



## **Cisco Data Center Network Manager Troubleshooting Guide, Release 11.x**

**First Published:** 2018-06-19

**Last Modified:** 2020-12-22

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2020 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### Full Cisco Trademarks with Software License ?

---

#### CHAPTER 1

##### Overview 1

Guidelines for Troubleshooting 1

Technical Support Files 2

Collecting Log Files 2

---

#### CHAPTER 2

##### Device Discovery 5

Troubleshooting Device Discovery or Device Status 5

Troubleshooting Device Management 7

Troubleshooting Device OS Management 7

Troubleshooting Event Browsing 8

High CPU Utilization due to Elasticsearch Heap Size 8

---

#### CHAPTER 3

##### Troubleshooting during Installation 11

Troubleshooting PMN 11

Telemetry Log files not Rotating 12

---

#### CHAPTER 4

##### Upgrade 13

Upgrade Failure Due to PGEvent 13

Upgrade Failure Due to Change in Remote Host Identification 13

Image Upgrade Fails with a Permission Error 13

---

#### CHAPTER 5

##### eth Interfaces Troubleshooting 15

IP Address Conflict in AFW Address and System Access 15

Recovering Deleted eth Interface 16

Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation 17  
Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation 26  
DHCP Relay Not Operational 27

---

CHAPTER 6

**Native HA Troubleshooting 29**  
    Switchover in DCNM HA 29  
    Failover causing Kafka not starting 30



# CHAPTER 1

## Overview

This guide describes some common issues you might experience while using Cisco Data Center Network Manager (DCNM), and provides solutions.

- [Guidelines for Troubleshooting, on page 1](#)
- [Technical Support Files, on page 2](#)
- [Collecting Log Files, on page 2](#)

## Guidelines for Troubleshooting

When you troubleshoot issues with Cisco DCNM or a device that it manages, follow the guidelines listed in the following table.

**Table 1: Troubleshooting Guidelines**

Guideline	Description
Check the release notes to see if the issue is a known problem.	The release notes are accessible through the Cisco DCNM Documentation Roadmap.
Take screenshots of the fault or error message dialog box, and other relevant areas.	These screenshots provide visual cues about the state of Cisco DCNM when the problem occurred. If your computer does not have software to take screenshots, check the documentation for your operating system, as it might include this functionality.
Record the steps that you took directly before the issue occurred.	If you have access to screen or keystroke recording software, repeat the steps you took and record what occurs in Cisco DCNM. If you do not have access to that type of software, repeat the steps you took and make detailed notes of the steps and what happens in Cisco DCNM after each step.
Create a technical support file.	The information about the current state of the Cisco DCNM instance is very helpful to Cisco support and frequently provides the information needed to identify the source of the problem.

# Technical Support Files

When you encounter an issue that requires troubleshooting or a request for assistance to the Cisco Technical Assistance Center (TAC), collect as much information as possible about the affected Cisco DCNM instance.

To collect the server-side log files, execute the following:

- On Windows, execute `$INSTALLDIR/dcm/fm/bin/techsupport.bat`
- On Linux, execute `$INSTALLDIR/dcm/fm/bin/techsupport.sh`

To collect client-side log files, execute the following:

- On Windows, zip the files under `%USERPROFILE%\.cisco_mds9000/logs`
- On Linux, tar the files under `tar cvf clientlog.tar $HOME/.cisco_mds9000/logs`

## Collecting Log Files

The default installation directory for Cisco DCNM-LAN and DCNM-SAN is:

- Microsoft Windows— `C:\Program Files\Cisco Systems`
- Linux— `/usr/local/cisco`



---

**Note** In Microsoft Windows, when a 32-bit installer is used to install on 64-bit environment, the default installation directory will be `C:\Program Files<x86>\Cisco Systems`.

