This article describes how to troubleshoot Cisco Fabric Services (CFS) problems on a Cisco NX-OS device.

Guide Contents
Troubleshooting Overview
Troubleshooting Installs, Upgrades, and Reboots
Troubleshooting Licensing
Troubleshooting VDCs
Troubleshooting CFS {this section}
Troubleshooting Ports
Troubleshooting vPCs
Troubleshooting VLANs
Troubleshooting STP
Troubleshooting Routing
Troubleshooting Unicast Traffic
Troubleshooting WCCP
Troubleshooting Memory
Troubleshooting Packet Flow Issues
Troubleshooting FCoE
Before Contacting Technical Support
Troubleshooting Tools and Methodology

Contents

Information About Troubleshooting CFS

Many features in Cisco NX-OS require configuration synchronization across multiple devices in the network. CFS provides a common infrastructure for automatic configuration synchronization for an application in the network. It provides the transport function as well as a rich set of common services to the applications. CFS can discover CFS-capable devices in the network as well as their application capabilities.

Some of the applications that can be synchronized using CFS are as follows:

- Call Home

- RADIUS
- TACACS+
- User roles

Note: Do not enable CFS for an application that you manage using Cisco DCNM.

You can use CFS regions to limit the CFS configuration distribution to a subset of devices on the network.

Initial Troubleshooting Checklist

Begin troubleshooting CFS issues by checking the following issues first:

Checklist	Check off
Verify that CFS is enabled for the same applications on all affected devices.	
Verify that CFS distribution is enabled for the same applications on all affected devices.	
If you are using CFS regions, verify that the application is in the same region on all the affected devices.	
Verify that there are no pending changes for an application and that a CFS commit was issued for any configuration changes in a CFS-enabled application.	
Verify that there are no unexpected CFS locked sessions. Clear any unexpected locked sessions.	

Verifying CFS Using the CLI

To verify CFS using the CLI, follow these steps:

1. Verify that CFS is globally enabled on all devices in the network or CFS region.

```
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Disabled
```

2. Verify that CFS is enabled for the application on all devices in the network or CFS region.

```
switch(config)# show cfs application
----------------------------------------------
 Application    Enabled   Scope &
----------------------------------------------
 ntp            No        Physical-fc-ip
```

```
 stp            Yes       Physical-eth
 vpc            Yes       Physical-eth
 igmp           Yes       Physical-eth
 l2fm           Yes       Physical-eth
 role           Yes       Physical-fc-ip
 radius         Yes       Physical-fc-ip
 tacacs         No        Physical-fc-ip
 callhome       Yes       Physical-fc-ip
Total number of entries = 9
```

The Physical-fc-ip scope means that CFS uses IP to apply the configuration for that application to all devices in the network or region. The Physical-eth scope means that CFS uses Ethernet to apply the configuration for that application to all devices in the network or region.

3. Verify that CFS distribution is enabled for the application on all devices in the network or CFS region.

```
switch(config)# show cfs application name radius
 Enabled        : Yes
 Timeout        : 20s
 Merge Capable  : Yes
 Scope          : Physical-fc-ip
 Region         : 99
```

4. If you configure CFS regions, verify that the application is in the same region on all applicable devices.

```
switch(config)# show cfs regions brief
----------------------------------------
 Region         Application   Enabled
----------------------------------------
   4            callhome      yes
   99           radius        yes
```

5. Verify the set of devices that are registered with CFS for that application.

```
switch# show cfs peers name radius
Scope      : Physical-fc-ip
------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------
 20:00:00:0e:d7:0e:bf:c0  192.0.2.51    [Local]
 20:00:00:0e:d7:00:3c:9e  192.0.2.52
Total number of entries = 2
```

6. Compare the output of the **show cfs merge status name** *application-name* command and the **show cfs peers name** *application-name* command to verify that the network is not partitioned.

```
switch# show cfs merge status name radius
Physical-fc-ip Merge Status: Success [ Mon Jan 5 11:59:36 2009 ]
 Local Fabric
------------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------------
 20:00:00:05:30:00:4a:de  192.0.2.51    [Merge Master]
 20:00:00:0d:ec:0c:f1:40  192.0.2.204
Total number of switches = 2
```

```
switch# show cfs peers name radius
Scope      : Physical-fc-ip
------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------
 20:00:00:0d:ec:0c:f1:40  192.0.2.51 [Local]
 20:00:00:05:30:00:4a:de  192.0.2.204
Total number of entries = 2
```

If the list of switch WWNs in the **show cfs merge status name** command output is shorter than the list of switch WWNs in the**show cfs peers name** command output, the network is partitioned into multiple CFS fabrics and the merge status may show that the merge has failed, is pending, or is waiting.

7. Verify that a distribution is not in progress in the network for the application.

```
switch# show cfs lock
Application: callhome
Scope      : Physical-fc-ip
------------------------------------------------------------------------------
 Switch WWN              IP Address                  User Name    User Type
------------------------------------------------------------------------------
 20:00:00:22:55:79:a4:c1 172.28.230.85               admin        CLI/SNMP v3
                        switch
Total number of entries = 1
```

If the application does not show in the output, the distribution has completed.

