Failover Configuration Guide for Cisco Digital Media Suite Release 5.5 and 5.6

March 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Failover Configuration Guide for Cisco Digital Media Suite Release 5.5 and 5.6

CONTENTS

Preface

March 2015

This document is for Cisco Digital Media Suite (DMS) administrators who are configuring failover for Cisco Show and Share and Cisco Digital Media Manager (DMM) installations. See these sections:

Change History

Release 5.6

Added support for Cisco Show and Share and Cisco DMM Release 5.6.

Release 5.5

New in Cisco Show and Share and Cisco DMM Release 5.5:

- High availability support—You can now configure automatic failover from one Cisco MXA UCS M3 server to another.
- Cisco Show and Share and Cisco DMM hardware and software compatibility—Release 5.5 is supported only on the Cisco MXA UCS M3 server appliance. Cisco Show and Share running on a Cisco MXA UCS M3 server is compatible only with Cisco DMM running on a Cisco MXA UCS M3 server.

Note Configuring Digital Signs failover on a DMM running Release 5.5 or 5.6 is not supported.

Related Documentation

For all Cisco Show and Share documentation, see the following:

http://www.cisco.com/c/en/us/support/conferencing/show-share/tsd-products-support-series-home.html

For more information about Cisco Digital Media Suite, see the following:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/roadmaps/dmsmap515253.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

About Failover

March 2015

This chapter describes the Cisco Digital Media Suite (DMS) failover configuration. The failover feature allows you to configure two Cisco DMS appliances so that a secondary appliance takes over operation if the primary appliance fails.

See these sections:

Overview

You can configure Cisco DMS appliances in a stateless, active/standby failover configuration. The failover configuration requires two identical Cisco DMS appliances connected to each other through a dedicated failover link. The health of the active unit is monitored to determine if specific failover conditions are met. When those conditions are met, failover occurs.

Failover Terminology

The following terms are used throughout this document for describing failover configurations:

- **Active appliance**—The appliance that is currently responding to user requests. Always access the active appliance by using the virtual IP address and the virtual FQDN.
- **Application interface**—The interface on a Cisco DMM or Cisco Show and Share appliance that users connect to. Health monitoring also occurs through this interface.
- **Dedicated FQDN**—An FQDN that is assigned to the appliance. The FQDN remains with the appliance during a failover. The appliance is reachable through the FQDN, but it should only be used if you are trying to access the AAI interface of the standby appliance (you cannot access the GUI of an appliance in the standby state).

  Users should never use the dedicated FQDN to access the Cisco DMM or Cisco Show and Share GUI on the active appliance; they should use the Virtual FQDN to access the active appliance GUI.

- **Dedicated IP address**—An IP address that is assigned to the appliance. This IP address remains with the appliance during a failover.
- **Primary appliance**—The appliance in a failover pair that is initially put into the active state and is the source of data during the initial configuration. When adding failover to an existing Cisco DMS installation, the existing Cisco DMS appliances are the primary appliances. The virtual IP address and virtual FQDN are obtained from the primary appliances.
- **Replication interface**—The interface that connects two appliances in a failover pair together. Health monitoring and data replication occur through the interface. You cannot access the Cisco DMM or Cisco Show and Share GUI through the replication interface.
- **Secondary appliance**—The appliance that is initially put into the standby state. When adding failover to an existing Cisco DMS installation, the secondary appliances are added to the existing configuration.
- **Standby appliance**—The appliance that is not actively responding to user requests. The standby appliance monitors the active appliance health for failover triggers. During a failover, the standby appliance becomes active and takes over the virtual IP address and FQDN.
- **Virtual FQDN**—The FQDN used by the active appliance, no matter which physical appliance is the active appliance. Users and administrators should always use the virtual FQDN to access the Cisco DMM or Cisco Show and Share appliance interface.
- **Virtual IP address**—The IP address used by the active appliance, no matter which physical appliance is the active appliance. If the active appliance fails, the virtual IP address is used by the standby appliance as it becomes active.

Supported Failover Configurations

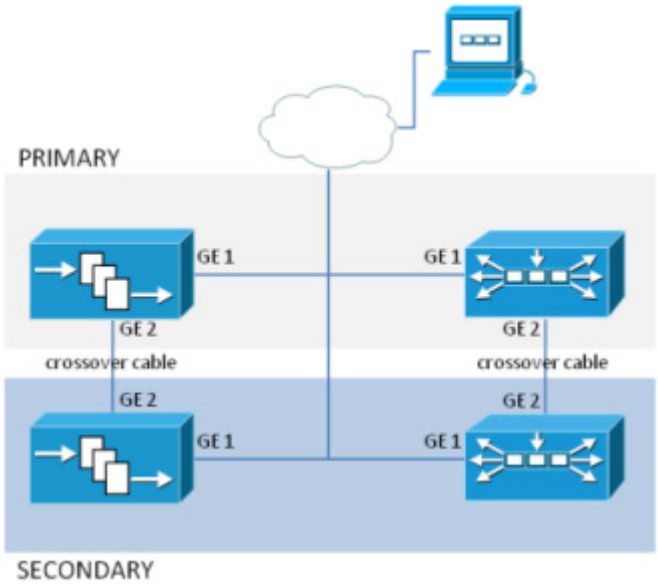
A Cisco Show and Share failover configuration requires the following devices:

- A primary and a secondary Cisco DMM appliance. The application interfaces (GE 1) must be on the same subnet. The appliances must be connected together by a crossover cable or a switch on their replication interfaces (GE 2). The application interfaces must be on a different subnet from the replication interfaces.
- A primary and a secondary Cisco Show and Share appliance. The application interfaces (GE 1) must be on the same subnet. However, the application interfaces can be on a different subnet from the Cisco DMM appliance. The appliances must be connected together by a crossover cable or a switch on their replication interfaces (GE 2). The application interfaces must be on a different subnet from the replication interfaces.

Note You cannot configure failover for only the Cisco Show and Share appliance; you must configure it for both the Cisco Show and Share and the Cisco DMM appliances.

Figure 1-1 shows an example Cisco Show and Share failover configuration.

Figure 1-1 Cisco Show and Share Failover Configuration



Failover Process

These events trigger failover:

- The standby device fails to receive 10 heartbeat messages from the active device.

  Heartbeat messages are sent once per second. Missing 10 consecutive heartbeats causes a failover.
- Manually restarting the following services by using the Appliance Administrative Interface (AAI):
  - Web services (Tomcat)
  - Database services
- Rebooting the active appliance.
- Loss of power (either because you powered the appliance off or there was a general power failure)
- Pairing the active appliances.
- Restoring a backup on the active appliance.
- Changing the logging level.
- Re-generating a certificate.
- Reaching the fail count threshold (5) for a monitored service running on the active appliance. When a service stops, the appliance automatically attempts to restart it. Each time the service fails, a fail counter increments. When the fail counter for any of the services reaches 5, failover is triggered. To clear the counters, you need to reboot the appliance. See Minor Failure Event Recovery, page 4-1 for more information.

A single disk failure on the active unit does not cause a failover. To fail over, you must force failover by rebooting the active appliance. A multiple-disk failure on the active will cause failover. See Major Failure Event Recovery, page 4-1 for more information about recovering from a disk failure.

These events occur during failover:

1. A failover event occurs. This causes the active appliance to go into a down or unknown state, depending on the type of failure. A “down” notification is sent.
2. The standby appliance becomes the active appliance by using the virtual FQDN and IP address.
3. The new active appliance restarts the application services. This can take up to three minutes for a Cisco Show and Share appliance. An “up” notification is sent.
4. When the failed appliance is brought back online, it becomes the standby unit and begins emitting heartbeat requests.

Failover is stateless. Therefore, any users with active sessions to the appliance will need to reconnect and, if they were logged in, log in again.

If users were viewing a Cisco Show and Share video that was hosted on an external server, the video will continue to play until the user attempts to navigate the application. If users were viewing a video that was streaming from Cisco Show and Share, the video will stop playing.

If users are uploading or publishing a video when a failover occurs, the process will fail and they will need to re-upload or re-publish their video.

After a failover, users will need to wait approximately three to five minutes before they can log back into the web interface.

Cisco Show and Share Failover Configuration

March 2015

This chapter describes how to configure failover on a Cisco Show and Share installation. It covers both new installations and adding failover to an existing installation.

See these topics:

Prerequisites

Before you can configure failover, you must meet the following requirements:

Licensing Requirements

When licensing your failover cluster, you only need to install the feature, author, and failover licenses on the primary Cisco DMM appliance. The secondary pair of appliances only need the base licenses that are included with the appliances. They will inherit the optional feature, device, and author licenses during the failover activation process.

Devices	Licenses Needed
Primary Cisco DMM and Cisco Show and Share Pair	• Base license • Failover license • (Optional) Feature licenses (Live Event Module, SNMP Notification Module, etc.) • (Optional) Author Licenses
Secondary Cisco DMM and Cisco Show and Share Pair	Base license

You must have a failover license installed on your primary Cisco DMM appliance to activate the failover configuration. You can enter the failover settings without the license, but you cannot activate failover until the license is installed. See the Cisco DMM User Guide Licensing Chapter:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dmm/user/guide/dmsug53x/licenses.html

Hardware Requirements

Failover configuration is supported on the following Cisco DMS hardware platforms:

- Cisco Show and Share Release 5.6 running on a Cisco MXA UCS M3 server is compatible only with Cisco DMM Release 5.6 running on a Cisco MXA UCS M3 server.
- Cisco Show and Share Release 5.5 running on a Cisco MXA UCS M3 server is compatible only with Cisco DMM Release 5.5 running on a Cisco MXA UCS M3 server.

