Failover Configuration Guide for Cisco Digital Media Suite 5.4.x

January 8, 2014

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.

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.

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 NONINFRINGEMENT 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.

Failover Configuration Guide for Cisco Digital Media Suite 5.4.x

CONTENTS

CHAPTER 1 **About Failover** 1-1

- Overview 1-1
  - Cisco DMS Failover Terminology 1-1
  - Supported Failover Configurations 1-2
  - Failover Triggers 1-3
  - The Failover Process 1-4
- Limitations and Restrictions 1-4
- Important Notes for Failover Configuration 1-7
- What to Do Next 1-7

CHAPTER 2 **Configure Failover for Cisco Digital Signs** 2-1

- Prerequisites 2-1
  - Licensing Requirements 2-1
  - Hardware Requirements 2-2
  - Configuration Requirements 2-2
- Pre-Configuration Worksheet 2-2
- Configure Failover 2-3
  - Set Up the Primary DMM Appliance 2-4
  - Set up the Secondary DMM Appliance 2-4
  - Connect the Primary and Secondary Appliance Replication Interfaces 2-4
  - Configure the Secondary Cisco DMM Appliance 2-5
  - Configure the Primary DMM 2-5
  - Activate the Failover Cluster 2-6
  - Monitor Replication Status 2-7
- Back Up Your Cluster 2-7

CHAPTER 3 **Monitor and Control Failover** 3-1

- Failover Alerts 3-1
  - SNMP Alerts 3-2
  - Syslog Alerts 3-2
  - E-Mail Alerts 3-3
- Monitor Failover from Cisco DMM 3-4
- Monitor Failover from AAI 3-5
  - Replication Status 3-5

Cluster Resource Status 3-6

Force a Unit to Fail Over 3-8

CHAPTER 4 Recover from a Failover 4-1

Recover from a Minor Failure Event 4-1

Recover from a Major Failure Event 4-1

Recover from Secondary Appliance Failure 4-2

Recover from Primary Appliance Failure 4-2

Recover from a Split-Brain Condition 4-3

CHAPTER 5 Troubleshoot Failover Configurations 5-1

Users cannot connect to the active server 5-1

NTP warning when trying to activate the failover cluster 5-1

“Failed to Resolve” error appears next to the FQDN fields on the primary Cisco DMM failover configuration page 5-1

Activation fails 5-2

On the failover status page in DMM, one server appears to be down and the replication status says, “No sync in progress” 5-2

Primary DMM does not send a “down” SNMP notification 5-2

“Failed to detect DRBD sync - aborting cluster setup” 5-2

FQDNs revert to IP addresses during configuration 5-2

Unable to publish cluster configuration to node 5-2

Unable to obtain system information from node 5-2

Using REBOOT_APPLIANCE causes split-brain 5-3

Primary FQDN and Secondary FQDN reverted to IP addresses after Activation failed. 5-3

CHAPTER 1

About Failover

Revised: January 8, 2014

This chapter describes how to configure two Cisco DMS appliances so that one will take over operation if the other one fails.

This chapter includes these sections.

- Overview, page 1-1
- Limitations and Restrictions, page 1-4
- Important Notes for Failover Configuration, page 1-7
- What to Do Next, page 1-7

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 these conditions are met, failover occurs.

This section contains these topics.

- Cisco DMS Failover Terminology, page 1-1
- Supported Failover Configurations, page 1-2
- Failover Triggers, page 1-3
- The Failover Process, page 1-4

Cisco DMS Failover Terminology

The following terms are used throughout this document to describe failover configurations.

- **Active appliance**—The appliance that is currently responding to user requests. Always access the active appliances using the virtual IP address and virtual FQDN.
- **Application interface**—the interface on a Cisco DMM appliance that users connect to. Health monitoring also occurs through this interface.

- **Dedicated FQDN**—an FQDN that is assigned to the appliance. This FQDN remains with the appliance during a failover. The appliance is reachable through this 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 Cisco DMM 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 happen through this interface. You cannot access the Cisco DMM 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 the ones you add 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 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

Failover is supported for Cisco Digital Signs implementations.

A Cisco Digital Signs implementation requires that the primary Cisco DMM appliance is paired with a secondary Cisco DMM appliance that acts as a standby appliance. The application interfaces (GigabitEthernet 1) of the appliances must be on the same subnet. The two appliances are connected by either a crossover cable (see Figure 1-1) or a switch (Figure 1-2) on their GigabitEthernet 2 interfaces. This connection is used to monitor failover health and replicate data between them.

Figure 1-1 Digital Signs Failover with a Crossover Cable

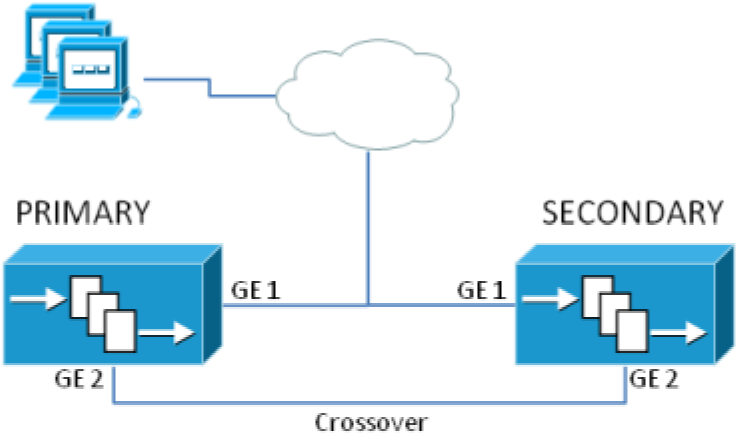
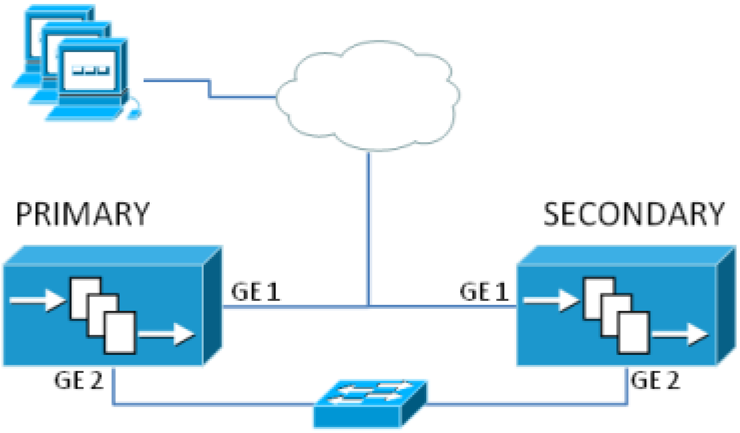


Figure 1-2 Digital Signs Failover with a Switch



For detailed information on how to configure Cisco Digital Signs failover, see Configure Failover for Cisco Digital Signs, page 2-1.