---



---

**Note** `<DCNM_HOME>` is the installation location of Cisco DCNM

---

Table 2: Installer Logs and Location

Log Name	Install Location
Installer Log	<p>After the installation is complete, the installer logs are available:</p> <ul style="list-style-type: none"> <li>• On Microsoft Windows at &lt;USER_HOME&gt;\dcnm_installer.log</li> <li>• On Linux at /root/dcnm_installer.log</li> </ul> <p><b>Note</b> If you have multiple Cisco DCNM installations on the same system, the logs are stored with the timestamp. If you have installed Cisco DCNM using the Debug mode, the dcnm_installer.log is not created and you need to copy the console log to a text file for future reference.</p>
PostgreSQL Log	<p>After the installation is complete, the postgresql logs are available:</p> <ul style="list-style-type: none"> <li>• On Microsoft Windows at &lt;USER_TEMP_DIR&gt;\installpostgresql.log</li> <li>• On Linux at /tmp/install-postgresql.log</li> </ul>
DCNM-LAN and DCNM SAN Sever Logs Logs	<p>After the installation and server startup is complete, the DCNM-LAN and DCNM_SAN server logs are available.</p> <ul style="list-style-type: none"> <li>• On Microsoft Windows at &lt;DCNM_HOME&gt;\dcm\wildfly\server\dcnm\logs</li> <li>• On Linux at &lt;DCNM_HOME&gt;/dcm/wildfly/server/dcnm/logs</li> </ul>







## CHAPTER 2

# Device Discovery

---

This chapter describes how to identify and resolve problems related to device discovery and management.

- [Troubleshooting Device Discovery or Device Status, on page 5](#)
- [Troubleshooting Device Management, on page 7](#)
- [Troubleshooting Device OS Management, on page 7](#)
- [Troubleshooting Event Browsing, on page 8](#)
- [High CPU Utilization due to ElasticSearch Heap Size, on page 8](#)

## Troubleshooting Device Discovery or Device Status

The table below shows the symptoms related to issues with device discovery or the device status. For each symptom that describes your problem, determine which possible causes apply and follow the corresponding solutions.

Table 3: Trouble with Device Discovery or Management

Symptoms	Possible Cause	Solution
A device discovery task fails. A device status changes to Unmanaged or Unreachable.	Incorrect device credentials were provided.	Reenter the username and password, and try discovering the device again.  If you are attempting to discover CDP neighbors of the seed device, ensure that the credentials that you provide are valid on all devices that you want to discover.
	The SSH server is disabled on the device.	Reenable the SSH server on the device and try discovering the device again.
	The maximum number of SSH sessions that the device can support has been reached.	Check the number of user sessions on the device. Free at least one connection and try discovering the device again.
	CDP is disabled on the device or on the device interface that the DCNM-LAN server connects to.	Ensure that CDP is enabled on the device globally and that it is enabled on the specific interface that the DCNM-LAN server connects to.
	The device interface that the DCNM-LAN server connects to is shut down.	Ensure that the device interface that the DCNM-LAN server connects to is up.
	The device restarted or shut down before discovery could complete.	Ensure that the device is running and try discovering the device again.
	The DCNM-LAN server cannot reach the device.	Ensure that the network requirements for device management are met.
	Discrepancy in system log messages.	Use the clear logging logfile command to clear the system log in the device and try to manually discover the device.
	Discrepancy in accounting log messages.	

Symptoms	Possible Cause	Solution
		<p>Use the clear accounting log command to clear the accounting log messages in the device and try to manually discover the device.</p> <p><b>Note</b> When working with a custom VDC, clear the accounting log messages only from the default VDC.</p>

## Troubleshooting Device Management

The table below shows symptoms related to device management. For each symptom that describes your problem, determine which possible causes apply and follow the corresponding solutions.

**Table 4: Trouble with Device Management**

Symptoms	Possible Cause	Solution
Clearing the log file or the accounting log on a Cisco NX-OS device does not cause DCNM LAN to rediscover the device automatically.	The device did not generate a system message about the accounting log or the log file being cleared. This problem is particularly likely if the device is a Cisco MDS 9000 Family Multilayer Switch running Cisco SAN-OS Release 3.1 or earlier releases.	Rediscover the device.
The DCNM-LAN shows device configuration information that is out of date.	The DCNM-LAN server was down.	<p>You can do either of the following:</p> <ul style="list-style-type: none"> <li>Rediscover the device.</li> <li>Restart the DCNM LAN server with a clean database. If the server was down for a long time, this action is the recommended solution.</li> </ul>

## Troubleshooting Device OS Management

The table below shows the symptoms related to the Device OS Management feature. For each symptom that describes your problem, determine which possible causes apply and follow the corresponding solutions.

