VMware Cloud Director Availability On-premises Guides

Guide #19
Troubleshooting

vmware®

Replications sync issues

If the replication is configured successfully, but sync stays at 0%, check the network connectivity between the ESXi hosts and the replicator. Check the network routes if existing, check the firewalls and network ports that are responsible for network communications. For more information, see:

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

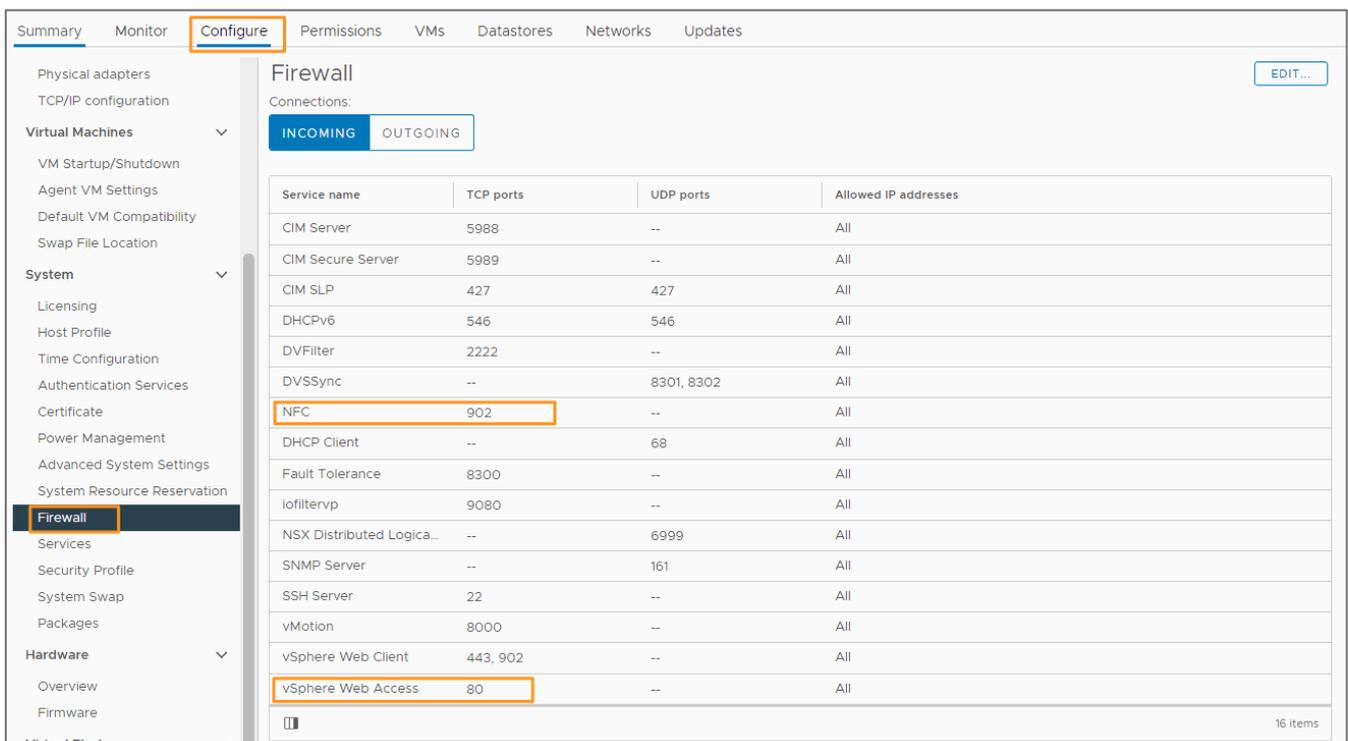## Check the connectivity from the replicator to the ESXi hosts

Open an SSH session to the replicator appliance and run the following commands for each ESXi host, by replacing the IP address with the IP address of each ESXi host:

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

If the connection is operational the output shows "0" (zero). If there is no connectivity on a specific network port, the command outputs the following:

```
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
```

If the connection times out for any of the network ports, check the network connectivity from the replicator to the ESXi host by checking the network routes and firewalls. In the vSphere UI, check the firewall settings for an ESXi host:

| Summary | Monitor | Configure | Permissions | VMs | Datastores | Networks | Updates |

Firewall

Connections:

INCOMING | OUTGOING

Service name	TCP ports	UDP ports	Allowed IP addresses
CIM Server	5988	--	All
CIM Secure Server	5989	--	All
CIM SLP	427	427	All
DHCPv6	546	546	All
DVFilter	2222	--	All
DVSSync	--	8301, 8302	All
NFC	902	--	All
DHCP Client	--	68	All
Fault Tolerance	8300	--	All
iofiltervp	9080	--	All
NSX Distributed Logica...	--	6999	All
SNMP Server	--	161	All
SSH Server	22	--	All
vMotion	8000	--	All
vSphere Web Client	443, 902	--	All
vSphere Web Access	80	--	All

Left navigation:
- Physical adapters
- TCP/IP configuration
- **Virtual Machines**
  - VM Startup/Shutdown
  - Agent VM Settings
  - Default VM Compatibility
  - Swap File Location
- **System**
  - Licensing
  - Host Profile
  - Time Configuration
  - Authentication Services
  - Certificate
  - Power Management
  - Advanced System Settings
  - System Resource Reservation
  - **Firewall**
  - Services
  - Security Profile
  - System Swap
  - Packages
- **Hardware**
  - Overview
  - Firmware
- **Virtual Flash**

EDIT...

16 items

Checking connectivity from an ESXi host to the replicator

Open an SSH connection and run the following command:

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

If the connection check fails, check the network connectivity from the ESXi host to the replicator by checking the network routes and firewalls.

Issues with the Lookup Service

When the Lookup Service connectivity is not operational, see the following connectivity articles:

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

If there are no connectivity issues, check the certificates for the Platform Service Controller and the vCenter Server instance(s) in the database of the Lookup Service.

1. To collect the vCenter Server certificate, run the following command, replacing the IP or FQDN of your vCenter Server:

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

The output of the command is the following:

```
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/uaDBLSnZUmfgbtO3VSIcUR9ItYFj+ZBuijF6yuAlcHoxfoiLEn7/Uyl7kc

dO49AaXE/AOxd8JsTNYhXvWCNYhjTV0OVxf9sL/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. In a browser open the Platform Service Controller address by using the path
'**/lookupservice/mob?moid=ServiceRegistration&method=List**' and replace the IP address with the IP or FQDN of your
Platform Services Controller.

Note: The IP address of the Platform Service Controller can be the same as the vCenter Server IP address, or can differ,
depending on the environment specifics.

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

3. Provide the SSO credentials.
4. In the value field, paste the following code:


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

5. In the page, search for **sslTrust** and compare the displayed certificate with the certificate collected by using
the **openssl** command. If the two certificates do not match, the vCenter support must update the certificates in the Lookup
Service.

Issues with pairing to a cloud site

When experiencing issues with pairing to a cloud site, check the network and security devices in front of the on-prem replicator.
These devices must be configured to not interfere with the TLS traffic (like certificate termination/replacement). All network
devices must be set to pass-through TLS mode. VMware Cloud Director Availability is sensitive to any changes in the encrypted
TLS traffic.

vmware®