Failover Triggers

The following events trigger failover:

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

  Heartbeat messages are sent once a second. Missing 10 consecutive heartbeats causes a failover.
- Manually restarting the following services using the AAI interface:
  - 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 Recover from a Minor Failure Event, 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 Recover from a Major Failure Event, page 4-1 for more information about recovering from a disk failure.

The Failover Process

The following events happen during failover:

1. A failover event occurs. This causes the active appliance to go into a down or unknown state, depending upon the type of failure. A "down" notification is sent.
2. The standby appliance becomes the active starts using the virtual FQDN and IP address.
3. The new active appliance restarts the application services. This can take up to 3 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 3 minutes before they can log back into the web interface.

Limitations and Restrictions

- The application interface of each pair of appliances 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 have a Cisco Show and Share appliance-only failover configuration.
- 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.
- 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.
- You need to configure Garbage Collector (GC) log in AAI (see Figure 1-3 and Figure 1-4) and configure external syslog through DMM GUI (see Figure 1-5) on both primary server and secondary server before cluster activation, to make sure that the functions work as expected. If the failover cluster has already been activated, configure the GC log and external syslog server on the active server, and then trigger a failover to configure the same settings on the standby server. Because the external syslog server page configuration is not porting as part of DRBD sync.

Figure 1-3 GC Log Option in AAI

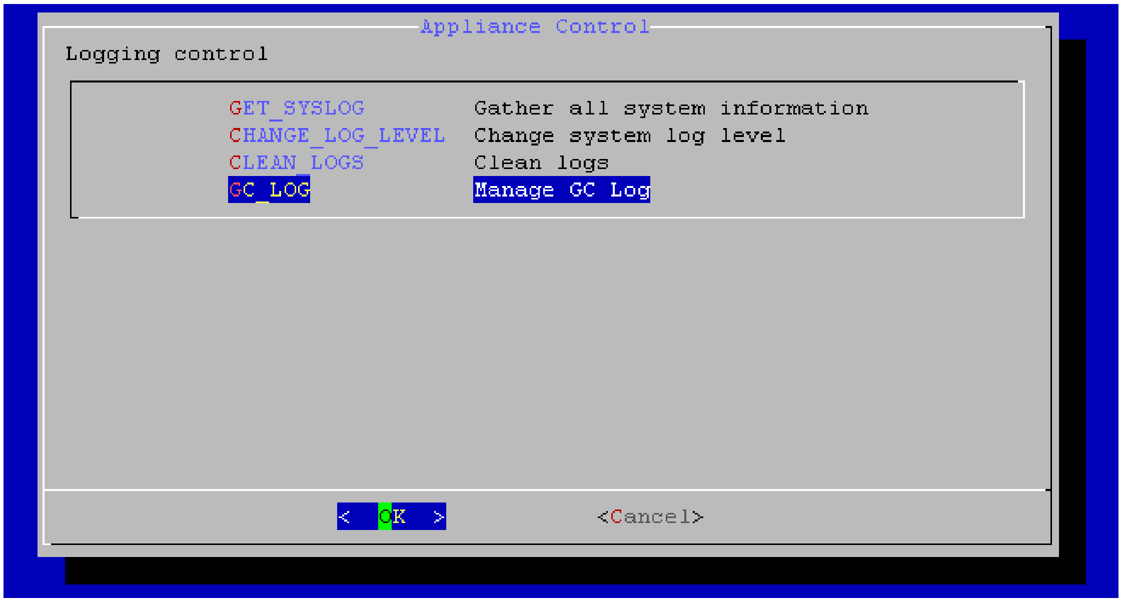
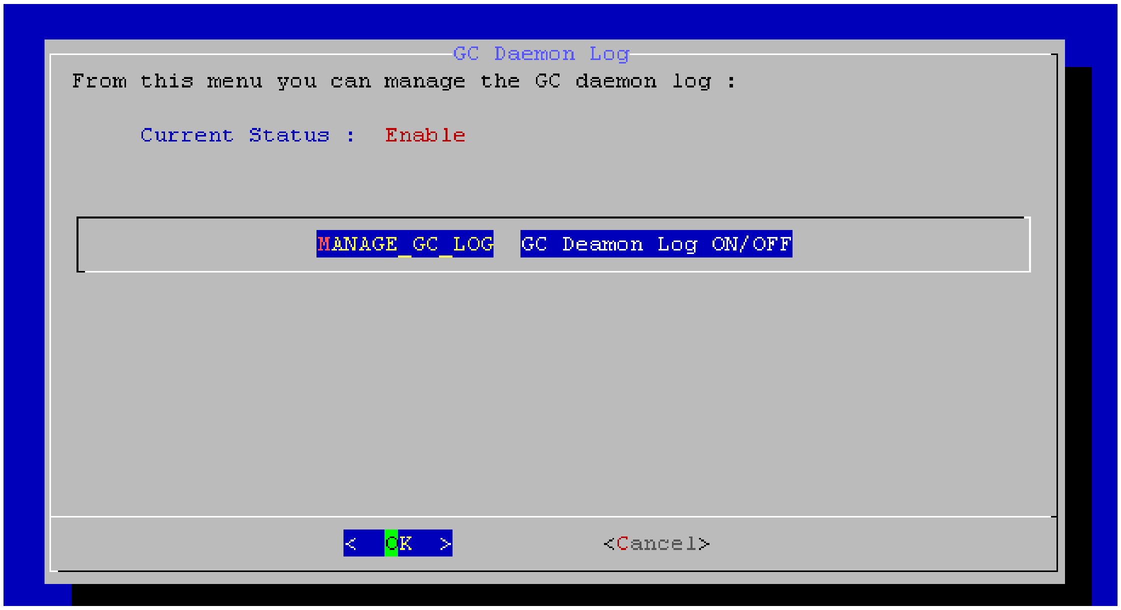