**Table 5: Troubleshooting Device OS Management**

Symptoms	Possible Cause	Solution
During a software installation job, the software image file transfer between a file server and a device takes too much time.	The connection between the file server and the device is slow.	Use a file server that is on the same LAN as the devices included in the software installation job.  If all of the available file servers transfer software image files too slowly, before you create the software installation job, manually copy the files to the devices that you will include the job and configure the job to use the manually copied files rather than a file server.

## Troubleshooting Event Browsing

The table below shows the symptoms related to event browsing issues. For each symptom that describes your problem, determine which possible causes apply and follow the corresponding solutions.

**Table 6: Troubleshooting Event Browsing**

Symptoms	Possible Cause	Solution
Events available on the device command line do not appear in the DCNM-LAN.	Logging levels on managed devices are set incorrectly.	Check the logging level configuration on managed devices.
Too few events are shown in Event Browser or an Events tab.	The DCNM-LAN fetches events that are not old enough.	Check the events-related setting in the DCNM-LAN preferences.
Too many events are shown in Event Browser or on an Events tab.	A managed device has an issue that is generating many system log messages.	Temporarily unmanage the device until you resolve the issues on the device.
	Logging levels on managed devices are set incorrectly.	Check the logging level configuration on managed devices.
A feature Events tab does not show events that appear in the Event Browser.	By design, an Events tab shows only messages that apply to the currently selected feature and may show only a subset of the possible messages for the feature.	Use the Event Browser to see status-related system messages received by DCNM-LAN.

## High CPU Utilization due to Elasticsearch Heap Size

**Problem** The CPU utilization is very high in the DCNM OVA in Standalone mode in the scaled setup.

**Possible Cause** When the Performance Manager and Alarms are enabled in Scale DCNM OVA Standalone deployment, the CPU utilization increases and may cause unpredictable results.

**Solution** You must increase the heap size of the elasticsearch to reduce the CPU utilization, by using the following command.

```
[root@DCNM]# ls -l elasticsearch
-rw-r--r-- 1 root root 2490 Jul 10 13:44 elasticsearch
[root@DCNM]# pwd
/etc/sysconfig

# Heap size defaults to 256m min, 1g max
# Set ES_HEAP_SIZE to 50% of available RAM, but no more than 31g
ES_HEAP_SIZE=4g
```





## CHAPTER 3

# Troubleshooting during Installation

- [Troubleshooting PMN, on page 11](#)
- [Telemetry Log files not Rotating, on page 12](#)

## Troubleshooting PMN

- **Problem:** The pmn.logs file contains the following error message:

An authentication Error sending PMN notification: Possibly caused by authentication failure.

**Scenario:** After you upgrade a DCNM Native-HA setup to Release 11.1(1), an authentication failure message is logged in the pmn.logs file. This error occurs because RabbitMQ is not started correctly, and it is missing the administrator user.

**Workaround:** Restart the AMQP service. If this issue is not resolved, create an admin user with full access.

- **Option 1** - Restart AMQP using the following commands:

```
#appmgr stop amqp
#appmgr start amqp
```

- **Option 2** - Create an admin user with full access using the following commands:

```
# rabbitmqctl add_user <username> <password>
# rabbitmqctl set_user_tags <username> administrator
# rabbitmqctl set_permissions -p "/" <username> ".*" ".*" ".*"
```

- **Problem:** When checking the “appmgr status all” for the AMQP status, you get the below error message.

```
Cluster status of node rabbit@sol-dcnml ...
Error:
{:aborted, {:no_exists, [:rabbit_runtime_parameters, :cluster_name]}}
```

**Scenario:** This issue might occur in a DCNM Native HA setup.

A workaround is not required for this issue because it is a temporary status. Due to the auto heal option, the AMQP services will come up automatically in both the nodes.

# Telemetry Log files not Rotating

## Release impacted

Cisco DCNM 11.1(1) only

DCNM collects telemetry logs everyday. If one log file exceeds more than the configured file size, the spill over logs will be created as a separate file. You can configure the maximum number of logs files that will be generated everyday. Any log files created beyond that maximum limit will be rotated, which means the latest log will be retained and the oldest log will be deleted.

Based on the number of days the feature is operational, it may cause the disc space issue and the logs will not be rotated.

