résumé des commandes disponibles dans cette catégorie.
`--disable`	Aucun	Quitte le Programme d'amélioration du produit VMware.
`--enable`	Aucun	Rejoint le Programme d'amélioration du produit VMware.
`--status`	Aucun	Affiche l'état de participation actuelle dans le Programme d'amélioration du produit VMware.

Exemple : Quitter le programme d'amélioration du produit VMware

Pour quitter le Programme d'amélioration du produit VMware, utilisez une commande semblable à celle-ci :

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
disableParticipation disabled
```

Après l'exécution de cette commande, le système n'envoie plus d'informations au programme d'amélioration du produit VMware.

Pour confirmer l'état actuel de participation dans le Programme d'amélioration du produit VMware, utilisez une commande semblable à celle-ci :

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
statusParticipation disabled
```

Mise à jour des paramètres de configuration des applications

Avec la sous-commande `manage-config` de l'outil de gestion des cellules, vous pouvez mettre à jour les paramètres de configuration de différentes applications, tels que les limitations de catalogue.

Tableau 5-25. Options et arguments de l'outil de gestion des cellules, sous-commande `manage-config`

Option	Argument	Description
`--help` (`-h`)	Aucun	Fournit un résumé des options disponibles avec cette sous-commande.
`--delete` (`-d`)	Aucun	Supprime le paramètre de configuration cible.
`--lookup` (`-l`)	Aucun	Recherchez la valeur du paramètre de configuration cible.
`--name` (`-n`)	Nom du paramètre de configuration	Le nom du paramètre de configuration cible. Requis avec les options `-d`, `-l` et `-v`.
`--value` (`-v`)	Valeur du paramètre de configuration	Ajoute ou met à jour la valeur du paramètre de configuration cible.

Par exemple, vous pouvez utiliser la sous-commande `manage-config` pour Configuration de la limite de synchronisation du catalogue.

Configuration de la limite de synchronisation du catalogue

Lorsque vous disposez de nombreux éléments du catalogue publiés ou auxquels d'autres organisations sont abonnées, pour éviter de surcharger le système pendant les synchronisations du catalogue, vous pouvez configurer une limite de synchronisation du catalogue. Vous pouvez utiliser la sous-commande `manage-config` de l'outil de gestion des cellules pour configurer une limite de synchronisation du catalogue en limitant le nombre d'éléments de bibliothèque qui peuvent être synchronisés en même temps.

Lorsqu'un catalogue abonné initie une synchronisation du catalogue, le catalogue publié télécharge d'abord les éléments de bibliothèque à partir du référentiel de vCenter Server vers le stockage du service de transfert de VMware Cloud Director, puis crée des liens de téléchargement pour le catalogue abonné. Vous pouvez limiter le nombre d'éléments de bibliothèque que l'ensemble des catalogues publiés peuvent télécharger en même temps. Vous pouvez limiter le nombre d'éléments de bibliothèque que l'ensemble des catalogues abonnés peuvent synchroniser en même temps. Vous pouvez limiter le nombre d'éléments de bibliothèque qu'un catalogue abonné unique peut synchroniser en même temps.

Vous pouvez utiliser la sous-commande `manage-config` de l'outil de gestion des cellules pour mettre à jour les paramètres de configuration pour la limitation des catalogues. Pour obtenir des informations sur l'utilisation de la sous-commande `manage-config`, reportez-vous à la section Mise à jour des paramètres de configuration des applications.

Tableau 5-26. Paramètres de configuration pour la limite de catalogues

Paramètre de configuration	Valeur par défaut	Description
`vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit`	30	La limite des éléments de bibliothèque que l'ensemble des catalogues publiés de l'instance de VMware Cloud Director peut télécharger de vCenter Server vers VMware Cloud Director en même temps. Si le nombre total d'éléments de bibliothèque publiés à télécharger depuis l'instance de VMware Cloud Director est supérieur à cette limite, les éléments de bibliothèque sont divisés en plusieurs parties respectant cette limite et téléchargés en séquence.
`vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit`	30	Limite des éléments de bibliothèque que l'ensemble des catalogues abonnés d'une instance de VMware Cloud Director peut synchroniser en même temps. Si le nombre total d'éléments de bibliothèque abonnés à synchroniser depuis l'instance de VMware Cloud Director est supérieur à cette limite, les éléments sont divisés en plusieurs parties respectant cette limite et synchronisés en séquence.
`contentLibrary.item.sync.batch.size`	10	Nombre maximal d'éléments de bibliothèque qu'un catalogue abonné unique peut synchroniser en même temps. Si un catalogue abonné tente de synchroniser un nombre d'éléments de bibliothèque qui est supérieur à cette limite, les éléments sont divisés en plusieurs parties respectant cette limite et synchronisés en séquence.