Figure 1-4 GC Log Configuration



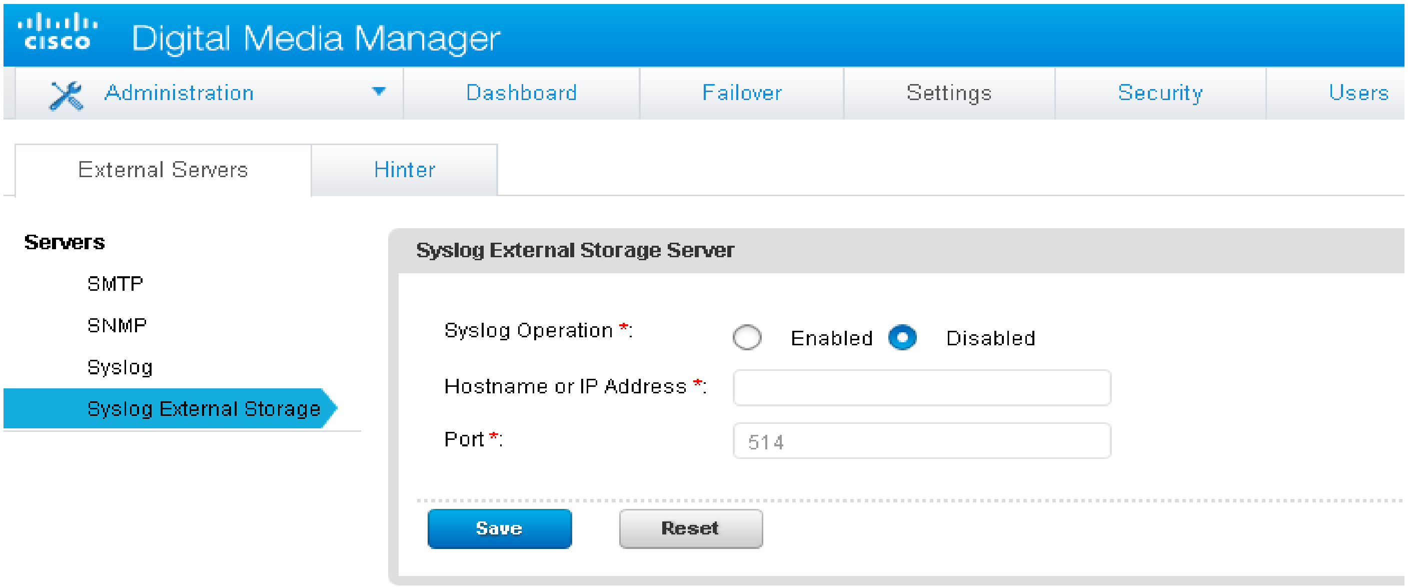
```
GC Daemon Log
From this menu you can manage the GC daemon log :

    Current Status :  Enable

        MANAGE_GC_LOG   GC Deamon Log ON/OFF

        <  OK  >            <Cancel>
```

Figure 1-5 External Syslog Server Configuration



Syslog External Storage Server

Syslog Operation *: ○ Enabled ● Disabled

Hostname or IP Address *:

Port *: 514

Important Notes for Failover Configuration

- Install external certificates on the primary pair of appliances before configuring failover. When the certificates expire, use the virtual FQDN when obtaining new certificates. Install the new certificates using the virtual FQDN to access the AAI interface.
- Back up your failover cluster (using the virtual FQDN to access AAI) immediately after configuring failover. Backups taken in standalone mode cannot be restored on a failover cluster.
- When using a switched interface for the replication interface connection, you need to make sure that the latency between the active and standby device is no more than 10 seconds. Latency of greater than 10 seconds will cause 10 consecutive heartbeat messages to be missed, initiating a failover.
- 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 when the standby appliance becomes active it will contain the correct data.
- In a switched configuration, the switch interfaces connected to the replication interfaces must be configured for 1000 Mbps.

What to Do Next

- To configure failover for a Cisco Digital Signs implementation, see Configure Failover for Cisco Digital Signs, page 2-1
- To configure alerts and monitor your appliances, see Monitor and Control Failover, page 3-1.
- To recover from a failover event, see Recover from a Failover, page 4-1.

Configure Failover for Cisco Digital Signs

Revised: January 8, 2014

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

This chapter contains these topics.

- Prerequisites, page 2-1
- Pre-Configuration Worksheet, page 2-2
- Configure Failover, page 2-3
- Back Up Your Cluster, page 2-7

Prerequisites

Before you can configure failover, you must meet these requirements.

- Licensing Requirements, page 2-1
- Hardware Requirements, page 2-2
- Configuration Requirements, page 2-2

Licensing Requirements

When licensing your failover cluster, you must install the feature, author, and failover licenses on the primary Cisco DMM appliance. The secondary appliance needs only the base license that come with the appliance. It will inherit the optional feature, device, and author licenses during the failover activation process.

Devices	Licenses Needed
Primary Cisco DMM appliance	• (Optional) Feature licenses (SNMP Notification Module, etc.) • (Optional) Device Licenses • Failover License
Secondary Cisco DMM appliance	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 following for information about installing licenses:

http://www.cisco.com/en/US/docs/video/digital_media_systems/5_x/5_4/dmm/user/guide/admin/licenses.html for information about installing licenses.

Hardware Requirements

Failover configuration is supported on the following DMS hardware platforms:

- DMM-SVR-C210-K9

You cannot configure failover for the following DMS hardware platforms:

- MCS-7835-H3

The primary and secondary appliance 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 number for Cisco DMM appliance.

Primary Appliance	Secondary Appliance
Cisco Digital Media Manager DMM-SVR-C210-K9	DMM-FA-C210-K9

Configuration Requirements

- Configure NTP on the appliances before configuring failover.
- You must add the required FQDNs to your name server before configuring failover.

Pre-Configuration Worksheet

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

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 users will use to access the DMM. This FQDN becomes the virtual FQDN for the Cisco DMM failover cluster.