In order for the telemetry logs to be rotated correctly, the `telelmetry.log` script file must be located under `/etc/logrotate.d/telemetry` in both Active and Standby nodes with the following contents:

```
/var/log/telemetry.log
{
    daily
    missingok
    notifempty
    copytruncate
    rotate 10          */maximum number of log files stored/*
    compress
    size 5000k        */maximum space allotted for each log file/*
    create 0600 root root
}
```

If Telemetry is enabled on the Active node, this log file is automatically created. The file is not created on the Secondary node. If Telemetry is not enabled, this file is not present on Active node either and the log rotation will not begin.

Generate the `telelmetry.log` with appropriate content, irrespective of whether telemetry is enabled or disabled. If the above log file is not present, then the log rotation may not happen correctly. Creating the above file manually serves as a safety-net and will ensure that Telemetry logs are always rotated.





2. Upgrade the switch. For information, see *Install & Upgrade* section in the respective configuration guides.
3. (Optional) Remove the old file on the switch with the incorrect permissions.

If you are running an older NX-OS version on the switch, perform the following steps:

1. Remove the image file with permission errors on the switch.
2. Perform ISSU from DCNM. For information, see the *Install & Upgrade* section in the respective configuration guides.

For more information, see [Configuration Guides](#).



## CHAPTER 5

# eth Interfaces Troubleshooting

- [IP Address Conflict in AFW Address and System Access, on page 15](#)
- [Recovering Deleted eth Interface, on page 16](#)
- [Modifying Network Interfaces \(eth0 and eth1\) Post DCNM Installation, on page 17](#)
- [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 26](#)
- [DHCP Relay Not Operational, on page 27](#)

## IP Address Conflict in AFW Address and System Access

**Problem** You cannot access the Cisco DCNM Web UI when the user system is configured in the same IP subnet as that of the internal subnet used by application framework in the Cisco DCNM.

**Possible Cause** Application framework IP address subnet that is configured on DCNM is conflicting with the IP address that is configured on a system that is accessed by the Cisco DCNM user.

### Solution

If the DCNM internal address space is conflicting with the address space that is used in the network where a user access DCNM, use the application framework configuration to modify the subnet used in DCNM.

From Cisco DCNM Release 11.0, DCNM Infrastructure uses specific subnets, by default, for its internal purpose. The IP address subnets are as follows:

- 10.1.0.0/16: Used by service containers to communicate between each other.
- 172.17.0.0/16: Used by containers to communicate with native services.
- 172.18.0.0/16: Used by containers to communicate with any other native services.

The above subnets are not used to communicate with any devices outside of the DCNM. But, they can conflict with some services if they are used by external devices. For example, your PC used to access DCNM on the browser may use one of the same subnets or failure to enable EPL if the fabric routing loopback is using the same subnet pool to pick loopback IPs.

While installing Cisco DCNM Release 11.2(1), you can configure all the above subnets from a single larger subnet. When upgrading from Release 11.0(1) or 11.1(1) to Release 11.2(1), you must reconfigure these subnets, as required.

Modify the subnets by using the following commands:

1. `appmgr afw setup-net<ipv4-subnet>`

IPv4 subnet must have minimum length of /24 and maximum length of /20.



**Note** This command is not supported on DCNM installations that have computes connected.

This command reconfigures inter-subnet address that is used by service containers to communicate between each other. Execute this command on the Active node first, and then on the Standby node.

## 2. `apmgr afw setup-bridge<ipv4-subnet>`

IPv4 subnet must have minimum length of /24 and maximum length of /20.

This command reconfigures the subnets that are used by service containers to communicate with any other native services in the DCNM. Execute this command on all the DCNM nodes, including the Compute install nodes.