Exemple : Configuration de la limite de synchronisation pour les catalogues abonnés

La commande suivante définit une limite maximale de cinq éléments de bibliothèque qu'un catalogue abonné unique peut synchroniser en même temps.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
contentLibrary.item.sync.batch.size -v 5
```

Si un catalogue abonné contient 13 éléments de bibliothèque, la synchronisation du catalogue s'effectue en une séquence de trois parties. La première partie contient cinq éléments, la deuxième partie contient les cinq éléments suivants et la dernière partie contient les trois éléments restants.

Résoudre les problèmes d'échec d'accès à l'interface utilisateur de VMware Cloud Director

Pour afficher et mettre à jour les adresses IP et les entrées DNS valides pour les cellules VMware Cloud Director dans votre environnement VMware Cloud Director, vous pouvez utiliser la sous-commande `manage-config` de l'outil de gestion des cellules.

Problème

Vous ne pouvez pas accéder au VMware Cloud Director Service Provider Admin Portal ou au VMware Cloud Director Tenant Portal après une connexion réussie.

Après avoir entré vos informations d'identification sur l'écran de connexion, le message d'erreur suivant s'affiche : `Échec du démarrage. Une erreur s'est produite lors de l'initialisation. Cela peut être dû à des problèmes tels que l'accès à l'application via une URL publique non prise en charge ou à des problèmes de mauvaise connexion.`

Cause

VMware Cloud Director utilise une implémentation de filtre CORS (Cross-Origin Resource Sharing) pour conserver une liste de tous les points de terminaison valides que vous pouvez utiliser pour accéder au Service Provider Admin Portal et au VMware Cloud Director Tenant Portal.

La liste de filtrage CORS est remplie et mise à jour lors de la configuration de la cellule. Elle contient des entrées HTTP et HTTPS avec des adresses IP et des noms DNS pour toutes les cellules du groupe de serveurs. Elle contient également une adresse IP publique qui est utilisée par l'équilibrage de charge placé devant le groupe de serveurs VMware Cloud Director.

Lors de la configuration des cellules des déploiements de dispositifs, la liste n'est pas mise à jour avec les noms DNS des cellules VMware Cloud Director et vous ne pouvez pas utiliser le nom DNS d'une cellule pour y accéder.

Solution

1. Connectez-vous ou ouvrez une session SSH en tant qu'utilisateur **racine** à l'une des cellules du groupe de serveurs.
2. Pour répertorier les URL valides que vous pouvez utiliser pour accéder aux cellules VMware Cloud Director dans votre environnement, exécutez la ligne de commande suivante.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -l
```

La sortie système est une liste qui contient des entrées HTTP et HTTPS avec des adresses IP et des noms DNS pour toutes les cellules du groupe de serveurs. Elle contient également une adresse IP publique qui est utilisée par l'équilibrage de charge placé devant le groupe de serveurs VMware Cloud Director.

La liste est une chaîne séparée par des virgules, sans espace entre les entrées.

3 (Facultatif) Pour mettre à jour le paramètre de configuration `webapp.allowed.origins`, exécutez la ligne de commande suivante. Dans la ligne de commande, le paramètre de valeur du paramètre est une liste d'adresses IP et de noms DNS dans une chaîne séparée par des virgules, sans espace entre les entrées.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

Débogage de la découverte de machines virtuelles vCenter

La sous-commande `debug-auto-import` de l'outil de gestion des cellules vous permet de déterminer la raison pour laquelle le mécanisme de découverte des vApp ignore une ou plusieurs machines virtuelles vCenter.