The primary and secondary appliances in a failover pair must be identical. Table 2-1 shows the failover appliance part numbers that correspond to the primary appliances.

Table 2-1 Failover Appliance Part Numbers

Primary Appliance	Secondary Appliance
Cisco Digital Media Manager Enterprise Cisco Show and Share Enterprise SNSC220-ENT-K9=	SNSC220-ENT-K9=
Cisco Digital Media Manager Workgroup Cisco Show and Share Workgroup SNSC220-WKG-K9=	SNSC220-WKG-K9=

Configuration Requirements

Before configuring failover, you should:

- Configure NTP on all appliances.
- Add the required FQDNs to your name server.
- Install external certificates on the primary pair of appliances. After a certificate expires, use the virtual FQDN when obtaining a new certificate. Install new certificates by using the virtual FQDN to access the AAI interface.

Installation Guidelines

Note Configuring Digital Signs failover on a DMM running Release 5.5 or 5.6 is not supported.

- The *application* interface of each appliance pair must be on the same subnet (although the Cisco DMM pair and the Cisco Show and Share pair are not required to be on the same subnet).
- The *replication* interface of each appliance pair must be on the same subnet. However, they cannot be on the same subnet as the application interface.
- You must install the base license on the secondary pair of appliances before you can configure failover.
- Failover activation and replication can take up to 15 hours.
  - During the activation phase (which takes up to 20 minutes), the Cisco DMM and Cisco Show and Share applications are not available to end users.
  - During replication phase, users can view and upload videos to Cisco Show and Share, but performance may be degraded.
  - Do not make any configuration or administrative changes or restart services during activation and replication.
- You cannot configure failover for only the Cisco Show and Share appliances; you must configure failover for both the Cisco DMM and the Cisco Show and Share appliances.
- In a switched configuration, the switch interfaces connected to the replication interfaces must be configured for 1000 Mbps.
- When using a switched interface for the replication interface connection, confirm that the latency between the active and standby device is no more than ten seconds. Latency of greater than ten seconds will cause ten consecutive heartbeat messages to be missed, initiating a failover.
- You cannot access the GUI of a standby appliance. You can access the AAI interface of a standby appliance by using the dedicated IP address or dedicated FQDN. Do not make any configuration changes to the standby appliance.
- Back up your failover cluster by using the virtual FQDN to access AAI immediately after configuring failover. Backups taken in standalone mode cannot be restored on a failover cluster.
- Backups taken from a standalone mode set of appliances cannot be restored on a failover cluster. However, backups taken from an active device in a failover cluster can be restored on the appliance when it is converted to standalone mode.

- Restoring data on a Cisco Show and Share appliance in a failover cluster causes the Cisco Show and Share to reboot, initiating failover. This is expected behavior. The data is written to the standby appliance during the restore so that when the standby appliance becomes active it will contain the correct data.

Pre-Configuration Worksheet

You will need the information in the following tables to complete the configuration. We recommend that you print out the tables and fill in the information before you begin.

- Table 2-2 on page 2-4, DMM Failover Pre-Configuration Worksheet.
- Table 2-3 on page 2-5, Show and Share Failover Pre-Configuration Worksheet

Table 2-2 DMM Failover Pre-Configuration Worksheet

Item	Value	Notes
DMM		
Primary Appliance FQDN		For existing installations, this is the FQDN of the existing appliance. For new installations, this is the FQDN used to access the DMM. The FQDN becomes the virtual FQDN for the Cisco DMM failover cluster.
Primary Appliance IP Address		For existing installations, this is the IP Address of the existing appliance. For new installations, this is the IP address used to access the DMM. This IP address becomes the virtual IP address for the Cisco DMM failover cluster.
Primary Appliance Alternate, Dedicated FQDN		This is the FQDN that is applied to the primary appliance when the original FQDN becomes the DMM virtual FQDN.
Primary Appliance Alternate, Dedicated IP Address		This is the IP address that is applied to the primary appliance when the original IP address becomes the DMM virtual IP address.
Secondary Appliance Dedicated FQDN		The FQDN for the secondary appliance.
Secondary Appliance Dedicated IP Address		The IP address for the secondary appliance.
(Optional) Primary Appliance Replication Interface IP Address		If using a switch between the primary and secondary DMM appliance replication interfaces, the IP address used by the interface on the primary appliance.
(Optional) Secondary Appliance Replication Interface IP Address		If using a switch between the primary and secondary DMM appliance replication interface, the IP address used by the interface on the secondary appliance.

Table 2-3 Show and Share Failover Pre-Configuration Worksheet

Item	Value	Notes
Show and Share		
Primary Appliance FQDN		For existing installations, this is the FQDN of the existing Show and Share appliance. For new installations, this is the FQDN used to access Cisco Show and Share. The FQDN becomes the virtual FQDN for the Cisco DMM failover cluster.
Primary Appliance IP Address		For existing installations, this is the IP Address of the existing appliance. For new installations, this is the IP Address used to access Cisco Show and Share. This IP address becomes the virtual IP address for the Cisco DMM failover cluster.
Primary Appliance Alternate FQDN		This is the FQDN that is applied to the primary appliance when the original FQDN becomes the Show and Share virtual FQDN.
Primary Appliance Alternate IP Address		This is the IP address that is applied to the primary appliance when the original IP address becomes the Show and Share virtual IP address.
Secondary Appliance FQDN		The FQDN for the secondary appliance.
Secondary Appliance IP Address		The IP address for the secondary appliance.
(Optional) Primary Appliance Replication Interface IP Address		If using a switch between the primary and secondary Cisco Show and Share appliance replication interface, the IP address used by the interface.
(Optional) Secondary Appliance Replication Interface IP Address		If using a switch between the primary and secondary Cisco Show and Share appliance replication interface, the IP address used by the interface on the secondary appliance.

Configuring Failover

To configure failover perform the following procedures in this order:

1. Set Up the Primary DMS Pair, page 2-6
2. Set up the Secondary DMS Pair, page 2-6
3. Connect the Primary and Secondary Appliance Replication Interfaces, page 2-7
4. Configure the Non-Master Appliances, page 2-8
5. Configure the Primary DMM (Cluster Master), page 2-9
6. Activate the Failover Cluster, page 2-12
7. Monitor Replication and Verify the Configuration, page 2-13

Set Up the Primary DMS Pair

If you have an existing DMS pair, skip this step. The existing FQDNs and IP addresses will become the virtual FQDNs and IP address for the cluster. Users will not need to change their bookmarks.

Set up the primary DMS pair as you would a standalone system. See the *Quick Start Hardware Installation Guide for Cisco Show and Share and Digital Media Manager Release 5.3.10 on the MXA UCS M3 Server* for information about setting up the system. When setting up the system, **use the primary FQDNs and IP addresses for the appliances. These are the FQDNs and IP addresses that you want users to access. They will become the virtual FQDNs and IP addresses during the failover configuration process.**

In a later step, you will replace the primary FQDNs and IP addresses used here with the alternate FQDNs and IP addresses.

Before continuing, confirm that you have:

1. Installed the failover license on the DMM.
2. Installed third party certificates on your appliances, if applicable.
3. Enabled NTP on the appliances.

Set up the Secondary DMS Pair

Set up the secondary DMS pair as you would a standalone system. See the *Quick Start Hardware Installation Guide for Cisco Show and Share and Digital Media Manager Release 5.3.10 on the MXA UCS M3 Server* for information about setting up the system.

Use the secondary FQDNs and IP addresses for the secondary pair.

The application interfaces for the appliances must be on the same subnet as the primary DMM and Show and Share appliances.

You only need to have the base licenses installed on the secondary DMS pair.

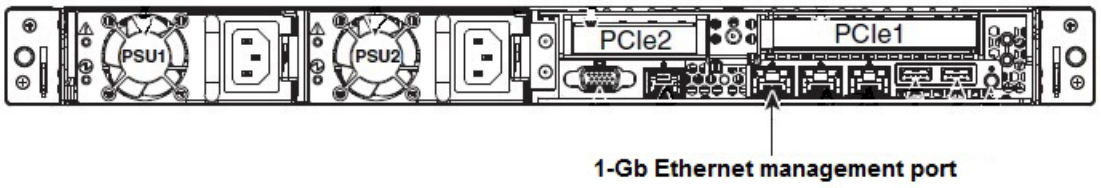
Connect the Primary and Secondary Appliance Replication Interfaces

You have two options for connecting the primary and secondary appliance replication interfaces:

- Crossover cable directly connecting the appliances.
- Connecting the appliances through a switch.

  If you are using a switch between the replication interfaces, the replication interfaces must be on a different subnet than the application interface.

Figure 2-1 Cisco MXA UCS M3 Appliance Connection Port



Procedure

To connect the primary appliances, follow these steps:

Step 1 Connect the 1-Gb Ethernet management port (Figure 2-1) on the primary DMM to the 1-Gb Ethernet management port of the secondary DMM. You can use a crossover cable for a direct connection, or connect the appliances through a switch.

Step 2 Connect the 1-Gb Ethernet management port (Figure 2-1) on the primary Show and Share appliance to the 1-Gb Ethernet management port of the secondary Show and Share appliance. You can use a crossover cable for a direct connection, or connect the appliances through a switch.

Configure the Non-Master Appliances

The primary DMM appliance is the cluster master. Before you configure the cluster master, you must configure the non-master appliances to recognize the primary DMM appliance as the cluster master.