To confirm the change to subnets used for communication to docker native services, use the following sample commands outputs.

```
root@dcnm# ifconfig docker0
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 0.0.0.0
    inet6 fe80::42:3aff:feal:dd09 prefixlen 64 scopeid 0x20<link>
    ether 02:42:3a:a1:dd:09 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 656 (656.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@dcnm# ifconfig docker_gwbridge
docker_gwbridge: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 0.0.0.0
    inet6 fe80::42:b0ff:fe9a:5adc prefixlen 64 scopeid 0x20<link>
    ether 02:42:b0:9a:5a:dc txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

# Recovering Deleted eth Interface

## Release Impacted

Cisco DCNM Release 10.4(2) only

**Problem** In DCNM Release 10.4(2), after you reboot DCNM, the existing fabrics are not visible on the Cisco DCNM **Web UI > Configure > LAN Fabric**. In the **Select a Fabric** drop-down list on Network Deployment page, the fabrics are displayed.

**Possible Cause** If you have accidentally deleted the eth1 interface on the VM, the fabrics may not appear on the Cisco DCNM **Web UI > Configure > LAN Fabric**.

## Solution

To recover the deleted eth1 interface on the DCNM VM, perform the following steps:

1. Logon to the Cisco DCNM appliance using SSH.
2. Navigate to the directory `/etc/udev/rules.d/` and save the file `70-persistent-net.rules` to your local directory.
3. Open the file and make a note of the MAC address for the eth1 interface.
4. On SSH client, navigate to the **more** directory using `cd more` command. Execute the following command: `/etc/sysconfig/network-scripts/ifcfg-*` Save the output to your local directory.
5. Select **Power > Power On** and shut down the VM.
6. Click **Edit > Virtual Machine Details** to edit the virtual machine settings.
7. Click **Add > Ethernet Adapter**. From the **Adapter Type** drop-down list, choose **VMNET3**.
8. From the **Network Connection** drop-down list, select **DCNM Fabric Management Network**.
9. Check the **Connect at power on** check box. Click **Next** and then click **Finish**.
10. Select the newly added NIC and choose **Manual** for MAC assignment. The first 3 bytes are auto-populated. Take the last 3 bytes from the MAC address assigned to the previous eth1 interface and enter the value.
11. Click **OK**. You must wait for the VM to reconfigure.
12. Power on the VM and wait until DCNM is operational.
13. On the SSH client, verify if the eth1 interface is configured with the originally assigned IP address, using the `ifconfig -a` command. Ensure that the status of the eth1 interface is UP.
14. On the DCNM SSH, ping the eth1 gateway or the management IP of the attached switches.
15. On the Cisco DCNM Web UI, choose **Configure > LAN Fabric**. Verify if the fabric is visible.
16. Choose **Configure > Network Deployment** and verify if the fabric is visible in fabric selection drop-down list.

## Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation

Along with the eth0 and eth1 IP address (IPv4 and/or IPv6), you can also modify the DNS and the NTP server configuration using the `appmgr update network-properties` command.

For step-by-step instructions on how to modify the network parameters using the `appmgr update network-properties` commands, see the following sections.

- [Modifying Network Properties on DCNM in Standalone Mode, on page 18](#)

[Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup, on page 18](#)

- [Modifying Network Properties on DCNM in Native HA Mode, on page 19](#)

[Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup, on page 21](#)

### Modifying Network Properties on DCNM in Standalone Mode

The following sample shows the output for the **appmgr update network-properties** command for a Cisco DCNM Standalone Appliance.



**Note** Execute the following commands on the DCNM Appliance console to avoid a premature session timeout.

1. Initiate a session on the console, using the following command:

```
appmgr update network-properties session start
```

2. Update the Network Properties using the following command:

```
appmgr update network-properties set ipv4 {eth0|eth1}<ipv4-address> <network-mask> <gateway>
```

Enter the new IPv4 address for the Management (eth0) interface, along with the subnet mask and gateway IP addresses.

3. View and verify the changes by using the following command:

```
appmgr update network-properties session show {config | changes | diffs}
```

4. After you validate the changes, apply the configuration using the following command:

```
appmgr update network-properties session apply
```

Wait for a few minutes before you can logon to the Cisco DCNM Web UI using the eth0 Management Network IP address.

### Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup

The following sample example shows how to modify the network parameters post installation for a Cisco DCNM Standalone setup.

```
dcnm# appmgr update network-properties session start

dcnm# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0 172.28.10.1
dcnm# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****

dcnm# appmgr update network-properties session show changes
eth0 IPv4 addr 172.28.10.246/255.255.255.0 -> 172.28.10.244/255.255.255.0
eth1 IPv4 addr 1.0.0.246/255.0.0.0 -> 100.0.0.244/255.0.0.0

dcnm# appmgr update network-properties session apply
*****
WARNING
Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.
```

