Cisco SME Cluster Management

The Cisco Fabric Manager provides a web-browser interface that displays real-time views of your network fabrics and lets you configure Cisco Storage Media Encryption with easy-to-use wizards. This chapter contains information about Cisco SME initial configuration and the tasks that are used to manage Cisco SME clusters using Cisco Fabric Manager.

This chapter contains the following sections:

- About SME Cluster Management, page 4-1
- Creating a Cisco SME Cluster Using the Cisco SME Wizard, page 4-1
- Deactivating and Purging a Cisco SME Cluster, page 4-20
- Viewing Cisco SME Cluster Details, page 4-23
- Viewing Cluster Information Using Fabric Manager Client, page 4-28
- Viewing Cluster Information Using Device Manager, page 4-29
- Cluster Quorum and Master Switch Election Overview, page 4-30
- In-Service Software Upgrade (ISSU) in a Two-Node Cluster, page 4-33

About SME Cluster Management

An SME cluster consists of a group of MDS switches running the SME application in a single fabric environment where each switch is a member or node. The cluster infrastructure enables the SME application to offer high availability and load balancing by providing the ability to communicate and coordinate with the other members to maintain a consistent and distributed view of the application’s configuration and operational state.

The process of configuring Cisco SME on an MDS switch with an installed MSM-18/4 module or on a Cisco MDS 9222i switch involves a number of configuration tasks that should be followed in chronological order. See the topics in the Before You Begin online help in Fabric Manager Web Server. Refer to Chapter 2, “Getting Started” and Chapter 3, “Cisco SME Interface Configuration” for information about the tasks that must be completed before creating a Cisco SME cluster.

Creating a Cisco SME Cluster Using the Cisco SME Wizard

The Cisco SME Wizard is an easy-to-use interface that walks you through the process of creating a Cisco SME cluster. The following sections describe the steps in this process:
Launching Cisco SME Wizard

To launch the Cisco SME wizard, follow these steps:

**Step 1** Open the web browser to the Fabric Manager Web Client. Log in with the user name and password. For login information, refer to the *Cisco Fabric Manager Fundamentals Configuration Guide.*
Step 2  In the Fabric Manager Web Client, click the SME tab.

Step 3  Select Clusters in the navigation pane.

Step 4  Click Create in the information pane.

The Cisco SME wizard launches to walk you through the easy configuration process.

**Choosing a Cluster Name**

In the Choose Name screen, enter a cluster name. Click Next.

---

**Note**

Cluster names must not contain spaces or special characters.
Selecting Fabrics

In the Select Fabrics screen, highlight the fabric you want to include in the cluster. Click **Next**.

Selecting Interfaces

In the Select Interfaces screen, highlight the SME interfaces you want to include in your cluster. Click **Next**. For information about adding interfaces, see Chapter 3, “Cisco SME Interface Configuration.”

**Note**
Cisco MDS SAN-OS Release 3.2(2c) or later, or Cisco NX-OS 4.x supports one cluster per switch.
Selecting Master Key Security Levels

There are three master key security levels: Basic, Standard, and Advanced. Standard and Advanced security levels require smart cards. Table 4-1 describes the master key security levels.

---

**Caution**

You cannot modify the cluster security level after a cluster is created. Before confirming the cluster creation, you will be prompted to review the cluster details. At that time, you can return to modify the security level.

---

**Note**

For information on cluster security, see the “Cisco Storage Media Encryption Security Overview” section on page 1-14 and the “Master Key Security Modes” section on page 6-3.

---

**Table 4-1 Master Key Security Levels**

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>The master key is stored in a file and encrypted with a password. To retrieve the master key, you need access to the file and the password.</td>
</tr>
<tr>
<td>Standard</td>
<td>Standard security requires one smart card. When you create a cluster and the master key is generated, you are prompted to insert the smart card into the smart card reader. The master key is then written to the smart card. To retrieve the master key, you need the smart card and the smart card pin.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Advanced security requires 5 smart cards. When you create a cluster and select Advanced security mode, you designate the number of smart cards (2 or 3 of 5 smart cards or 2 of 3 smart cards) that are required to recover the master key when data needs to be retrieved. For example, if you specify 2 of 5 smart cards, then you will need 2 of the 5 smart cards to recover the master key. Each smart card is owned by a Cisco SME Recovery Officer. The greater the number of required smart cards to recover the master key, the greater the security. However, if smart cards are lost or if they are damaged, this reduces the number of available smart cards that could be used to recover the master key.</td>
</tr>
</tbody>
</table>

---

**Note**

For Basic and Standard security modes, one user should hold the Cisco SME Administrator and the Cisco SME Recovery Officer roles.