Table 2-2 DMM Failover Pre-Configuration Worksheet

Item	Value	Notes
Primary Appliance IP Address		For existing installations, this is the IP Address of the existing appliance. For new installations, this is the IP address users will use 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 will be applied to the primary appliance after the original FQDN becomes the DMM virtual FQDN.
Primary Appliance Alternate, Dedicated IP Address		This is the IP address that will be applied to the primary appliance after 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 that 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 that interface on the secondary appliance.

Note Please make sure that all "A" records in DNS have corresponding "PTR" (reverse zone) configured correctly. This is required for DMM and failover setup to work properly.

Configure Failover

To configure failover for your DMS installation, perform the following procedures in the order presented:

1. Set Up the Primary DMM Appliance, page 2-4
2. Set up the Secondary DMM Appliance, page 2-4
3. Connect the Primary and Secondary Appliance Replication Interfaces, page 2-4
4. Configure the Secondary Cisco DMM Appliance, page 2-5
5. Configure the Primary DMM, page 2-5
6. Activate the Failover Cluster, page 2-6
7. Monitor Replication Status, page 2-7

Set Up the Primary DMM Appliance

When you have an existing DMM appliance, its existing FQDN and IP address will become the virtual FQDN and IP address for the failover configuration. Users will not need to change their bookmarks.

When you are setting up a new Cisco DMM appliance, set up the primary DMM as you would a standalone system. See *Quick Start Guide for Cisco Digital Media Suite 5.4.x* for information about setting up the appliance.

When setting up the appliance, use the primary FQDN and IP address for the appliance. They will become the virtual FQDNs and IP address during the failover configuration process. In a later step, you will replace the primary FQDNs and IP addresses used here with the alternate, dedicated FQDNs and IP addresses.

Before you continue to the next step, make sure you:

- Install the failover license on the DMM. See the Licenses chapter in *User Guide for Cisco Digital Media Manager 5.4.x*.
- Install third party certificates on your appliances if you are using them. See the Manage Digital Certificates chapter in *Administration Guide for Cisco Digital Media Suite 5.4.x Appliances*.
- Enable NTP on the appliances. See the Configure System Time chapter in *Administration Guide for Cisco Digital Media Suite 5.4.x Appliances*.

Set up the Secondary DMM Appliance

Set up the secondary DMM Appliance as you would a standalone system. See *Quick Start Guide for Cisco Digital Media Suite 5.4.x* for information about setting up the system.

Use the secondary appliance dedicated FQDN and IP address for the appliance.

The application interfaces for both DMM appliances must be on the same subnet as the primary DMM appliance.

Install the base licenses installed that came with the appliance. You do not need to install additional feature or device licenses on the secondary DMM appliance.

Connect the Primary and Secondary Appliance Replication Interfaces

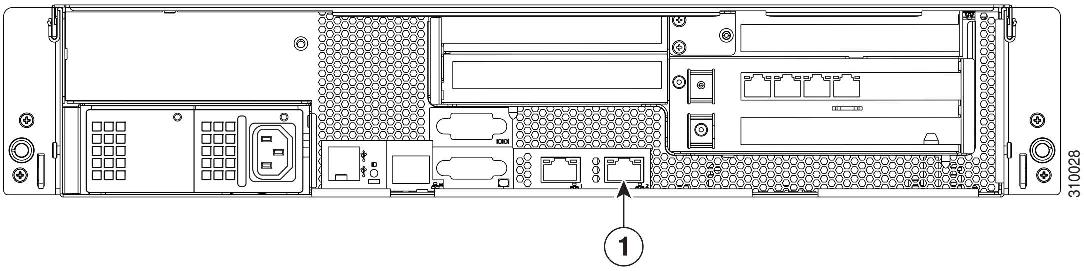
You have two options for connecting the primary and secondary appliance replication interfaces:

- 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.

GigabitEthernet 2 is the replication interface. Figure 2-1 shows the location of the replication interface (marked by the arrow labeled 1) on a Cisco DMM-SVR-C210-K9 appliance.

Figure 2-1 The replication interface on a DMM-SVR-C210-K9 appliance



Configure the Secondary Cisco DMM Appliance

Configure the secondary appliance to recognize the primary Cisco DMM appliance as the cluster master.

Procedure

Step 1 Using the **secondary FQDN** to access the secondary DMM interface, log into 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 Verify that **Master FQDN** is selected in the Digital Media Suite Cluster Settings area and enter the **primary appliance FQDN** in the Master FQDN field. DO NOT use the alternate FQDN.

Step 5 Click **Save**.

Step 6 Exit the DMM interface.

Configure the Primary DMM

To configure the primary DMM, follow these steps:

Step 1 Using the **primary FQDN** to access the primary DMM interface, log into 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.

Step 6 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 (GigabitEthernet 2) of the primary DMM.
Secondary IP	The IP address of the replication interface (GigabitEthernet 2) of the secondary DMM.
Subnet Mask	The subnet mask of the addresses.

Step 7 Click **Save**.

What to do next

Next, see Activate the Failover Cluster, page 2-6.

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.

Procedure

Step 1 Click **Activate**.

A dialog displays a summary of the failover cluster settings.

Step 2 Click **OK**.

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.

What to do next

- Monitor the replication progress and verify your configuration. See Monitor Replication Status, page 2-7.

Monitor Replication Status

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

While replication is in progress, the primary appliance 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.

During replication, users can access and use the Cisco DMM GUI. However, performance will be degraded.

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 the secondary system is in the Down state when replication has completed, access the system AAI interface reboot the system. See *Administration Guide for Cisco Digital Media Suite 5.4.x Appliances* on Cisco.com for information about using AAI.

Back Up Your Cluster

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

See the Back Up and Restore Appliance Configurations chapter in *Administration Guide for Cisco Digital Media Suite 5.3.4 Appliances*.

Monitor and Control Failover

Revised: January 8, 2014,

This chapter contains these sections.

- Failover Alerts, page 3-1
- Monitor Failover from Cisco DMM, page 3-4
- Monitor Failover from AAI, page 3-5
- Force a Unit to Fail Over, page 3-8

Failover Alerts

Two alerts on the Cisco DMM Administration > Alerts >Notification Rules page 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.

When 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.