```

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****

dcnm# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
dcnm#

```


### Modifying Network Properties on DCNM in Native HA Mode

The following sample shows output to modify the network parameters using the **appmgr update network-properties** command for a Cisco DCNM Native HA Appliance.



- Note**
- Execute the following commands on the DCNM Active and Standby node console to avoid premature session timeout.
  - Ensure that you execute the commands in the same order as mentioned in the following steps.

1. Stop the DCNM Applications on the Standby node by using the following command:  
**appmgr stop all**  
Wait until all the applications stop on the Standby node before you go proceed.
2. Stop the DCNM Applications on the Active node by using the following command:  
**appmgr stop all**

3. Initiate a session on the Cisco DCNM console of both the Active and Standby nodes by using the following command:  
**appmgr update network-properties session start**
  4. On the Active node, modify the network interface parameters by using the following commands:
    - a. Configure the IP address for eth0 and eth1 address by using the following command:  
**appmgr update network-properties set ipv4 {eth0|eth1}<ipv4-address> <network-mask>  
<gateway>**  
Enter the new IPv4 or IPv6 address for the eth1 interface, along with the subnet mask and gateway IP addresses.
    - b. Configure the VIP IP address by using the following command:  
**appmgr update network-properties set ipv4 {vip0|vip1}<ipv4-address> <network-mask>**  
Enter the vip0 address for eth0 interface. Enter the vip1 address for eth1 interface.
    - c. Configure the peer IP address by using the following command:  
**appmgr update network-properties set ipv4 {peer0|peer1}<ipv4-address>**  
Enter the eth0 address of the Standby node as peer0 address for Active node. Enter the eth1 address of the Standby node as peer1 address for Active node.
    - d. View and validate the changes that you have made to the network parameters by using the following command:  
**appmgr update network-properties session show {config | changes | diffs}**  
View the changes that you have configured by using the following command:
  5. On the Standby node, modify the network interface parameters using the commands described in [Step 4](#).
  6. After you validate the changes, apply the configuration on the Active node by using the following command:  
**appmgr update network-properties session apply**  
Wait until the prompt returns, to confirm that the network parameters are updated.
  7. After you validate the changes, apply the configuration on the Standby node by using the following command:  
**appmgr update network-properties session apply**
  8. Start all the applications on the Active node by using the following command:  
**appmgr start all**
-  **Note** Wait until all the applications are running successfully on the Active node, before proceeding to the next step.
9. Start all the applications on the Standby node by using the following command:  
**appmgr start all**
  10. Establish peer trust key on the Active node by using the following command:



**appmgr update ssh-peer-trust**

11. Establish peer trust key on the Standby node by using the following command:

```
appmgr update ssh-peer-trust
```

**Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup**

The following sample example shows how to modify the network parameters post installation for a Cisco DCNM Native HA setup.



**Note** For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

```
[root@dcnm2]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm2 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm2]#

[root@dcnm1]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm1 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm1]#

[root@dcnm1]# appmgr update network-properties session start
[root@dcnm2]# appmgr update network-properties session start

[root@dcnm1]# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
172.28.10.1
[root@dcnm1]# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm1]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm1]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm1]# appmgr update network-properties set ipv4 peer0 172.28.10.245
[root@dcnm1]# appmgr update network-properties set ipv4 peer1 100.0.0.245
[root@dcnm1]# appmgr update network-properties session show changes

[root@dcnm2]# appmgr update network-properties set ipv4 eth0 172.28.10.245 255.255.255.0
```

```

172.28.10.1
[root@dcnm2]# appmgr update network-properties set ipv4 eth1 100.0.0.245 255.0.0.0
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm2]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm2]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm2]# appmgr update network-properties set ipv4 peer0 172.28.10.244
[root@dcnm2]# appmgr update network-properties set ipv4 peer1 100.0.0.244
[root@dcnm2]# appmgr update network-properties session show changes

[root@dcnm1]# appmgr update network-properties session show changes
eth0 IPv4 addr 172.28.10.246/255.255.255.0 -> 172.28.10.244/255.255.255.0
eth1 IPv4 addr 1.0.0.246/255.0.0.0 -> 100.0.0.244/255.0.0.0
eth0 VIP 172.28.10.248/24 -> 172.28.10.238/24
eth1 VIP 1.0.0.248/8 -> 100.0.0.238/8
Peer eth0 IP 172.28.10.247 -> 172.28.10.245
Peer eth1 IP 1.0.0.245 -> 100.0.0.245