To configure the failover settings on the non-master devices, follow these steps:

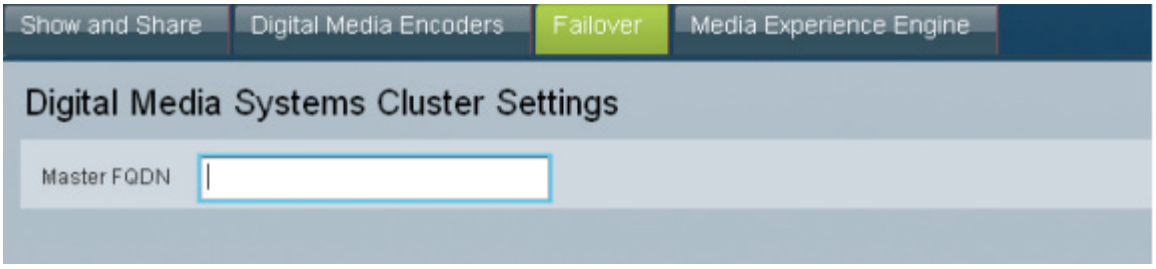
Step 1 Configure the secondary Cisco Show and Share appliance:

a. Using the **primary FQDN** to access the primary Cisco Show and Share interface, log in to Cisco Show and Share using the superuser or an administrator account.

b. From the Global Navigation menu, choose **Administration**.

c. Click the **Failover** tab.

d. Enter the DMM **primary FQDN** in the Master FQDN field. DO NOT use the alternate FQDN.



e. Click **Save**.

f. Exit Cisco Show and Share.

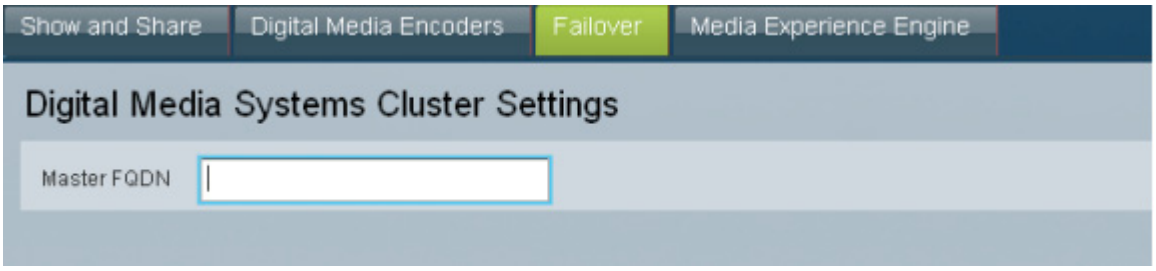
Step 2 Configure the secondary Cisco Show and Share appliance:

a. Using the **secondary FQDN** to access the secondary Cisco Show and Share interface, log in to Cisco Show and Share using the superuser or an administrator account.

b. From the Global Navigation menu, choose **Administration**.

c. Click the **Failover** tab.

d. Enter the DMM **primary FQDN** in the Master FQDN field. DO NOT use the alternate FQDN.



e. Click **Save**.

f. Exit Cisco Show and Share.

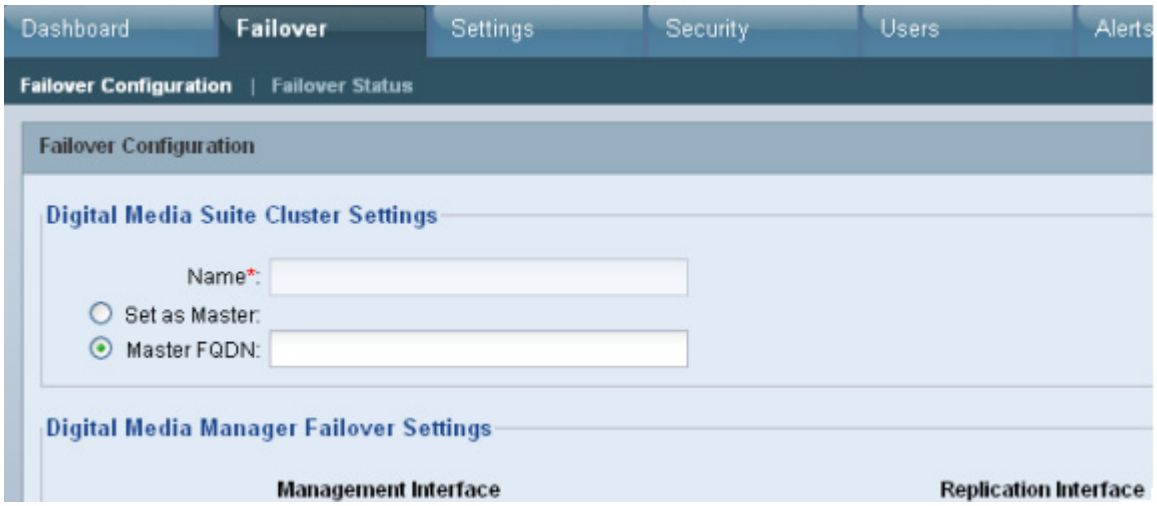
Step 3 Configure the secondary DMM appliance:

a. Using the **secondary FQDN** to access the secondary DMM interface, log in to DMM using the superuser or an administrator account.

b. From the home page, choose **Administration**.

c. Click the **Failover** tab.

The Failover Configuration page appears.



d. Verify that **Master FQDN** is selected in the Digital Media Suite Cluster Settings area and enter the DMM **primary FQDN** in the Master FQDN field. DO NOT use the alternate FQDN.

e. Click **Save**.

f. Exit DMM.

Configure the Primary DMM (Cluster Master)

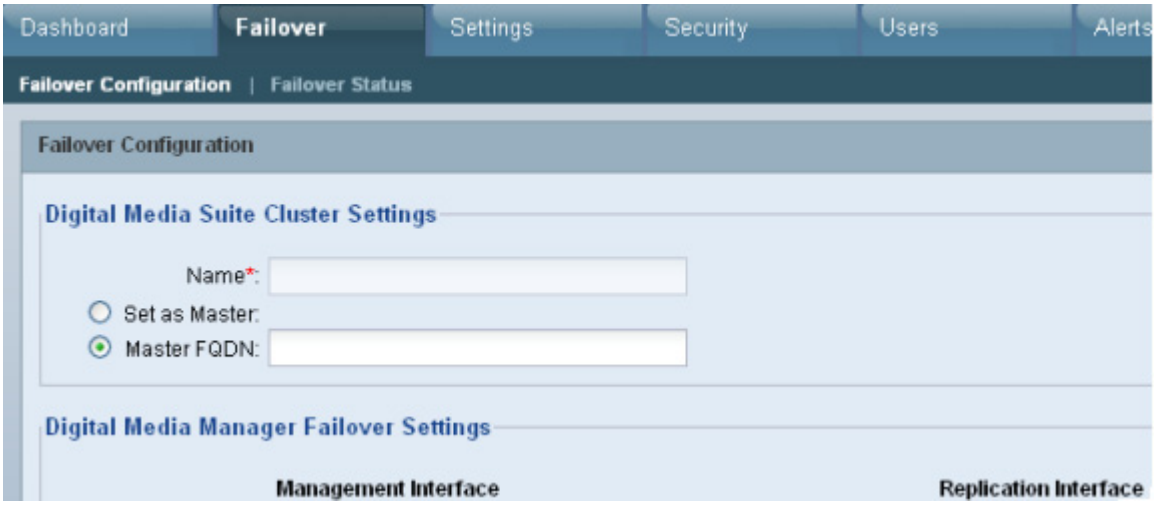
To configure the primary DMM, follow these steps:

Step 1 Using the **primary FQDN** to access the primary DMM interface, log in to DMM using the superuser or an administrator account.

Step 2 From the home page, choose **Administration**.

Step 3 Click the **Failover** tab.

The Failover Configuration page appears.



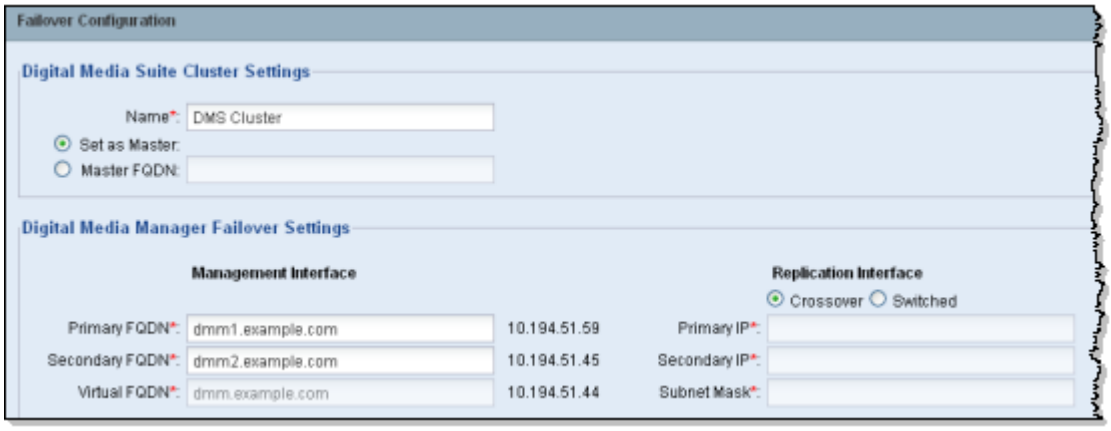
Step 4 Set the primary DMM as the cluster master:

a. Choose **Set as Master** in the Digital Media Suite Cluster Settings.

b. (Optional) Type a name for the cluster in the **Name** field. By default, the system assigns "DMS Cluster" as the cluster name.