For information about enabling events, configuring your SNMP server, and populating your MIB browser, see *the Events and Notifications* chapter in *User Guide for Cisco Digital Media Manager 5.4.x*:

http://cisco.com/en/US/docs/video/digital_media_systems/5_x/5_3/dmm/user/guide/admin/eventnotify.html

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

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

SNMP Alerts

For information about enabling events, configuring your SNMP server, and populating your MIB browser, see *the Events and Notifications* chapter in *User Guide for Cisco Digital Media Manager 5.4.x*:

http://cisco.com/en/US/docs/video/digital_media_systems/5_x/5_3/dmm/user/guide/admin/eventnotify.html

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:

```
05-17-2011 10:56:42   Local7.Debug   10.0.0.1       May 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 ]
```

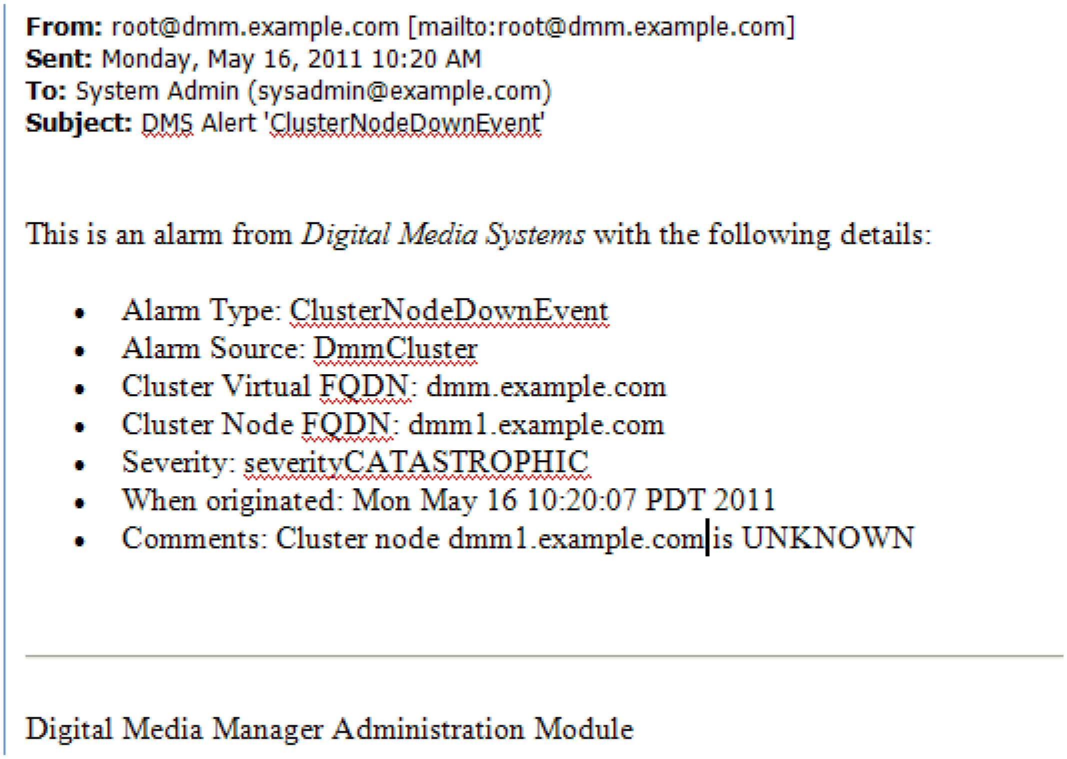
For information about enabling events, configuring your SNMP server, and populating your MIB browser, see *the Events and Notifications* chapter in *User Guide for Cisco Digital Media Manager 5.4.x*:

http://cisco.com/en/US/docs/video/digital_media_systems/5_x/5_3/dmm/user/guide/admin/eventnotify.html

E-Mail Alerts

Figure 3-1 shows a typical event e-mail notification.

Figure 3-1 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

The following information is set by e-mail:

Table 3-1 Event E-Mail Notification Fields

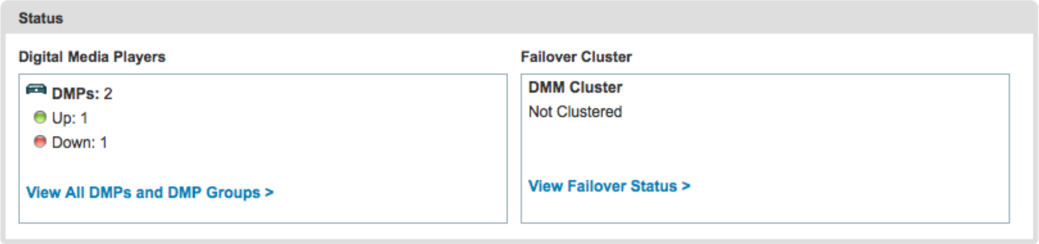
Field	Description
Alarm Type	• ClusterNodeDownEvent—The appliance failed or been taken offline. • ClusterNodeUpEvent—The appliance has come online and has entered the active or standby state.
Alarm Source	• DmmCluster—The alarm came from a Cisco DMM appliance.
Cluster Virtual FQDN	The virtual FQDN of the appliance cluster.
Cluster Node FQDN:	The dedicated FQDN of the appliance.

Table 3-1 Event E-Mail Notification Fields

Field	Description
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.

Monitor Failover from Cisco DMM

The Administration Dashboard in Cisco DMM shows a summary status of your failover cluster.



Status

Digital Media Players

DMPs: 2
● Up: 1
● Down: 1

View All DMPs and DMP Groups >

Failover Cluster

DMM Cluster
Not Clustered

View Failover Status >

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

The Failover Status screen provides the following 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.

Table 3-2 Failover Status

Field	Description
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% and the failover cluster is configured. During normal operation, this value should remain at 100%

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 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 Recover from a Split-Brain Condition, 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 Force a Unit to Fail Over, page 3-8) and then proceed with the recovery procedure (see Recover from a Failover, page 4-1).