Dans la configuration par défaut, un VDC d'organisation découvre automatiquement les machines virtuelles vCenter créées dans un pool de ressources supportant le VDC. Reportez-vous aux informations sur la découverte et l'adoption de vApp dans *Guide du portail d'administration des fournisseurs de services VMware Cloud Director*. Si une machine virtuelle vCenter n'apparaît pas dans un vApp découvert, vous pouvez exécuter la sous-commande `debug-auto-import` pour la machine virtuelle ou le VDC.

```
cell-management-tool debug-auto-import options
```

La sous-commande `debug-auto-import` renvoie la liste des machines virtuelles vCenter et des informations sur les raisons possibles pour lesquelles le mécanisme de découverte les ignore. La liste inclut également les machines virtuelles vCenter découvertes, mais dont l'importation vers le VDC d'organisation a échoué.

Tableau 5-27. Options et arguments de l'outil de gestion des cellules, sous-commande `debug-auto-import`

Option	Argument	Description
`--help` (`-h`)	aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--org`	Nom de l'organisation	Facultatif. Répertorie des informations sur les machines virtuelles ignorées pour l'organisation spécifiée.
`--vm`	Nom ou partie d'un nom de machine virtuelle	Répertorie des informations sur les machines virtuelles ignorées qui contiennent le nom de machine virtuelle spécifié. Facultatif si l'option `--org` est utilisée.

Exemple : Débogage de la découverte de machines virtuelles vCenter pour le nom de machine virtuelle `test`

La commande suivante renvoie des informations sur les machines virtuelles vCenter ignorées sur toutes les organisations.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc
can be skipped for the following reasons:
1) Virtual machine is already imported in vCD or is managed by vCD
2) Virtual machine is created by vCD

VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc
can be skipped for the following reasons:
1) Virtual machine is not present in a vCD managed resource pool

VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry
```

Dans cet exemple, la sortie système renvoie des informations sur les trois machines virtuelles vCenter ignorées par le mécanisme de découverte et dont les noms contiennent la chaîne `test`. La machine virtuelle `importation test3` est un exemple de machine virtuelle découverte, mais dont l'importation vers le VDC échoue.

Régénération des adresses MAC pour les réseaux étirés multisites

Si vous associez deux sites VMware Cloud Director qui sont configurés avec le même ID d'installation, vous pouvez rencontrer des conflits d'adresses MAC dans les réseaux étirés entre

ces sites. Pour éviter de tels conflits, vous devez régénérer les adresses MAC d'un des sites en se basant sur une valeur initiale personnalisée qui est différente de l'ID d'installation.

Au cours de la configuration initiale de VMware Cloud Director, vous définissez un ID d'installation. VMware Cloud Director utilise l'ID d'installation pour générer des adresses MAC pour les interfaces réseau de la machine virtuelle. Deux installations de VMware Cloud Director configurées avec le même ID d'installation peuvent générer des adresses MAC identiques. Des adresses MAC en double peuvent générer des conflits dans les réseaux étirés entre deux sites associés.

Avant la création de réseaux étirés entre des sites associés qui sont configurés avec le même ID d'installation, vous devez régénérer les adresses MAC d'un des sites à l'aide de la sous-commande `mac-address-management` de l'outil de gestion des cellules.