Step 5 Configure the DMM failover settings:

Note The original primary DMM FQDN is automatically entered into the Virtual FQDN field. You cannot change the Virtual FQDN.



a. In the **Primary FQDN** field, replace the FQDN shown with the alternate primary FQDN.

b. Enter the secondary FQDN into the Secondary FQDN field.

c. Do one of the following to configure the DMM replication interface:

- If using a crossover cable between the devices, verify that Crossover is selected.
- If using a switch between the devices, select Switched and enter the following information:

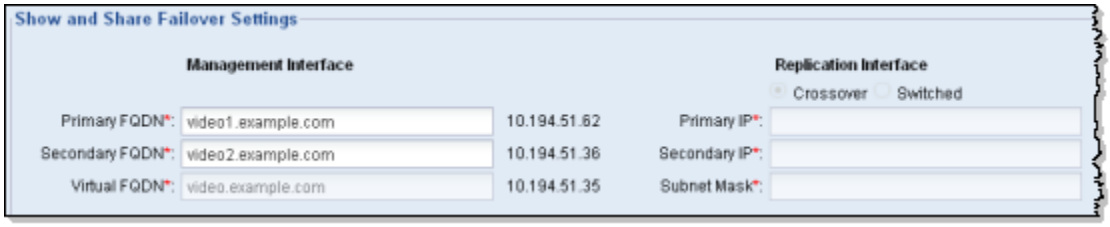
Primary IP	The IP address of the replication interface (1-Gb Ethernet management port) of the primary DMM.
Secondary IP	The IP address of the replication interface (1-Gb Ethernet management port) of the secondary DMM.
Subnet Mask	The address subnet mask

Step 6 Configure the Cisco Show and Share failover settings:

Note The original Primary FQDN is automatically entered into the Virtual FQDN field. You cannot change the Virtual FQDN.

a. In the **Primary FQDN** field, replace the primary FQDN shown with the alternate primary FQDN.

b. Enter the secondary FQDN into the Secondary FQDN field.



c. Do one of the following to configure the Cisco Show and Share appliance replication interface:

Note You must use the same type of replication interface (Crossover or Switched) as you are using for the DMM.

- If using a crossover cable between the devices, verify that Crossover is selected.
- If using a switch between the devices, select Switched and enter the following information:

Primary IP	The IP address of the replication interface (1-Gb Ethernet management port) of the primary DMM.
Secondary IP	The IP address of the replication interface (1-Gb Ethernet management port) of the secondary DMM.
Subnet Mask	The address subnet mask.

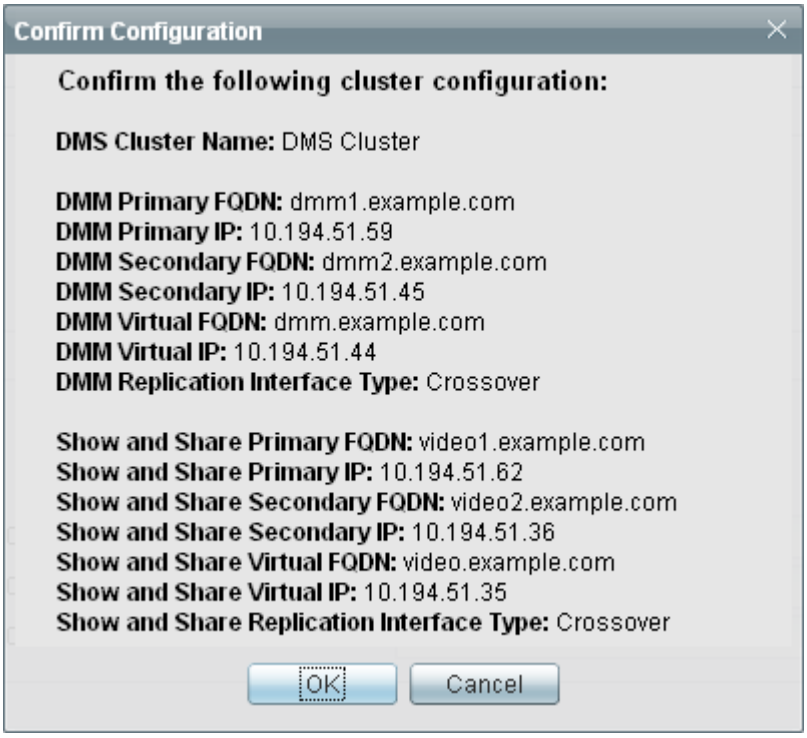
Step 7 Click **Save**.

Activate the Failover Cluster

When you activate the DMM cluster, the primary DMM configures and activates the other appliances in the failover cluster. Activation can take up to 20 minutes. After activation, the primary appliances are replicated to the secondary appliances. Replication process can take up to 15 hours. However, the primary appliances are available during replication and users can view and upload files as normal.

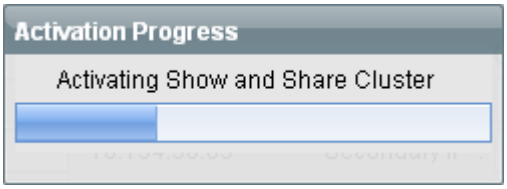
Step 1 Click **Activate**.

A dialog displays a summary of the failover cluster settings.



Step 2 Click **OK**.

The activation begins. A series of activation progress dialogs appear.



You cannot navigate away from this page by clicking in the interface while the activation is in progress. If you close the browser or use the browser navigation to move away from this page and then return, the Activate button appears to be enabled. However, if you attempt to activate again you will receive the message: `[FailoverConfig]: Another request already in progress.`

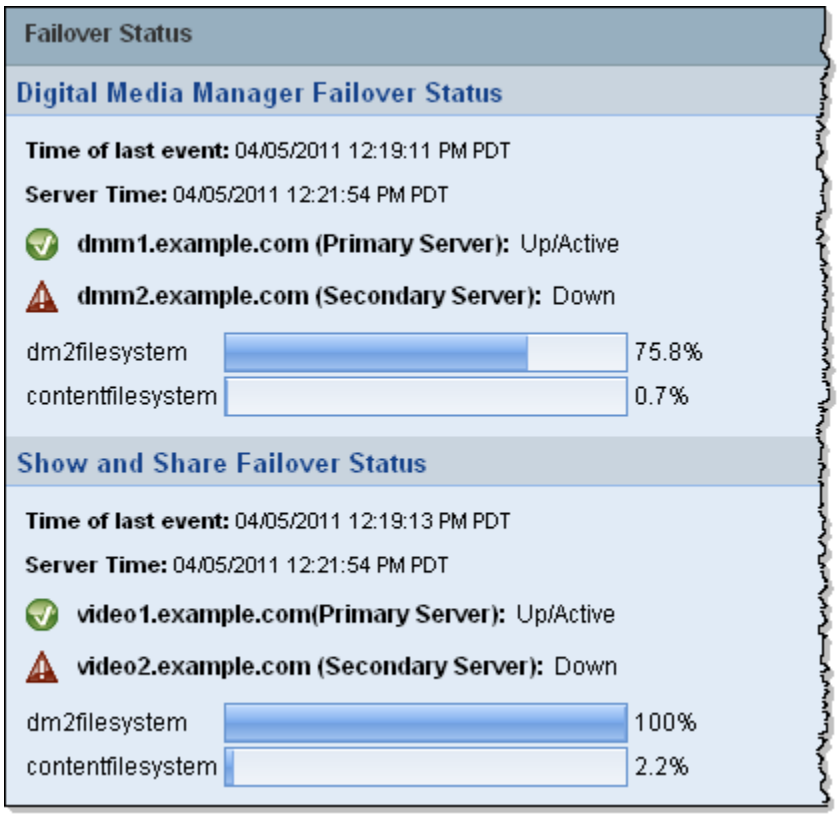
Activation can take up to 20 minutes. Once activation is complete, replication occurs. You can monitor replication progress on the Failover Status page. Replication can take up to 15 hours.

Monitor Replication and Verify the Configuration

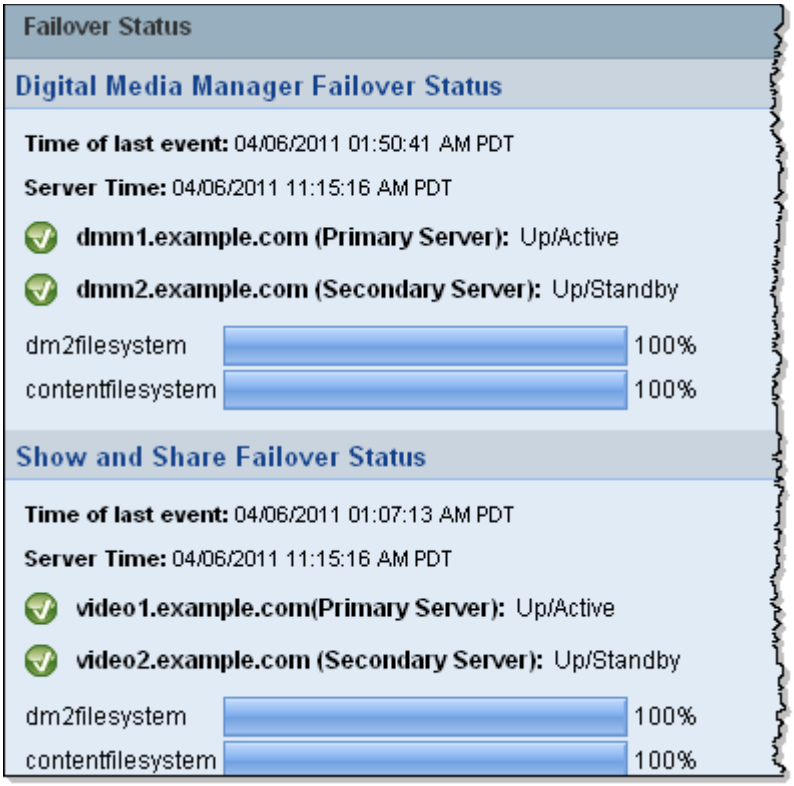
Go to the Failover Status page (**Administration > Failover > Failover Status**).