8. Verify that there are no CFS sessions in progress for the application.

```
switch(config)# show radius session status
Last Action Time Stamp     : Wed Dec 24 13:25:00 2008
Last Action                : Commit
Last Action Result         : Success
Last Action Failure Reason : none
```

Troubleshooting Merge Failures

During a merge, the merge managers in the merging networks exchange their configuration databases with each other. The application on the merge master device merges the information, decides if the merge is successful, and informs all devices in the combined network of the status of the merge. When a merge is successful, the merge master distributes the database to all devices in the combined network and the combined network remains in a consistent state. A merge failure indicates that the merged network contains inconsistent data that could not be merged.

If you add a new device to the network and the merge status for any application shows "In Progress" for a prolonged period of time, then there may be an active session for that application in some other device. Use the **show cfs lock** command to check the lock status for that application on all the devices. The merge will not proceed if there are any locks present for that application on any device in the network or CFS region. Use the *application-name* **commit** command to commit the changes or use the **clear** *application-name* **session** command to clear the session lock so that the merge can proceed.

To recover from a merge failure using the CLI, follow these steps:

1. Identify a device that shows a merge failure.

```
switch# show cfs merge status
-------------------------------------------------------------
 Application       Scope             Vsan       Status
-------------------------------------------------------------
 role              Physical-fc-ip      -        Success
 radius            Physical-fc-ip      -        Success
 callhome          Physical-fc-ip      -        Failed
```

2. Commit the application configuration to restore all peers in the fabric to the same configuration database.

```
switch(config)# callhome commit
```

Troubleshooting Lock Failures

In order to distribute a configuration in the network, CFS must first acquire a lock on all devices in the network or CFS region. Once CFS acquires the locks, CFS issues a commit to distribute the configuration to all devices in the network or CFS region. Under normal circumstances, CFS releases the lock after the commit.

When another application peer acquires a lock, you cannot commit new configuration changes. This is a normal operation and you should postpone any changes to an application until the application peer releases the lock.

An inconsistent lock state also occur in the following scenarios:

- When locks are not held on all of the devices in the network or CFS region.
- When locks are held on all devices in the network or region, but a CFS session does not exist on the device that holds the lock.

Note: Use the troubleshooting steps in this section only if you believe the lock has not been properly released.

To troubleshoot a lock failure, follow these steps:

1. Determine all the devices that participate in the CFS distribution for this application.

```
switch1# show cfs peers name radius
Scope      : Physical-fc-ip
------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------
 20:00:00:0d:ec:0c:f1:40  192.0.2.51 [Local]
 20:00:00:05:30:00:4a:de  192.0.2.204
Total number of entries = 2
```

2. Check for a lock for this application on all CFS peer devices to determine the name of the administrator who owns the lock for the application.

```
switch2# show cfs lock
Application: radius
Scope      : Physical-fc-ip
--------------------------------------------------------------------------------
 Switch WWN              IP Address                  User Name    User Type
--------------------------------------------------------------------------------
20:00:00:05:30:00:4a:de  192.0.2.204                  admin        CLI/SNMP v3
                         switch
Total number of entries = 1
```

You should check with that administrator before clearing the lock.

3. Connect to the device that owns the CFS lock.

4. Release the CFS lock on the device that owns the lock.

```
switch2# radius abort
```

5. If the device does not release the lock, clear the CFS session on the device that owns the lock.

```
switch2# clear radius session
```

Troubleshooting CFS Regions

The following rules apply to CFS regions:

- When using CFS regions, an application on a given device can only belong to one region at a time.
- An application in a CFS region ignores all CFS distributions in any other region (including the default region).
- All applications that you do not assign to a CFS region exist in the default region.

To resolve a configuration distribution failure to all devices in a CFS region, follow these steps:

1. Verify the list of devices in a region for the application.

```
switch(config)# show cfs region name radius
Region-ID  : 4
Application: radius
Scope      : Physical-fc-ip
--------------------------------------------------------------------------
 Switch WWN              IP Address
--------------------------------------------------------------------------
 20:00:00:22:55:79:a4:c1 172.28.230.85                        [Local]
                         switch
Total number of entries = 1
```

2. Verify that the application distribution is enabled and is in the same region on all devices in the region.

```
switch2# show cfs application name radius
 Enabled        : Yes
 Timeout        : 20s
 Merge Capable  : Yes           >>>>> Application is capable of being merged.
 Scope          : Physical-fc-ip
 Region         : 1              >>>>> Application is in Region 1.

switch2(config)# cfs region 4
switch2(config-cfs-region)# radius
```

Note: You must reassign an application to a region whenever you disable that application. CFS assigns new applications in the default region.

Changing CFS Regions

If you move an application from one region to another, you may encounter a database mismatch when attempting a merge. Follow the steps outlined in the Troubleshooting Merge Failures to identify and resolve the conflicts.

Note: When an application is moved from one region to another (including the default region), the application loses all CFS history.

See Also

Before Contacting Technical Support

Further Reading

The following links contain further information on this topic from Cisco.com:

Configuring CFS

External Links

External links contain content developed by external authors. Cisco does not review this content for accuracy.