```
cell-management-tool mac-address-management options
```

Pour générer de nouvelles adresses MAC, vous définissez une valeur initiale personnalisée qui est différente de l'ID d'installation. La valeur initiale ne remplace pas l'ID d'installation, mais la base de données stocke la dernière valeur initiale sous la forme d'un deuxième paramètre de configuration, qui remplace l'ID d'installation.

Vous exécutez la sous-commande `mac-address-management` depuis un membre VMware Cloud Director arbitraire du groupe de serveurs. La commande s'exécute sur la base de données de VMware Cloud Director, vous devez donc exécuter la commande une fois par groupe de serveurs.

Important La régénération des adresses MAC requiert une interruption de service de VMware Cloud Director. Avant de commencer la régénération, vous devez suspendre les activités sur toutes les cellules du groupe de serveurs.

Tableau 5-28. Options et arguments de l'outil de gestion des cellules, sous-commande `mac-address-management`

Option	Argument	Description
`--help` (`-h`)	Aucune	Fournit un résumé des commandes disponibles dans cette catégorie.
`--regenerate`	Aucun	Supprime toutes les adresses MAC qui ne sont pas en cours d'utilisation et génère de nouvelles adresses MAC en se basant sur la valeur initiale actuelle. Si aucune valeur initiale n'est définie, les adresses MAC sont régénérées en se basant sur l'ID d'installation. Les adresses MAC en cours d'utilisation sont conservées. **Note** Toutes les cellules du groupe de serveurs doivent être inactives. Pour plus d'informations sur la mise au repos des activités sur une cellule, reportez-vous à la section Gestion d'une cellule.
`--regenerate-with-seed`	Valeur initiale comprise entre 0 et 63	Définit une nouvelle valeur initiale personnalisée dans la base de données, supprime toutes les adresses MAC qui ne sont pas en cours d'utilisation et génère de nouvelles adresses MAC en se basant sur la nouvelle valeur initiale. Les adresses MAC en cours d'utilisation sont conservées. **Note** Toutes les cellules du groupe de serveurs doivent être inactives. Pour plus d'informations sur la mise au repos des activités sur une cellule, reportez-vous à la section Gestion d'une cellule.
`--show-seed`	Aucun	Renvoie la valeur initiale actuelle et le nombre d'adresses MAC en cours d'utilisation pour chaque valeur initiale.

Important Les adresses MAC en cours d'utilisation sont conservées. Pour basculer d'une adresse MAC en cours d'utilisation vers une adresse MAC régénérée, vous devez réinitialiser l'adresse MAC de l'interface réseau. Pour plus d'informations sur la modification des propriétés d'une machine virtuelle, reportez-vous à la section *Guide du portail de locataires de VMware Cloud Director*.

Exemple : Régénération des adresses MAC en se basant sur une nouvelle valeur initiale personnalisée

La commande suivante définit la valeur initiale actuelle sur *9* et régénère toutes les adresses MAC qui ne sont pas en cours d'utilisation en se basant sur la nouvelle valeur initiale :

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

Exemple : Affichage de la valeur initiale actuelle et du nombre d'adresses MAC en cours d'utilisation pour chaque valeur initiale

La commande suivante renvoie des informations sur la valeur initiale actuelle et le nombre d'adresses MAC par valeur initiale :

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by     12 MAC addresses
MAC address seed    1 is in use by      1 MAC addresses
```

Dans cet exemple, la sortie système indique que la valeur initiale actuelle est 9, sur laquelle il existe 12 adresses MAC. En outre, il existe une adresse MAC qui est basée sur une valeur initiale précédente ou sur un ID d'installation de 1.

Mettre à jour les adresses IP de la base de données sur des cellules VMware Cloud Director

Pour mettre à jour les adresses IP des cellules VMware Cloud Director dans un cluster haute disponibilité d'une base de données, vous pouvez utiliser l'outil de gestion des cellules.

Conditions préalables

Pour mettre à jour les adresses IP des cellules dans un cluster haute disponibilité de base de données, vous devez fournir l'adresse IP du nœud principal actuel. Pour trouver l'adresse IP, vous devez utiliser l'API du dispositif VMware Cloud Director pour noter les ID des nœuds en veille du cluster. Reportez-vous à la section *Référence de schéma de l'API du dispositif VMware Cloud Director* sur http://code.vmware.com.

Procédure

1 Connectez-vous, directement ou à l'aide d'un client SSH, au système d'exploitation de l'une des cellules du cluster en tant que **racine**.

2 Vérifiez si la cellule est en cours d'exécution sur ce nœud.

```
service vmware-vcd pid cell
```

Si l'ID de processus de cellule n'est pas NULL, la cellule VMware Cloud Director est en cours d'exécution et vous pouvez modifier l'adresse IP de la base de données sans redémarrer la cellule VMware Cloud Director.