While replication is in progress, the primary appliances will be in the Up/Active state and the secondary appliances in the Down state. This is normal. You will see status bars that show the percent complete of the replication.

Note This page will not contain any information until activation is complete and replication has started.



When replication is complete, you should see the primary appliances in the Up/Active state and the secondary appliances in the Up/Standby state.



If any of the systems still in the Down state when replication has completed, access the down systems by using AAI and reboot the system. See the *Administration Guide for Cisco Digital Media Suite 5.3.x Appliances* on Cisco.com for more information about using AAI.

Back Up Your Cluster

You cannot restore backups taken from a standalone Cisco DMS configuration on a failover configuration. You should immediately back up the active appliances when activation and replication is complete.

See the *Backup and Restore Appliance Configuration* chapter in the *Administration Guide for Cisco Digital Media Suite 5.3.x Appliances* on Cisco.com.

How to Upgrade a Failover Configuration

If you are upgrading a Show and Share installation in failover configuration, you must complete the tasks in the order shown in Table 2-4.

Note Upgrade only when all nodes are Up: DMM nodes are Active/Standby and Show and Share nodes are Active/Standby.

Table 2-4 Workflow for Upgrading a Failover Configuration

—	Task	Reference
Step 1	In cluster mode, use the Virtual FQDNs of the active DMM and Show and Share appliances to log in to AAI and back up the appliances.	See the *Backup and Restore Appliance Configuration* chapter in the *Administration Guide for Cisco Digital Media Suite 5.3.x Appliances* on Cisco.com.
Step 2	Revert the configuration to Standalone mode on both the active and standby appliances.	1. Revert the standby appliances to Standalone mode: a. Log in to AAI. b. Choose FAIL_OVER > REVERT. 2. Revert the active appliances to Standalone mode: a. Log in to AAI. b. Choose FAIL_OVER > REVERT. 3. Apply the virtual FQDN and IP address to the primary appliances. This reverts them to the pre-failover configuration. 4. Pair the primary appliances. The primary appliances now operate as a standard, standalone configuration.
Step 3	Upgrade the primary DMM and Show and Share appliances.	See the *Release Notes for Cisco Show and Share and Digital Media Manager Release 5.5 or 5.6 on theMXA UCS M3 Server* on Cisco.com.
Step 4	Reimage the secondary DMM and Show and Share appliances. Install the same software release that you upgraded the primary appliances to.	—
Step 5	Configure failover again for your Show and Share installation.	See "Cisco Show and Share Failover Configuration" in this guide.

Monitoring and Controlling Failover

March 2015

This chapter contains these topics:

Failover Alerts

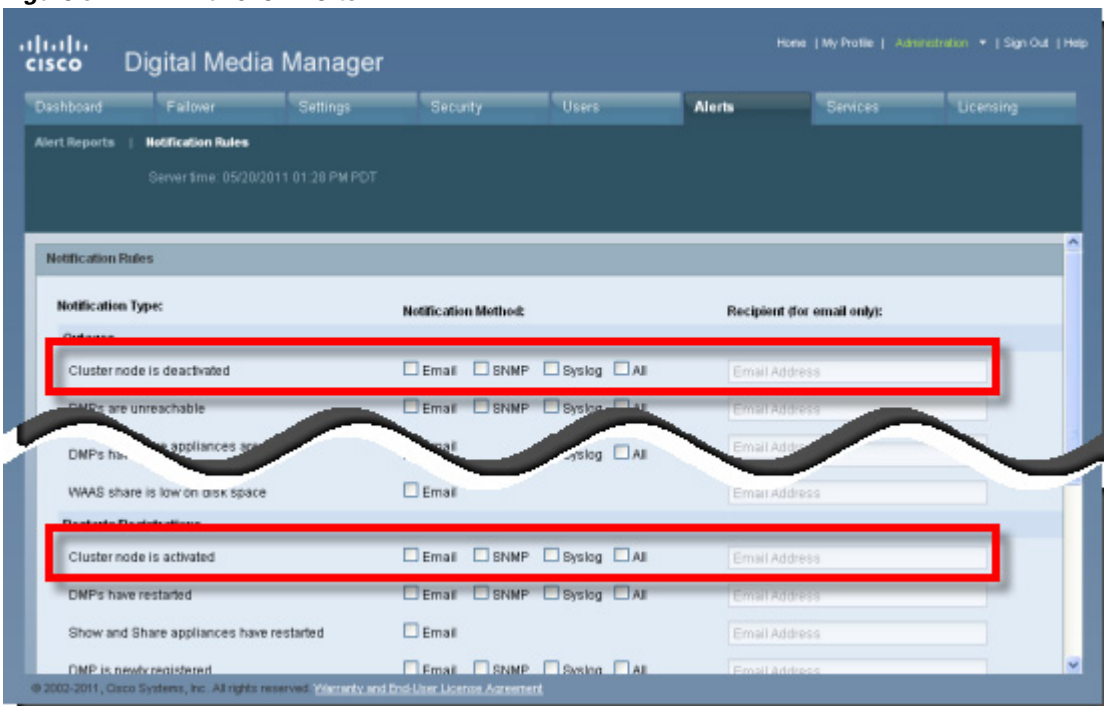
Two additional alerts have been added to the Cisco DMM Administration > Alerts > Notification Rules page to support failover:

- Cluster node is deactivated—When configured, this alert is triggered whenever an appliance in a failover configuration goes offline.
- Cluster Node is activated—When configured, this alert is triggered whenever an appliance in a failover configuration comes online.

When an appliance in a failover configuration fails, you will receive a cluster node down notification.

If you reboot an appliance, you will receive a cluster down notification followed by a cluster node activated notification for that appliance as the appliances reboots into the standby state.

Figure 3-1 Failover Alerts



See the *Events and Notifications Chapter* in the *User Guide for Cisco Digital Media Manager 5.3.x* for information about enabling events, configuring your SNMP server, and populating your MIB browser.

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dmm/user/guide/dmsug53x/eventnotify.html

For more information about each type of alert, see the following topics:

- SNMP Alerts, page 3-2
- Syslog Alerts, page 3-3
- E-Mail Alerts, page 3-3

SNMP Alerts

The following traps pertain to appliance Up/Down events:

- .1.3.6.1.4.1.9.9.655.0.6—cluster node down
- .1.3.6.1.4.1.9.9.655.0.5—cluster node up

Syslog Alerts

The following are sample UP/DOWN syslog alerts:

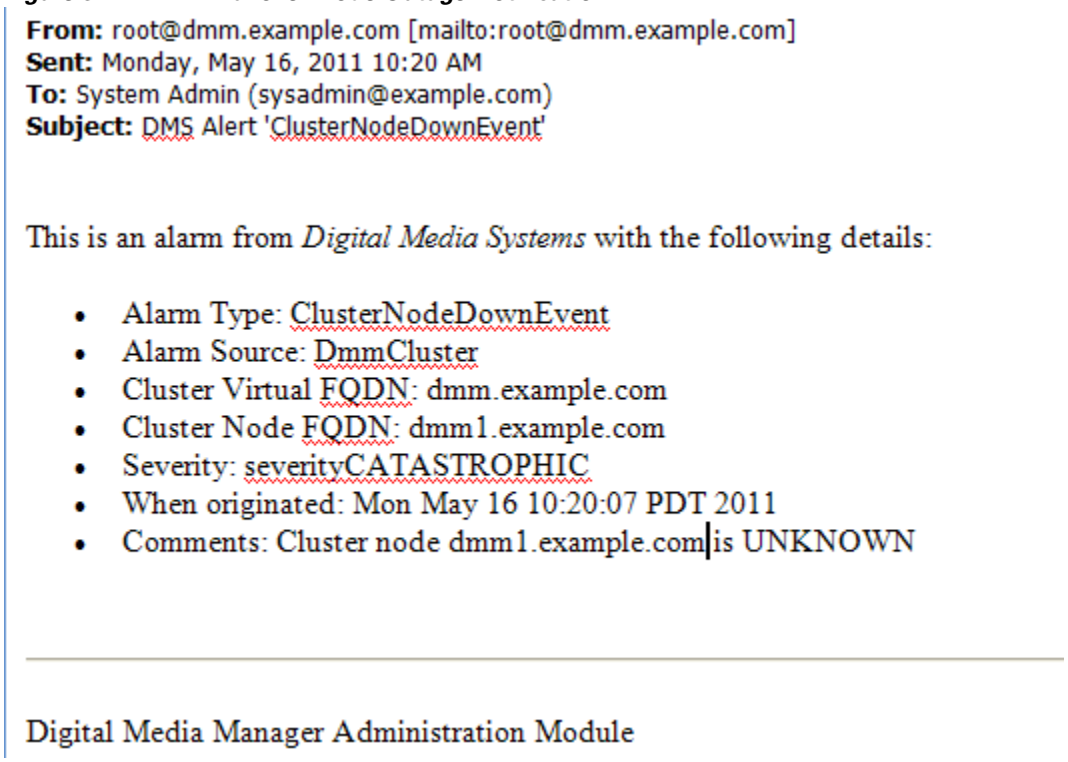
```
05-17-201110:56:42Local7.Debug10.0.0.1May 16 22:54:51 dmm.example.com
%DMS-1-ClusterNodeDownEvent: Cluster node dmm1.example.com is DOWN[DmmCluster] [
Original severity = severityCATASTROPHIC ]


05-17-201110:58:11Local7.Debug10.194.51.45May 16 22:56:21 dmm1.example.com
%DMS-1-ClusterNodeUpEvent: Cluster node dmm1.example.com is UP[DmmCluster] [ Original
severity = severityINFO ]
```

E-Mail Alerts

Figure 3-2 shows a typical event e-mail notification.