In the Master Key Security screen, select the cluster security type you wish to use. You can choose any of the following security levels:

- Selecting Basic Security, page 4-6
- Selecting Standard Security, page 4-6
- Selecting Advanced Security, page 4-7
Selecting Basic Security

In the Master Key Security screen, select Basic. Click Next.

For the Basic security level, after the cluster is created, the switch generates the master key file and you are prompted for a password to protect the file.

Selecting Standard Security

In the Master Key Security screen, select Standard and click Next. For Standard security, one Cisco SME Recovery Officer must be present to log in and enter the smart card PIN.
Selecting Advanced Security

When Advanced security is selected, you need to designate the number of cards that are required to recover the master key. This can be 2 or 3 of 5 smart cards or 2 of 3 smart cards. You will need to configure all 5 smart cards during the cluster creations process; however, you will only need the quorum number (that you designated in this step), to recover the master key.

In the Master Key Security screen, select Advanced. Enter the number of required smart cards for the quorum (2 of 3 or 2 of 5 or 3 of 5). Click Next.

- For Advanced security, 5 Cisco SME Recovery Officers must be present to login and enter the smart card PIN for each of the 5 smart cards.
- Be sure that the smart card reader is connected using the USB port (see “Installing Smart Card Drivers” section on page 2-17 in Chapter 2, “Getting Started”).
- When you insert a smart card into the reader, the card will be verified. You will be prompted to initialize the card if the card has not been previously initialized.

![Create Cluster: Master Key Security](image-url)
Selecting Media Key Settings

Caution
You cannot modify the media key settings after a cluster is created.

In the Media Key Settings screen, select the media key settings.

Table 4-2 lists the media key settings and definitions.
For additional information on media key settings, see “Key Management Settings” section on page 6-4.
Specifying the Key Management Center Server

In the Key Management Server screen, you can choose the primary and the secondary key management center servers from the drop-down menu. You can specify an IP address or a host name for the servers. Click Next.

The dual server settings will be available after you configure the high availability settings in the Key Manager Settings screen. For more information on the configuration, see the “Choosing High Availability Settings” section on page 6-5.
Selecting Transport Settings

In the Transport Settings screen, to enable Transport Settings, select On. If enabled, specify the Trust Point from the drop-down menu.

For more information about Trust Points, see the Cisco Fabric Manager IP Services Configuration Guide and the Cisco MDS 9000 Family NX-OS IP Services Configuration Guide.

To enable Transport settings, select On.

If On is selected in the Transport Setting, SSL is enabled on KMC with the following results:

- New clusters are created. If Off is selected, cluster creation fails.
- Previously created clusters are updated by enabling SSL with trustpoint on the switches. KMC server connection state remains as ‘none’ until the cluster is updated.

To disable Transport Settings, select Off.
Confirming the Cluster Creation

In the Confirmation screen, review the cluster configuration information. Click Back to change any settings. Click Confirm to create the cluster.

You will see an indication that the operation is in progress until the entire configuration is applied.
Downloading Key File and Storing Keyshares

This section describes how to download the key file for basic security level and store keyshares for the standard and advanced security level.

- Basic Security Download Key File, page 4-12
- Standard Security Confirmation and Stored Keyshares, page 4-13
- Advanced Security Confirmation and Stored Keyshares, page 4-15

Basic Security Download Key File

For the basic security level, follow these steps:

**Step 1**
Enter the password to encrypt the master key file. Retype the password to confirm it. Click Download.

**Step 2**
A File Download screen prompts you to open or save the encrypted file.
**Standard Security Confirmation and Stored Keyshares**

For the standard security level, follow these steps:

**Step 1**
In the Confirmation screen, click **Confirm** to create the cluster.

**Step 2**
A Store Keyshares screen opens. After the smart card applet finishes loading, click **Next**.

When entering smart card information, note the following:

- Be sure that the smart card reader is connected using the USB port (see the “Installing Smart Card Drivers” section on page 2-17 in Chapter 2, “Getting Started”).
- When you insert a smart card into the reader, the card will be verified. You will be prompted to initialize the card if the card has not been previously initialized.
- Make sure that you have the appropriate smart card drivers installed before proceeding.