3 Pour mettre à jour les adresses IP sur toutes les cellules du groupe de serveurs, exécutez la commande suivante :

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address --pid cell process ID --remote-sudo-user postgres --private-key-path /opt/vmware/vcloud-director/id_rsa
```

La sortie du système indique que la reconfiguration a réussi.

4 (Facultatif) Vérifiez que chaque cellule VMware Cloud Director pointe vers l'adresse IP de base de données appropriée.

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

La sortie système indique que la cellule est mise à jour.

5 Si l'une des cellules n'est pas mise à jour, exécutez la commande pour la reconfigurer.

- Si la cellule n'est pas en cours d'exécution, exécutez la commande suivante :

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address
```

- Si la cellule est en cours d'exécution, exécutez la commande suivante :

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address -i cell process ID
```

6 Si vous avez reconfiguré une cellule qui n'est pas en cours d'exécution, exécutez la commande pour redémarrer le service `vmware-vcd`.

a Exécutez la commande pour arrêter le service.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

b Exécutez la commande pour démarrer le service.

```
systemctl start vmware-vcd
```

Collecter les journaux VMware Cloud Director

6

VMware Cloud Director fournit des informations de journalisation pour chaque cellule de cloud de votre groupe de serveurs. Vous pouvez afficher les journaux pour surveiller vos cellules et résoudre les problèmes que vous rencontrez pendant l'exécution quotidienne de VMware Cloud Director.

Journaux VMware Cloud Director

Fichier ou répertoire de nom de journal	Description
`/opt/vmware/vcloud-director/logs/cell.log`	Sortie de console de la cellule VMware Cloud Director.
`/opt/vmware/vcloud-director/logs/cell-management-tool`	Messages du journal de l'outil de gestion des cellules à partir de la cellule.
`/opt/vmware/vcloud-director/logs/cell-runtime`	Messages du journal d'exécution à partir de la cellule.
`/opt/vmware/vcloud-director/logs/cloud-proxy`	Messages du journal du serveur proxy du Cloud à partir de la cellule.
`/opt/vmware/vcloud-director/logs/console-proxy`	Messages du journal du serveur proxy de la console distante à partir de la cellule.
`/opt/vmware/vcloud-director/logs/server-group-communications`	Communications du groupe de serveur à partir de la cellule.
`/opt/vmware/vcloud-director/logs/statsfeeder`	Récupération de mesures de machines virtuelles depuis vCenter Server, informations sur le stockage et message d'erreur.
`/opt/vmware/vcloud-director/logs/vcloud-container-debug.log`	Messages du journal de niveau débogage à partir de la cellule.
`/opt/vmware/vcloud-director/logs/vcloud-container-info.log`	Messages du journal d'information à partir de la cellule. Ce journal affiche aussi les avertissements ou les erreurs rencontrés par la cellule.
`/opt/vmware/vcloud-director/logs/vmware-vcd-watchdog.log`	Messages du journal d'information à partir de la surveillance de la cellule. Il enregistre le moment où la cellule cesse de répondre, redémarre, etc.

Fichier ou répertoire de nom de journal	Description
`/opt/vmware/vcloud-director/logs/diagnostics.log`	Journal de diagnostic de la cellule. Ce fichier est vide, sauf si la journalisation de diagnostics est activée dans la configuration de la journalisation locale.
`/opt/vmware/vcloud-director/logs/`*`YYYY_MM_DD`*`.request.log`	Journalisation des demandes HTTP au format de journal courant Apache.

Journaux du dispositif VMware Cloud Director

Le dispositif VMware Cloud Director offre des fichiers journaux supplémentaires.

Fichier journal	Description
`/opt/vmware/var/log/firstboot`	Contient des informations de journalisation liées au premier démarrage du dispositif.
`/opt/vmware/var/log/vcd`	Contient des journaux liés à la configuration de la suite d'outils Replication Manager (`repmgr`), à la reconfiguration et à la synchronisation du dispositif.
`/opt/vmware/var/log/vcd/pg`	Contient des journaux liés à la sauvegarde de la base de données de dispositif intégrée.
`/opt/vmware/etc/vami/ovfEnv.xml`	Contient les paramètres de déploiement OVF.
`/var/vmware/vpostgres/current/pgdata/log`	Contient des journaux liés à la base de données PostgreSQL intégrée.
`/opt/vmware/var/log/vami/updatecli.log`	Contient une journalisation liée aux mises à niveau du dispositif.

Utilisez n'importe quel éditeur de texte, visionneuse de texte ou outil tiers pour afficher les journaux.

Désinstallation du logiciel VMware Cloud Director 7

Utilisez la commande Linux `rpm` pour désinstaller le logiciel VMware Cloud 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 VMware Cloud Director.