Figure 3-2 A Failover Node Outage Notification



From: root@dmm.example.com [mailto:root@dmm.example.com]
Sent: Monday, May 16, 2011 10:20 AM
To: System Admin (sysadmin@example.com)
Subject: DMS Alert 'ClusterNodeDownEvent'

This is an alarm from *Digital Media Systems* with the following details:

- Alarm Type: ClusterNodeDownEvent
- Alarm Source: DmmCluster
- Cluster Virtual FQDN: dmm.example.com
- Cluster Node FQDN: dmm1.example.com
- Severity: severityCATASTROPHIC
- When originated: Mon May 16 10:20:07 PDT 2011
- Comments: Cluster node dmm1.example.com is UNKNOWN

Digital Media Manager Administration Module

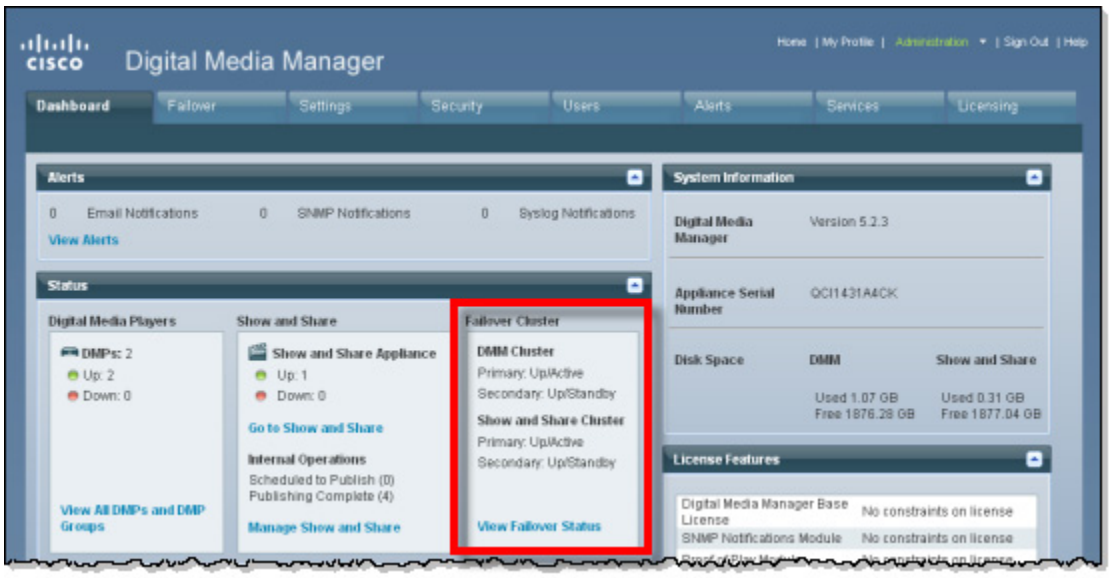
Table 3-1 shows the information that is sent by e-mail:

Table 3-1 Event E-Mail Notification Fields

Field	Description
Alarm Type	• ClusterNodeDownEvent—The appliance failed or has been taken offline. • ClusterNodeUpEvent—The appliance has come online and has entered the active or standby state.
Alarm Source	• DmmCluster—The alarm came from a Cisco DMM appliance. • VpCluster—The alarm came from a Cisco Show and Share appliance.
Cluster Virtual FQDN	The virtual FQDN of the appliance cluster.
Cluster Node FQDN:	The dedicated FQDN of the appliance.
Severity	• severityCATASTROPHIC—The appliance has experienced a failover event. • severityINFO—The message is an informational event (such as an UP message).
Comments:	The comment takes the form of: Cluster node *dedicated_fqdn* is *status* The *status* is one of the following values: • UNKNOWN—The appliance is transitioning between states. • UP—The appliance is up and in the active state. • DOWN—The appliance has failed. STANDBY—The appliance is up and in the standby state.

Monitoring Failover from Cisco DMM

The Cisco DMM home page displays a summary status of the failover cluster.



Click **View Failover Status** to go to the **Administration > Failover > Status** page.

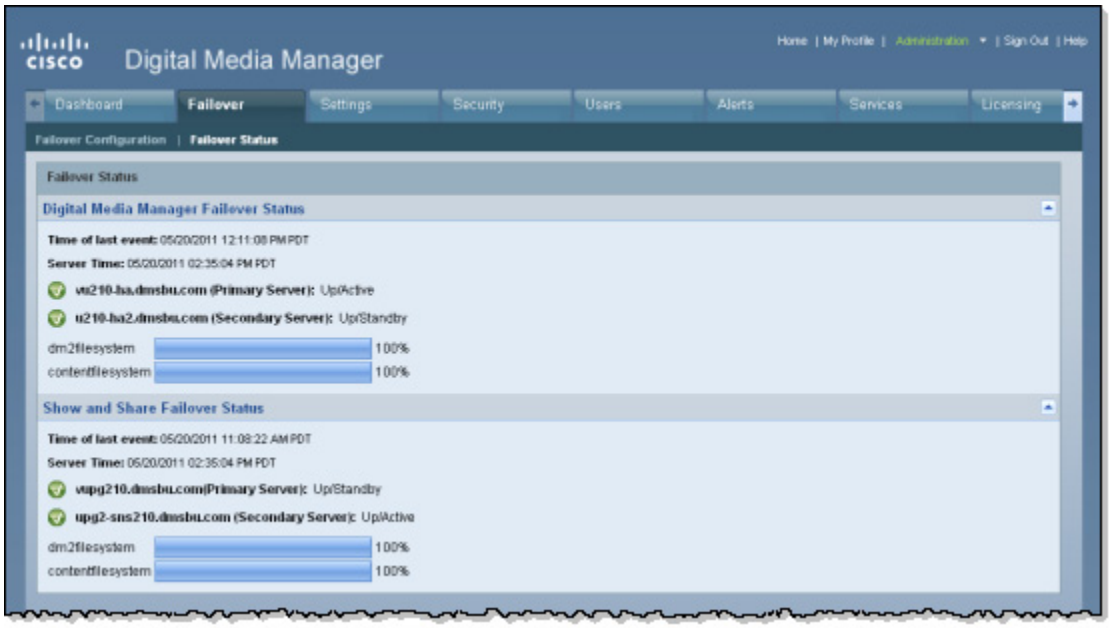


Table 3-2 provides the Failover Status information.

Table 3-2 Failover Status

Field	Description
Time of last event	The time (determined by the appliance time) of the last failover event.
Server Time	The time on the appliance.
Server status	For each server (Primary and Secondary), one of the following states: • Up/Active—The appliance is operating normally and is in the active state. • Up/Standby—The appliance is operating normally and is in the standby state. • Down—The appliance experienced a failover event and is currently in a failed state. Depending upon the failure, you may be able to access the appliance AAI interface. • Unknown—The appliance is transitioning between the UP and DOWN states.
Replication Status	The percentage complete the replication of information between the primary and secondary appliance. During initial activation, this value will be below 100 percent and the failover cluster is configured. During normal operation, this value should remain at 100 percent.

What to Look For on This Page

The following conditions indicate abnormal operation and should be investigated:

- An appliance in the Down state. Use the Cluster Resource Status, page 3-8 page to determine which resources have failed.
- An appliance in the Unknown state. This state indicates that the appliance is transitioning between UP and DOWN.
- One node down and and the message “No sync in progress”. There can be several causes for this. The failover cluster may be in Split Brain mode (see Split Brain Recovery, page 4-3, for information on how to confirm and recover from split brain)

  The active mode may have had a disk fail but not failed over. In this case, you can force a failover (see Forcing an Appliance to Fail Over, page 3-10) and then proceed with the recovery procedure (see Recovering from a Failover, page 4-1).