[root@dcnm1]# appmgr update network-properties session show config
===== Current configuration =====
NTP Server 1.ntp.esl.cisco.com
eth0 IPv4 addr 172.28.10.246/255.255.255.0
eth0 IPv4 GW 172.28.10.1
eth0 DNS 171.70.168.183
eth0 IPv6 addr 2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW 2001:420:284:2004:4:112:210:1
eth1 IPv4 addr 1.0.0.246/255.0.0.0
eth1 IPv4 GW
eth1 DNS 1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr /
eth2 IPv4 GW
Peer eth0 IP 172.28.10.247
Peer eth1 IP 1.0.0.247
Peer eth2 IP
eth0 VIP 172.28.10.248/24
eth1 VIP 1.0.0.248/8
eth2 VIP /
eth0 VIPv6 /
eth1 VIPv6 /

===== Session configuration =====
NTP Server 1.ntp.esl.cisco.com
eth0 IPv4 addr 172.28.10.244/255.255.255.0
eth0 IPv4 GW 172.28.10.1
eth0 DNS 171.70.168.183
eth0 IPv6 addr 2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW 2001:420:284:2004:4:112:210:1
eth1 IPv4 addr 100.0.0.244/255.0.0.0
eth1 IPv4 GW
eth1 DNS 1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr /
eth2 IPv4 GW
Peer eth0 IP 172.28.10.245
Peer eth1 IP 100.0.0.245
Peer eth2 IP
eth0 VIP 172.28.10.238/24
eth1 VIP 100.0.0.238/8
eth2 VIP /
eth0 VIPv6 /
eth1 VIPv6 /

```

```

[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session show config
===== Current configuration =====
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.247/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.247/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.246
Peer eth1 IP    1.0.0.246
Peer eth2 IP
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /

===== Session configuration =====
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.245/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  100.0.0.245/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.244
Peer eth1 IP    100.0.0.244
Peer eth2 IP
eth0 VIP        172.28.10.238/24
eth1 VIP        100.0.0.238/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /

[root@dcnm2]#

[root@dcnm1]# appmgr update network-properties session apply
*****
WARNING

Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).

```

```

log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****
Please run 'appmgr update ssh-peer-trust' on the peer node.
*****
[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session apply
*****
WARNING

Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
afwnetplugin:0.1
server signaled
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****
Please run 'appmgr update ssh-peer-trust' on the peer node.
*****
[root@dcnm2]#

[root@dcnm1]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm1]#

```

**Wait until dcnm1 becomes active again.**

```
[root@dcnm2]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.
```

```
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm2]#
```

```
[root@dcnm1]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '172.28.10.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '100.0.0.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no'
'dcnm-247.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm1]#
```

```
[root@dcnm2]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '172.28.10.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '100.0.0.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no'
'dcnm-246.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm2]#
```

# Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation

During the DCNM installation, you can configure the In-Band Management interface. You must associate this network with the port group that corresponds to a fabric in-band connection. The In-Band Network provides reachability to the devices via the front-panel ports.



**Note** If you need to modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again.



**Note** You cannot use Endpoint Locator and Telemetry features if the eth2 interface is not configured.

To configure the eth2 interface for the in-band management network, use the **appmgr setup inband** command.

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Standalone Appliance.

```
[root@dcnm]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.250
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
Validating Inputs ...

You have entered these values..
PIP=2.0.0.250
NETMASK=255.0.0.0
GATEWAY=2.0.0.1

Press 'y' to continue configuration, 'n' to discontinue [y] y
{"ResponseType":0,"Response":{"Refreshed"}}
{"ResponseType":0,"Response":{"AfwServerEnabled":true,"AfwServerReady":true,"InbandSubnet":"2.0.0.0/8",
"InbandGateway":"2.0.0.1","OutbandSubnet":"0.0.0.0/8","OutbandGateway":"0.0.0.0","UnclusteredMode":true}}

Done.
[root@dcnm]#
```

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Native HA Appliance.

On Cisco DCNM Primary appliance:

```
[root@dcnm-primary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.244
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
```

```
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...
```

You have entered these values..

```
PIP=2.0.0.244
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244
```

Press 'y' to continue configuration, 'n' to discontinue [y] **y**

Done.

```
[root@dcnm-primary]#
```

On Cisco DCNM Secondary appliance:

```
[root@dcnm-secondary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.245
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...
```

You have entered these values..