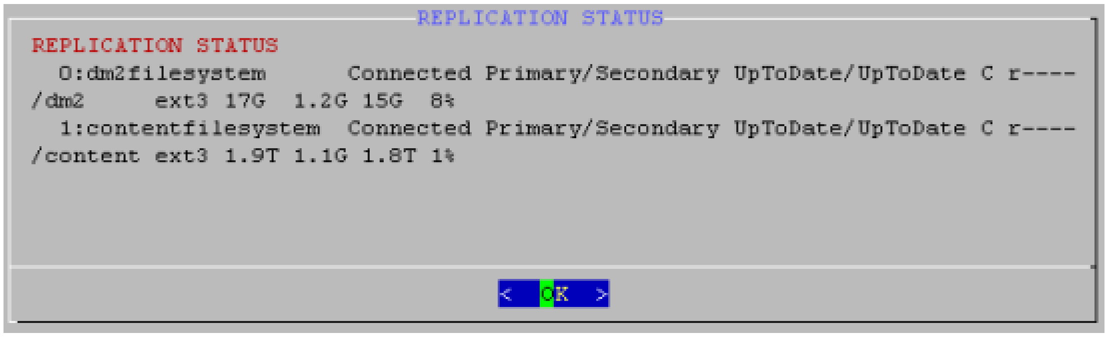
Monitor Failover from AAI

You can monitor the following using AAI:

- Replication Status, page 3-5
- Cluster Resource Status, page 3-6

Replication Status

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



```
REPLICATION STATUS
  0:dm2filesystem      Connected Primary/Secondary UpToDate/UpToDate C r----
/dm2      ext3 17G  1.2G 15G  8%
  1:contentfilesystem  Connected Primary/Secondary UpToDate/UpToDate C r----
/content ext3 1.9T 1.1G 1.8T 1%
```

Procedure

To access the Replication Status screen, do the following:

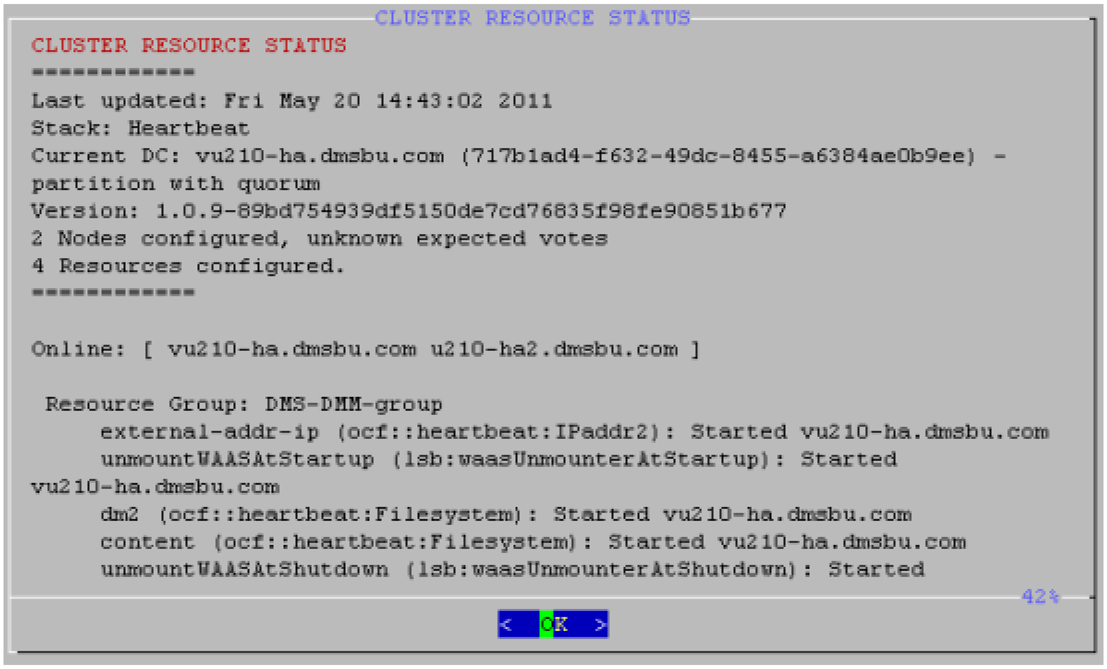
Step 1 Log into AAI.

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.



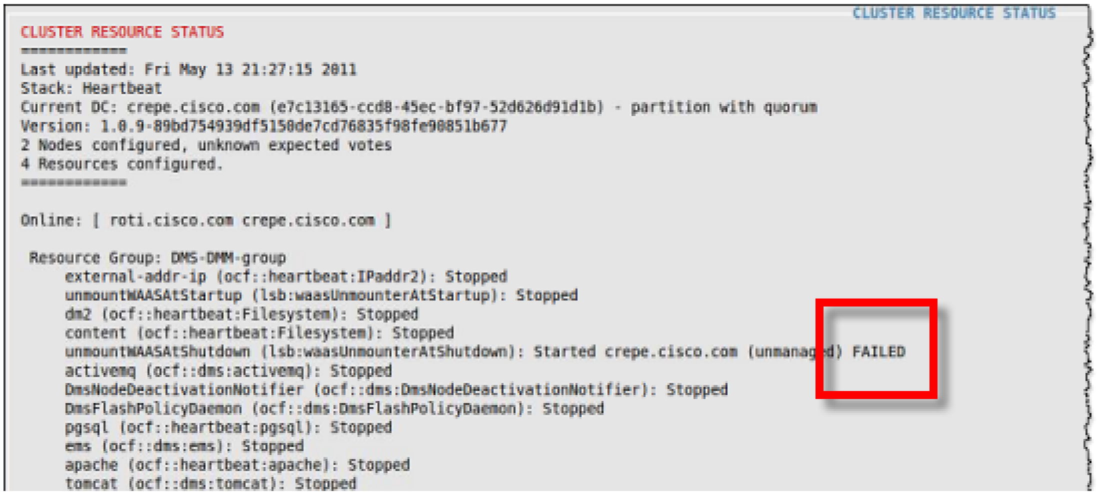
```
CLUSTER RESOURCE STATUS
============
Last updated: Fri May 20 14:43:02 2011
Stack: Heartbeat
Current DC: vu210-ha.dmsbu.com (717b1ad4-f632-49dc-8455-a6384ae0b9ee) -
partition with quorum
Version: 1.0.9-89bd754939df5150de7cd76835f98fe90851b677
2 Nodes configured, unknown expected votes
4 Resources configured.
============

Online: [ vu210-ha.dmsbu.com u210-ha2.dmsbu.com ]

 Resource Group: DMS-DMM-group
     external-addr-ip (ocf::heartbeat:IPaddr2): Started vu210-ha.dmsbu.com
     unmountWAASAtStartup (lsb:waasUnmounterAtStartup): Started
vu210-ha.dmsbu.com
     dm2 (ocf::heartbeat:Filesystem): Started vu210-ha.dmsbu.com
     content (ocf::heartbeat:Filesystem): Started vu210-ha.dmsbu.com
     unmountWAASAtShutdown (lsb:waasUnmounterAtShutdown): Started
```

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.
- FAILED - The node on which resource is shown as Failed should be restarted.