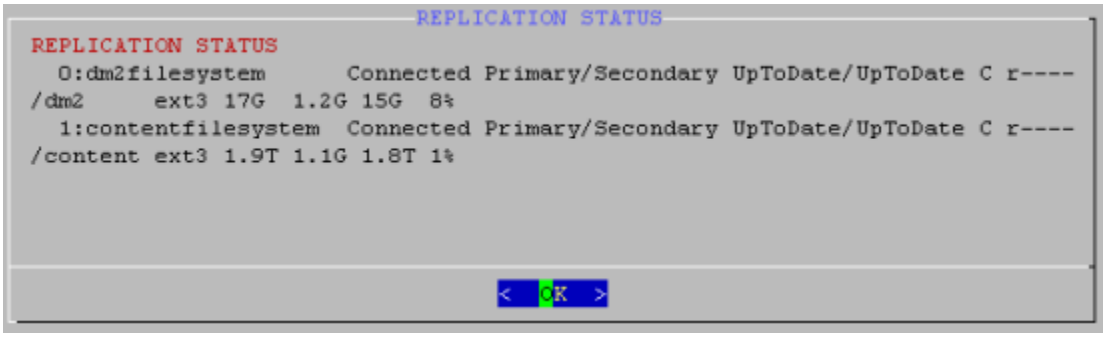
Monitoring Failover from AAI

You can monitor the following by using AAI:

- Replication Status, page 3-7
- Cluster Resource Status, page 3-8

Replication Status

The AAI replication status screen provides you with the same information as the Cisco DMM **Administration > Failover > Failover Status** page. You can use this screen to track the progress of data replication.



Procedure

To access the Replication Status screen, do the following:

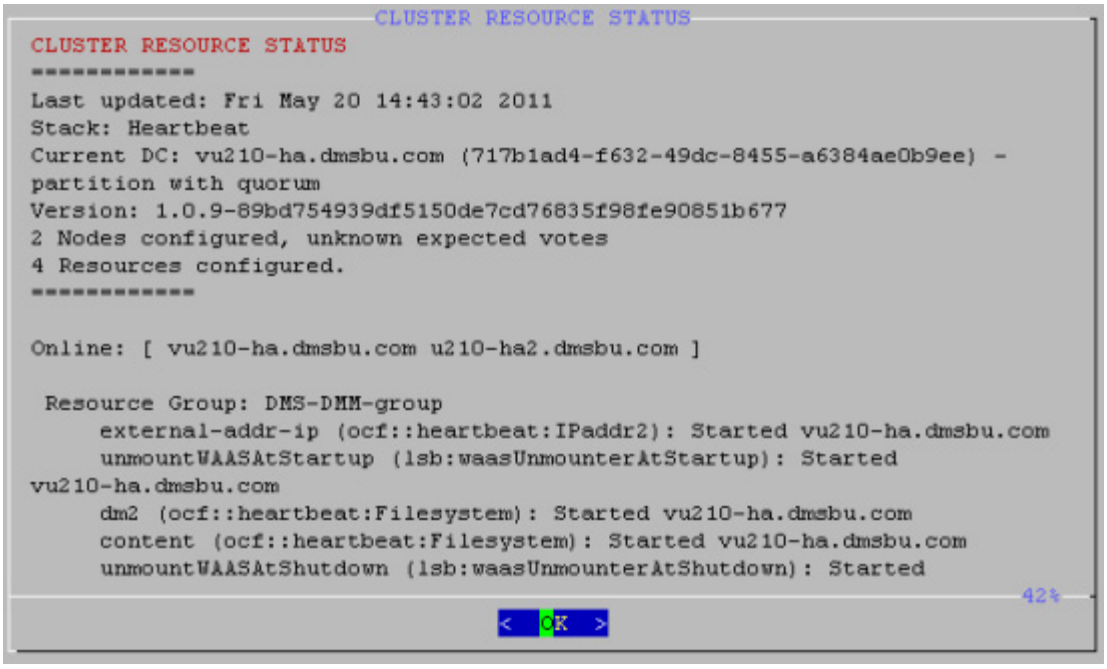
Step 1 Log in to AAI.

Step 2 Choose FAIL_OVER > STATUS > REPLICATION.

Cluster Resource Status

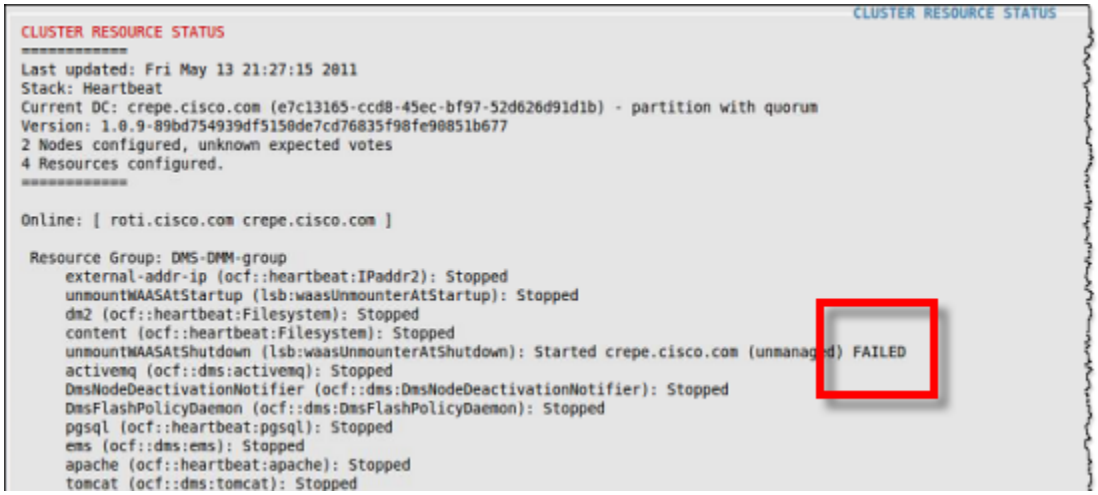
The cluster resource status screen displays the status of the monitored components and services. When determining the cause of a failover, use this screen to check the status of the monitored services.

- Services with a status of “Started” are operating normally.
- Services with a status of “Stopped” have failed.



When a service is shown as “unmanaged” or “failed”, the nodes should be restarted according to the following:

- UNMANAGED FAILED—Both nodes should be restarted, starting first with the node showing unmanaged, then the other node.
- FAILED—The node on which the resource is shown as Failed should be restarted.



The fail count for each service appears in the Migration summary section at the bottom of the screen:

Procedure

To access the Cluster Resource Status screen, do the following:

Step 1 Log in to AAI.

Step 2 Choose FAIL_OVER > STATUS > CLUSTER_RESOURCE.

Step 3 Use the up and down arrow keys to scroll through the displayed information.

Forcing an Appliance to Fail Over

To force an appliance to fail over, do the following:

Step 1 Log in to the active appliance AAI interface. Use the virtual FQDN or IP address to ensure that you are accessing the active appliance.

Step 2 Choose APPLIANCE_CONTROL > RESTART_OPTIONS > RESTART_WEB_SERVICES.

Restarting the web services on the active appliance triggers a failover to the secondary appliance. The appliance reboots to the standby state and uses the dedicated FQDN and IP address.

Recovering from a Failover

March 2015

This chapter contains these topics:

Minor Failure Event Recovery

A minor failure event is an event that caused a failover and can be cleared without replacing hardware or reimaging the appliance. Some examples include:

- A monitored service failing more than 5 times on the active unit.
- A service failed to start or stop.
- An external event, such as a network failure.
- A single disk failure is a minor failure. Replace the disk and reboot the appliance. If more than one disk fails, you have to perform a major failure event recovery.

When a failover occurs, clear the cause of the failover and reboot the failed appliance. It will boot to standby and receive data from the active unit. Rebooting the appliance also clears the monitored service fail counters.

If you cannot clear the condition that caused failover, you may have to perform a major event recovery.

Major Failure Event Recovery

Major failure events are events that require the appliance to be reimaged or replaced in order to bring it back into service.

If you need to replace hardware, obtain the replacement hardware before starting the recovery process. If you need to replace an appliance, you will need to obtain and install a new license for the appliance.

Note A single disk failure is a minor failure event. Multiple disk failures are a major failure event.

Caution You cannot revert a secondary appliance to standalone mode and then bring it back online as a primary appliance. When you convert a cluster to standalone mode, you must reimage the secondary appliances.

There are two major recovery procedures, depending upon which appliance failed:

- If a secondary appliance failed, see Secondary Appliance Failure Recovery, page 4-2.
- If a primary appliance failed, see Primary Appliance Failure Recovery, page 4-2.

Prerequisites

This procedure must be performed from the appliance console. You cannot perform this procedure through an SSH session.

Secondary Appliance Failure Recovery

To recover from a major failure event, you must:

Step 1 On the pair of appliances that did not fail, make the primary appliance the active appliance.

Step 2 Back up the active appliances in your failover cluster.

Step 3 Revert the active appliances to Standalone mode:

a. Log in to AAI.

b. Choose FAIL_OVER > REVERT.

Step 4 Revert the standby appliances to Standalone mode:

a. Log in to AAI.

b. Choose FAIL_OVER > REVERT.

Step 5 Apply the virtual FQDN and IP address to the primary appliances. This reverts them to the pre-failover configuration.

Step 6 Pair the primary appliances.

The appliances operate as a standard, standalone configuration.

Step 7 Reimage the secondary appliances.

Step 8 Re-configure failover. See Cisco Show and Share Failover Configuration, page 2-1 for the failover configuration process.

Primary Appliance Failure Recovery

Recovering a failed primary appliance requires additional steps because you cannot use a secondary appliance as a primary appliance. You must reimage secondary appliances after converting the failover cluster to standalone mode.

Procedure

Step 1 On the pair of appliances that did not fail, make the primary appliance the active appliance.

Step 2 Back up the active appliances in your failover cluster.

Step 3 Revert the standby appliances to Standalone mode:

a. Log in to AAI.

b. Choose FAIL_OVER > REVERT.

