

VMware Cloud Director Availability

Guides sur site

Guide n° 19
Dépannage

Vous trouverez la documentation technique la plus à jour sur le site Web VMware à l'adresse : <https://docs.vmware.com/>
Si vous avez des commentaires sur cette documentation, envoyez vos commentaires à : vcav-light@vmware.com

Problèmes de synchronisation des répliquions

Si la répliquion est configurée, mais que la synchronisation reste à 0 %, vérifiez la connectivité réseau entre les hôtes ESXi et le répliquion. Vérifiez les routes réseau si elles existent, vérifiez les pare-feu et les ports réseau responsables des communications réseau. Pour plus d'informations, cliquez sur ce lien :

- <https://ports.vmware.com/home/VMware-Cloud-Director-Availability>
- <https://docs.vmware.com/fr/VMware-Cloud-Director-Availability/4.3/VMware-Cloud-Director-Availability-Install-Config-Upgrade-On-Prem/GUID-B60E073E-D857-4B6E-B17B-3978C3F7874B.html>

Vérifier la connectivité entre le répliquion et les hôtes ESXi

Ouvrez une session SSH sur le dispositif répliquion et exécutez les commandes suivantes pour chaque hôte ESXi, en remplaçant l'adresse IP par celle de chaque hôte ESXi :

```
</dev/tcp/192.168.113.11/80 ; echo $?
</dev/tcp/192.168.113.11/902 ; echo $?
```

Si la connexion est opérationnelle, la sortie indique « 0 » (zéro). En l'absence de connectivité sur un port réseau spécifique, la commande génère les éléments suivants :

```
root@onprem01 [ ~ ]# </dev/tcp/192.168.113.11/902 ; echo $?
-bash: connect: Connection timed out
-bash: /dev/tcp/192.168.113.11/902: Connection timed out
1
```

Si la connexion expire pour l'un des ports réseau, vérifiez la connectivité réseau entre le répliquion et l'hôte ESXi en consultant les routes réseau et les pare-feu. Dans l'interface utilisateur de vSphere, vérifiez les paramètres de pare-feu d'un hôte ESXi :

The screenshot shows the vSphere configuration interface for a host's firewall. The 'Configure' tab is active, and the 'Firewall' section is expanded. A table lists various services and their associated ports. The 'NFC' and 'vSphere Web Access' rows are highlighted with orange boxes.

Nom du service	Ports TCP	Ports UDP	Adresses IP autorisées
CIM Server	5988	--	Tous
CIM Secure Server	5989	--	Tous
CIM SLP	427	427	Tous
DHCPv6	546	546	Tous
DVSSync	--	8301, 8302	Tous
NFC	902	--	Tous
DHCP Client	--	68	Tous
Fault Tolerance	8300	--	Tous
iofiltervp	9080	--	Tous
SNMP Server	--	161	Tous
SSH Server	22	--	Tous
VMotion	8000	--	Tous
vSphere Web Client	443, 902	--	Tous
vSphere Web Access	80	--	Tous

Vérification de la connectivité entre un hôte ESXi et le réplicateur

Ouvrez une connexion SSH et exécutez la commande suivante :

```
[root@esx01:~] nc -zv 192.168.2.11 44046
Connection to 192.168.2.11 44046 port [tcp/*] succeeded!
```

En cas d'échec de la vérification de la connexion, vérifiez la connectivité réseau entre l'hôte ESXi et le réplicateur en consultant les routes réseau et les pare-feu.

Problèmes liés à Lookup Service

Lorsque la connectivité de Lookup Service n'est pas opérationnelle, consultez les articles de connectivité suivants :

- <https://ports.vmware.com/home/VMware-Cloud-Director-Availability>
- <https://docs.vmware.com/fr/VMware-Cloud-Director-Availability/4.3/VMware-Cloud-Director-Availability-Install-Config-Upgrade-On-Prem/GUID-B60E073E-D857-4B6E-B17B-3978C3F7874B.html>

En l'absence de problèmes de connectivité, vérifiez les certificats d'une ou de plusieurs instances de Platform Services Controller et de vCenter Server dans la base de données de Lookup Service.

1. Pour collecter le certificat de vCenter Server, exécutez la commande suivante, en remplaçant l'adresse IP ou le nom de domaine complet de vCenter Server :

```
openssl s_client -connect 192.168.113.201:443 </dev/null 2>/dev/null
```

La sortie de la commande est la suivante :

```
root@onprem01 [ ~ ]# openssl s_client -connect 192.168.113.201:443 </dev/null 2>/dev/null
CONNECTED(00000003)

Certificate chain
 0 s:/CN=192.168.113.201/C=US
   i:/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=localhost/OU=VMware Engineering
---
Server certificate
-----BEGIN CERTIFICATE-----
MIID3jCCAsagAwIBAgIJAPkNzNYD5w+PMA0GCSqGSIb3DQEBCwUAMIGQMqswCQYD
...
...
8+dZL/uaDBLSnZUmfgbt03VSIcUR9ItYFj+ZBuijF6yuA1cHoxfoiLEn7/Uy17kc
d049AaXE/A0xd8J5TNYhXvWCNYhjTV00Vxf9sL/wTyJxDg==
-----END CERTIFICATE-----
subject=/CN=192.168.113.201/C=US

issuer=/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=localhost/OU=VMware Engineering
```

2. Dans un navigateur, ouvrez l'adresse de Platform Services Controller à l'aide du chemin d'accès « `/lookupservice/mob?moid=ServiceRegistration&method=List` » et remplacez l'adresse IP par l'adresse IP ou le nom de domaine complet de Platform Services Controller.

Remarque : L'adresse IP de Platform Services Controller peut être la même que celle de vCenter Server ou varier selon les spécificités de l'environnement.

```
https://192.168.113.201/lookupservice/mob?moid=ServiceRegistration&method=List
```

3. Fournissez les informations d'identification SSO.
4. Dans le champ Valeur, collez le code suivant :

Managed Object Type: **LookupServiceRegistration**
Managed Object ID: **ServiceRegistration**
Method: **List**

ArrayOfLookupServiceRegistrationInfo List

Parameters

NAME	TYPE	VALUE
filterCriteria (optional)	LookupServiceRegistrationFilter	<pre><filterCriteria> <serviceType> <product>com.vmware.cis</product> <type>vcenterserver</type> </serviceType> </filterCriteria></pre>

[Invoke Method](#)

```
<filterCriteria>
  <serviceType>
    <product>com.vmware.cis</product>
    <type>vcenterserver</type>
  </serviceType>
</filterCriteria>
```

5. Sur la page, recherchez **sslTrust** et comparez le certificat affiché à celui collecté à l'aide de la commande **openssl**. Si les deux certificats ne correspondent pas, le support vCenter doit mettre à jour les certificats dans Lookup Service.

Problèmes de couplage avec un site cloud

Lorsque vous rencontrez des problèmes de couplage à un site cloud, vérifiez les périphériques réseau et de sécurité devant le réplicateur sur site. Vous devez configurer ces périphériques afin qu'ils n'interfèrent pas avec le trafic TLS (comme la terminaison ou le remplacement du certificat). Tous les périphériques réseau doivent être définis sur le mode TLS relais. VMware Cloud Director Availability est sensible aux modifications du trafic TLS chiffré.