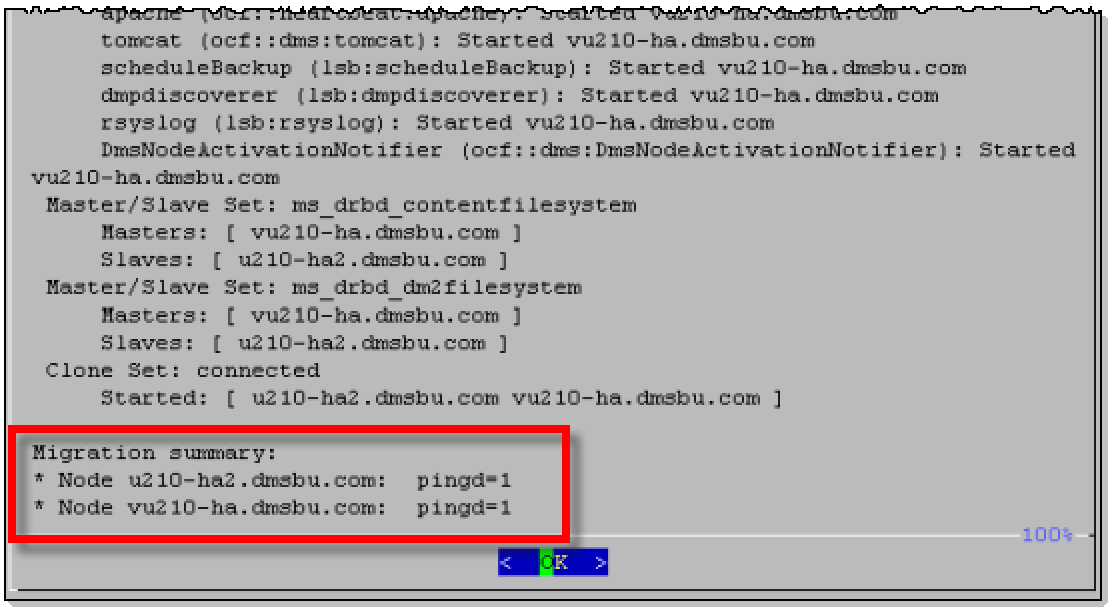


```
CLUSTER RESOURCE STATUS
============
Last updated: Fri May 13 21:27:15 2011
Stack: Heartbeat
Current DC: crepe.cisco.com (e7c13165-ccd8-45ec-bf97-52d626d91d1b) - partition with quorum
Version: 1.0.9-89bd754939df5150de7cd76835f98fe90851b677
2 Nodes configured, unknown expected votes
4 Resources configured.
============

Online: [ roti.cisco.com crepe.cisco.com ]

 Resource Group: DMS-DMM-group
     external-addr-ip (ocf::heartbeat:IPaddr2): Stopped
     unmountWAASAtStartup (lsb:waasUnmounterAtStartup): Stopped
     dm2 (ocf::heartbeat:Filesystem): Stopped
     content (ocf::heartbeat:Filesystem): Stopped
     unmountWAASAtShutdown (lsb:waasUnmounterAtShutdown): Started crepe.cisco.com (unmanaged) FAILED
     activemq (ocf::dms:activemq): Stopped
     DmsNodeDeactivationNotifier (ocf::dms:DmsNodeDeactivationNotifier): Stopped
     DmsFlashPolicyDaemon (ocf::dms:DmsFlashPolicyDaemon): Stopped
     pgsql (ocf::heartbeat:pgsql): Stopped
     ems (ocf::dms:ems): Stopped
     apache (ocf::heartbeat:apache): Stopped
     tomcat (ocf::dms:tomcat): Stopped
```

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



```
        apache (ocf::heartbeat:apache): Started vu210-ha.dmsbu.com
        tomcat (ocf::dms:tomcat): Started vu210-ha.dmsbu.com
        scheduleBackup (lsb:scheduleBackup): Started vu210-ha.dmsbu.com
        dmpdiscoverer (lsb:dmpdiscoverer): Started vu210-ha.dmsbu.com
        rsyslog (lsb:rsyslog): Started vu210-ha.dmsbu.com
        DmsNodeActivationNotifier (ocf::dms:DmsNodeActivationNotifier): Started
vu210-ha.dmsbu.com
 Master/Slave Set: ms_drbd_contentfilesystem
        Masters: [ vu210-ha.dmsbu.com ]
        Slaves: [ u210-ha2.dmsbu.com ]
 Master/Slave Set: ms_drbd_dm2filesystem
        Masters: [ vu210-ha.dmsbu.com ]
        Slaves: [ u210-ha2.dmsbu.com ]
 Clone Set: connected
        Started: [ u210-ha2.dmsbu.com vu210-ha.dmsbu.com ]

Migration summary:
* Node u210-ha2.dmsbu.com:   pingd=1
* Node vu210-ha.dmsbu.com:   pingd=1
```

Procedure

To access the Replication Status screen, do the following:

Step 1 Log into AAI.

Step 2 Choose **FAIL_OVER > STATUS > CLUSTER_RESOURCE**.

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

Force a Unit to Fail Over

To force a unit to fail over, do the following:

Step 1 Log into the active appliance AAI interface. Use the virtual FQDN or IP address to ensure 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.

CHAPTER 4

Recover from a Failover

Revised: January 8, 2014

Recover from a Minor Failure Event

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 stopped.
- 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.

Recover from a Major Failure Event

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

Prerequisites

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

Recover from Secondary Appliance Failure

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

Step 5 Pair the primary appliances.

The appliances operate as a standard, standalone configuration.

Step 6 Reimage the secondary appliances.