Step 4 Revert the active appliances to Standalone mode:

a. Log in to AAI.

b. Choose FAIL_OVER > REVERT.

Step 5 Reimage the failed primary appliance and the two standby appliances.

Step 6 Apply the virtual FQDN and IP address to the primary appliances. This reverts them to the pre-failover configuration.

Step 7 Pair the primary appliances.

Step 8 Restore the cluster backup on the appliances.

Step 9 Re-configure failover. See Cisco Show and Share Failover Configuration, page 2-1 for the failover configuration process.

Split Brain Recovery

Split brain occurs when both nodes become active or when the data on each node becomes out of sync with the other node. To recover, you need to determine which set of data you are going to keep. The recovery process overwrites one set of data.

Procedure

Step 1 Determine which device that will be used as the data source. This is the appliance whose data will be used to populate the cluster.

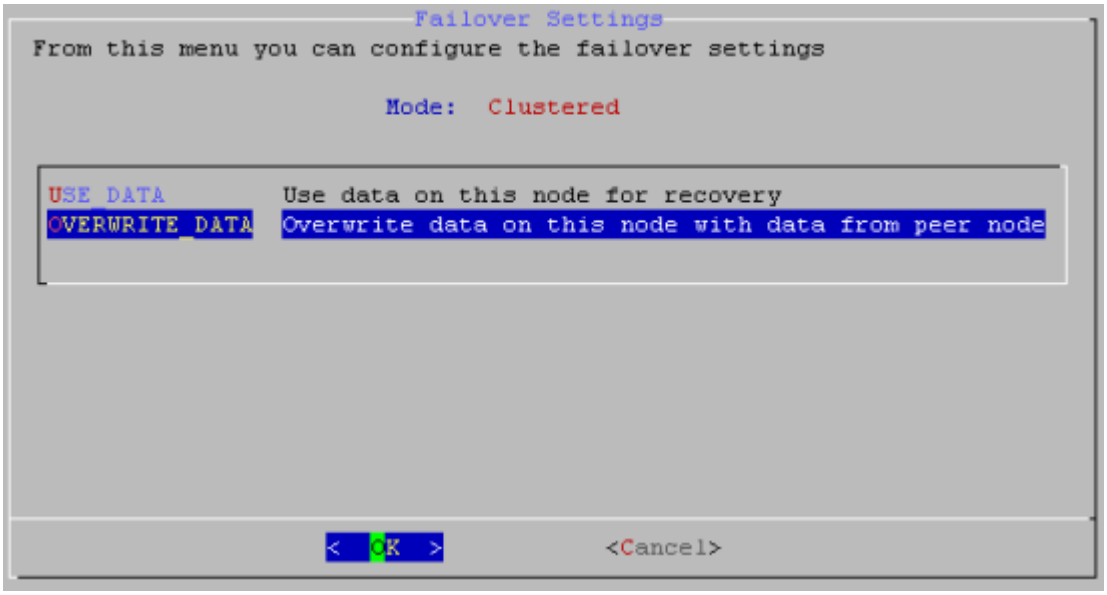
Step 2 On the appliance you want to receive the data, do the following:

a. Log in to AAI.

b. Choose **FAIL_OVER > RECOVER**.

If split brain is not occurring, you will receive a message that split brain was not detected. Cancel the split brain recovery process.

If split brain is occurring, the data selection page appears.



c. Choose **OVERWRITE_DATA**.

d. Choose **Yes** if prompted to continue.

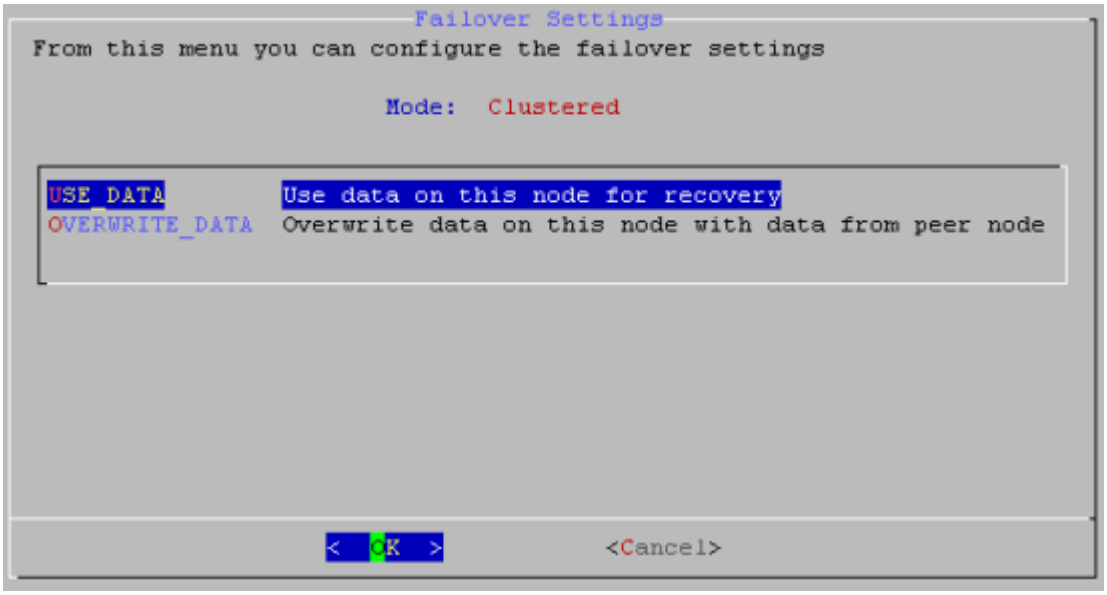
Step 3 On the appliance you are going to use as the data source, do the following:

a. Log in to AAI.

b. Choose **FAIL_OVER > RECOVER**.

If split brain is not occurring, you will receive a message that split brain was not detected. Cancel the split brain recovery process.

If split brain is occurring, the data selection page appears.



c. Choose **USE_DATA**.

d. Choose **Yes** if prompted to continue.

CHAPTER 5

Troubleshooting Failover Configurations

March 2015

Users cannot connect to the active server.

Make sure that the users are pointing to the virtual FQDN. If they are using the dedicated FQDN, they may be attempting to connect to an appliance that is in the Standby state.

NTP warning when trying to activate the failover cluster.

Warning: You cannot activate failover on the cluster because NTP is not enabled on the following node(s): {list}. Use the AAI interface to configure NTP on the specified devices before activating failover.

NTP must be enabled on the appliances before you can activate failover. Use AAI to enable NTP on your appliances, then attempt to activate the cluster again.

"Failed to Resolve" error appears next to the FQDN fields on the primary Cisco DMM failover configuration page.

If you receive a `Failed to Resolve` error for an IP address while configuring the primary DMM, do the following:

1. Make sure that the FQDN entry exists in your DNS server and that the DNS server is reachable from your cluster appliances.
2. Make sure that the entry in the field is correct.
3. Make sure that you do not have any trailing spaces in the FQDN fields on the cluster master.
4. Make sure that you do not have any trailing spaces in the Master FQDN fields on the non-master devices.

The secondary Cisco Show and Share appliance fails to start after initial configuration and activation.

After the initial configuration, activation, and data replication, the standby Cisco Show and Share appliance appears in the Down state.

Confirm that the replication is at 100 percent for both appliance pairs in the cluster. Reboot the Cisco Show and Share server by using the AAI interface (and the dedicated IP address or FQDN).

The appliance will reboot into the Up/Standby state.

Activation fails.

When using the switched configuration for the replication interface, make sure that the replication interface is on a different subnet from the application interface.

In the Cisco DMM failover status page, one server appears to be down and the replication stats displays "No sync in progress".

In AAI, check the replication status. If at least one partition shows "standalone" instead of "connected", you are in Split Brain Mode. See Split Brain Recovery, page 4-3, for information about how to recover.

Primary DMM does not send a "down" SNMP notification.

However, when the standby becomes active, an "Up" notification is sent; look for "Up" notification without a corresponding "Down" notification. You can configure other forms of notifications in addition to SNMP.

"Failed to detect DRBD sync - aborting cluster setup"

This message appears when one of the following occurs:

- The Ethernet link for the replication interface is below 1000 Mbps. If the interfaces are connected through a switch, make sure that the switch interfaces are configured for 1000 Mbps.
- The crossover cable is not connected.
- The switch between the appliance replication interfaces is not reachable.

FQDNs revert to IP addresses during configuration

The appliance is unable to resolve the FQDN. Check connectivity to your DNS server, verify that the FQDN is configured in your DNS server, and check the network settings on your appliance. If you are experiencing this problem, you can save your failover settings, but failover activation will fail.

Unable to publish cluster configuration to node

Make sure that the cluster master has been specified on the node.

Unable to obtain system information from node

The node is not reachable from the cluster master or the web services are down on that node.

Using REBOOT_APPLIANCE causes split-brain

When you use REBOOT_APPLIANCE from AAI, split brain may occur.

You can resolve the split brain by using this procedure: Split Brain Recovery, page 4-3.

To avoid causing split brain, avoid using REBOOT_APPLIANCE in AAI. If you want to cause a failover, you can use RESTART_WEB_SERVICES or RESTART_DATABASE_SERVICES. If you need to reboot the appliance, hard reboot it.

Primary FQDN and Secondary FQDN reverted back to IP addresses after Activation failed.

This is caused by the DNS configuration for the server IP address and FQDN. Make sure that your DNS server can perform both DNS and reverse DNS lookup for the IP addresses and FQDNs.