```
PIP=2.0.0.245
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244
```

Press 'y' to continue configuration, 'n' to discontinue [y] **y**

HA Role is Active {"ResponseType":0,"Response":"Refreshed"}

Done.

```
[root@dcnm-secondary]#
```

## DHCP Relay Not Operational

### Release impacted

Cisco DCNM Release 11.0(1) only

**Problem** After Cisco DCNM Installation, DHCP relay may not be operational.

**Possible Cause** Configuring eth1 interface is an optional parameter during Cisco DCNM Installation. If you do not configure eth1 gateway, DHCP relay may not be operational.

**Solution** Configure the eth1 gateway by using the following command:

```
dcnm# echo "2.0.0.0/8 via 1.0.0.100 dev eth1"
/etc/sysconfig/network-scripts/route-eth1
/etc/sysconfig/network-scripts/ifup-routes eth1
```







## CHAPTER 6

# Native HA Troubleshooting

- [Switchover in DCNM HA, on page 29](#)
- [Failover causing Kafka not starting, on page 30](#)

## Switchover in DCNM HA

**Problem** When Active node (represented as A) goes down, the Standby node (represented as B) takes the role of the Active node. However, when A node comes up, it takes the role of the Active node again. This condition is known as Switchover in DCNM HA. The old Active node must not take the role of Active node unless a failover is triggered or the HA heartbeat instances cannot talk to each other.

**Possible Cause** This occurs when **shutdown** or **no shutdown** command is executed on the switch interfaces connected to DCNM eth1 interfaces. Heartbeat detects a Split-Brain syndrome. As both the nodes detect this condition, both the nodes will shut down and restart. Therefore, the DCNM Web UI A node becomes active again, when node A is operational again.

### Solution

HA Ping feature allows you to shut down the heartbeat instances that cannot reach (ping) a specified device on the network.

Configure HA Ping IP address and Peer IP address on the device, by using the following commands on both the HA nodes.

```
HA_PING_ADDRESS=  
PEER_ETH1_IP=  
echo "* * * * * root /sbin/ha-ping.sh" > /etc/cron.d/ha-ping  
echo "IP=$HA_PING_ADDRESS" > $DCNM_HOME/ha-ping.conf  
echo "PEER_IP=$PEER_ETH1_IP" >> $DCNM_HOME/ha-ping.conf  
chkconfig heartbeat off  
sed -i "s/APP_STATUS_HEARTBEAT=.* /APP_STATUS_HEARTBEAT=ha-ping/g" /root/.DO_NOT_DELETE
```

To avoid HA Switchover, increase the Heartbeat's deadtime to 60 or 90 seconds. This avoids re-occurrence of this issue if shut and no shut duration is 30 to 60 seconds apart.

To increase the timers and thereby avoid the HA Switchover, you must edit the **deadtime** specified in the `/etc/ha.d/ha.cfg` file.

The following shows an example to edit the `edit /etc/ha.d/ha.cfg` file.

```
dcnm-standby# stop ha-apps  
dcnm-active# stop ha-apps
```

Edit the deadtime value in `/etc/ha.d/ha.cfg` file on both the nodes.

Execute the **appmgr start ha-apps** on old Active node.

```
dcnm-active# appmgr start ha-apps
```

Wait until the Active node is active again. Verify the role using the **show ha-role** command.

Execute the **appmgr start ha-apps** on old Standby node.

```
dcnm-standby# appmgr start ha-apps
```

## Failover causing Kafka not starting

### Release Impacted

Cisco DCNM Release 11.1(1) only

**Problem** Cisco DCNM failover occurs and Kafka does not start after recovery.

**Possible Cause** The `server.properties` in Kafka must be configured based on the Zookeeper application. The application framework assigns IP address for all the services. In the failover scenario, the **fmserver** is not operational and application framework is operational. In such situation, the Kafka application starts with wrong configuration.

**Solution** Let us indicate Cisco DCNM Active node as **dcnm1** and the Standby node as **dcnm2**. To troubleshoot this issue, you must restart the application framework services on both Active and Standby in the below mentioned order.

```
dcnm2# appmgr stop afw      /* Stop services on Standby node */
dcnm1# appmgr stop afw      /* Stop services on Active node */

dcnm1# appmgr start afw     /* Start services on Active node */
dcnm2# appmgr start afw     /* Start services on Standby node */
```