Step 7 Re-configure failover. See Configure Failover for Cisco Digital Signs, page 2-1, for the failover configuration process.

Recover from Primary Appliance Failure

Recovering a failed primary requires some additional steps because you cannot use a secondary appliance as a primary appliance. You must reimage the 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 into AAI.

b. Choose **FAIL_OVER > REVERT**.

Step 4 Revert the active appliances to Standalone mode:

a. Log into 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 Configure Failover for Cisco Digital Signs, page 2-1, for the failover configuration process.

Recover from a Split-Brain Condition

Split brain occurs when both nodes become active or when the data on each node become 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 the other set of data.

Procedure

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

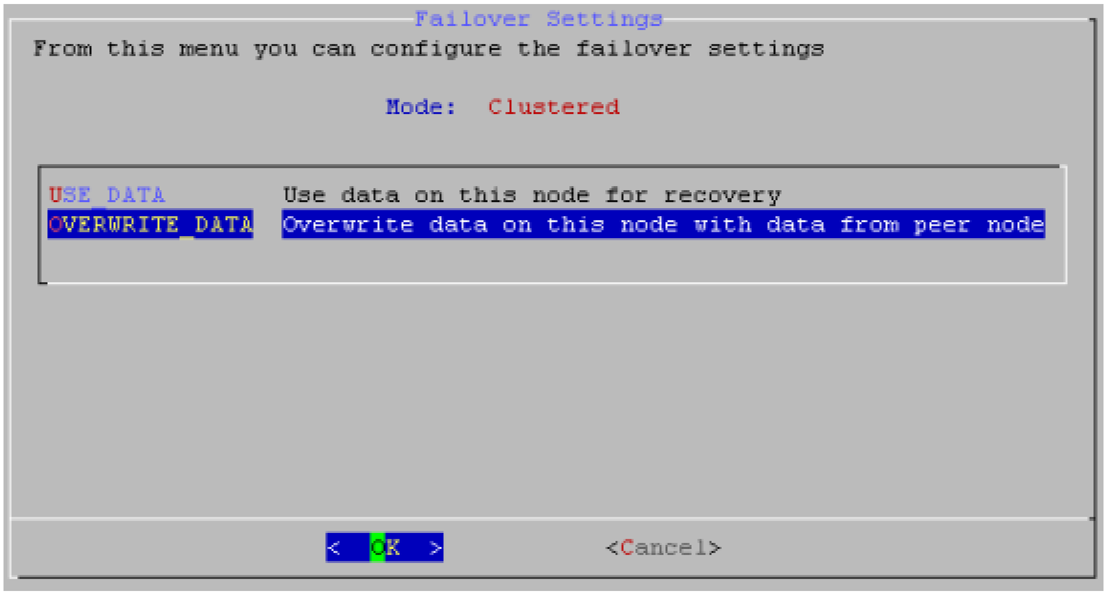
Step 2 On the appliance you want to receive the data, do the following:

a. Log into AAI.

b. Choose **FAIL_OVER > RECOVER**.

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

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



```
Failover Settings
From this menu you can configure the failover settings

Mode:  Clustered

USE_DATA         Use data on this node for recovery
OVERWRITE_DATA   Overwrite data on this node with data from peer node
```

c. Choose **OVERWRITE_DATA**.

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

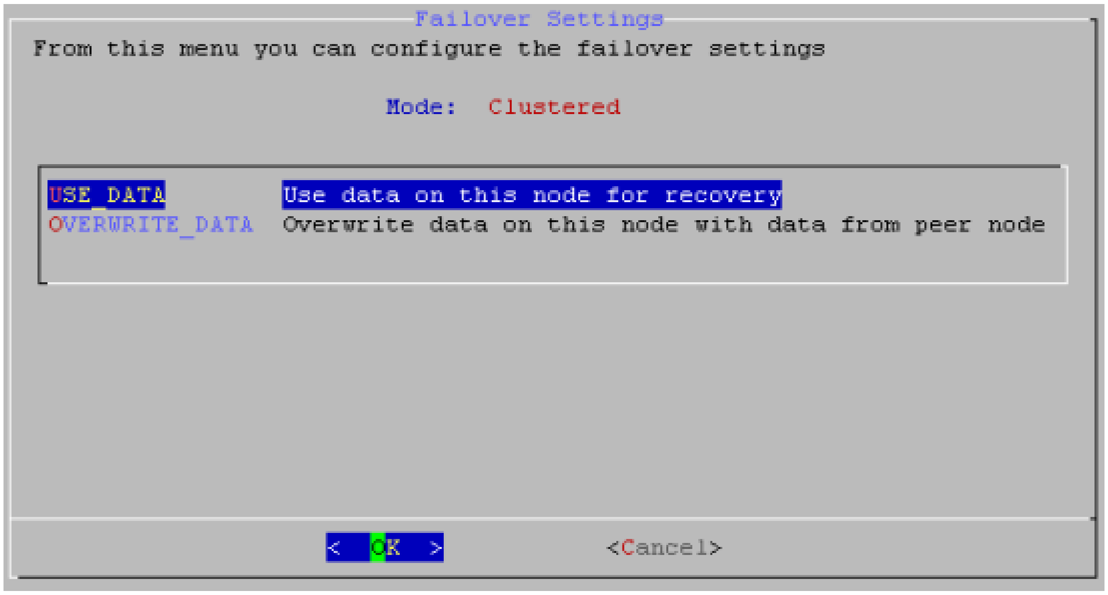
Step 3 On the appliance you are going to use as the data source, do the following:

a. Log into AAI.

b. Choose **FAIL_OVER > RECOVER**.

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

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



```
Failover Settings
From this menu you can configure the failover settings

                  Mode:  Clustered

USE_DATA         Use data on this node for recovery
OVERWRITE_DATA   Overwrite data on this node with data from peer node
```

c. Choose **USE_DATA**.

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

CHAPTER 5

Troubleshoot Failover Configurations

Revised: January 8, 2014

Users cannot connect to the active server

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

Activation fails

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

On the failover status page in DMM, one server appears to be down and the replication status says, "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 Recover from a Split-Brain Condition, 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. Additionally, 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 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 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: Recover from a Split-Brain Condition, 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 to IP addresses after Activation failed.

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