**Step 3**
Enter the switch login information (username and password used to log in to Fabric Manager), the PIN number for the smart card, and a label that will identify the smart card. The PIN number and label were defined during the smart card initialization. Click **Next**.
Step 4  Click Finish to create a cluster.

Step 5  After the cluster creation is completed, click Close to return to the Fabric Manager Web Client and to view the smart card information.
Step 6  View the smart card information.

Advanced Security Confirmation and Stored Keyshares

To configure the advanced security level, follow these steps:

Step 1  In the Confirmation screen, click Confirm to create the cluster.
**Step 2**  A Store Keyshares screen opens. After the smart card applet finishes loading, click **Next**.

When entering smart card information, note the following:

- Be sure that the smart card reader is connected using the USB port (see the “Installing Smart Card Drivers” section on page 2-17 in Chapter 2, “Getting Started”).
- When you insert a smart card into the reader, the card will be verified. You will be prompted to initialize the card if the card has not been previously initialized.
- For each smart card, each Cisco SME Recovery Officer must login and enter the smart card pin.
- Make sure that you have the correct smart card drivers installed before proceeding.

**Step 3**  Enter the switch login information (username and password used to log in to Fabric Manager), the PIN number for the smart card, and a label that will identify the smart card. The PIN number and label were defined during the smart card initialization. Click **Next**.
You will see a notification that the keyshare is being stored. This notification will be shown after each keyshare is stored.

**Step 4** Click Next.

**Step 5** Enter the switch credentials and PIN information for the second recovery officer. Click Next.
Step 6  Enter the switch credentials and PIN information for the third recovery officer. Click Next.

Step 7  Enter the switch credentials and PIN information for the fourth recovery officer. Click Next.
Step 8 Enter the switch credentials and PIN information for the fifth recovery officer. Click Next.

Step 9 Click Finish to return to the Fabric Manager Web Client to view the smart card information.
Deactivating and Purging a Cisco SME Cluster

You can archive clusters that are Online, Pending, or Deprecated. For information on cluster states, see the “Viewing Cluster States” section on page 4-23.

Archiving and then purging a Cisco SME cluster involves the following steps:

- Delete all tape groups, tape devices, and tape volume groups (see Chapter 5, “Cisco SME Tape Configuration”)
- Delete all switches and Cisco SME interfaces from the cluster (see Chapter 3, “Cisco SME Interface Configuration”)
- Change the cluster state to deactivated (see Deactivating a Cisco SME Cluster, page 4-21)
- Purge (permanently delete) a Cisco SME cluster (see Purging a Cisco SME Cluster, page 4-22)

Note

You can only purge a cluster that is in the deactivated state.

This section covers the following topics:

Step 10

View the smart card information by selecting Smartcards.

Deactivating and Purging a Cisco SME Cluster

You can archive clusters that are Online, Pending, or Deprecated. For information on cluster states, see the “Viewing Cluster States” section on page 4-23.

Archiving and then purging a Cisco SME cluster involves the following steps:

- Delete all tape groups, tape devices, and tape volume groups (see Chapter 5, “Cisco SME Tape Configuration”)
- Delete all switches and Cisco SME interfaces from the cluster (see Chapter 3, “Cisco SME Interface Configuration”)
- Change the cluster state to deactivated (see Deactivating a Cisco SME Cluster, page 4-21)
- Purge (permanently delete) a Cisco SME cluster (see Purging a Cisco SME Cluster, page 4-22)

Note

You can only purge a cluster that is in the deactivated state.

This section covers the following topics:

Deactivating and Purging a Cisco SME Cluster

You can archive clusters that are Online, Pending, or Deprecated. For information on cluster states, see the “Viewing Cluster States” section on page 4-23.

Archiving and then purging a Cisco SME cluster involves the following steps:

- Delete all tape groups, tape devices, and tape volume groups (see Chapter 5, “Cisco SME Tape Configuration”)
- Delete all switches and Cisco SME interfaces from the cluster (see Chapter 3, “Cisco SME Interface Configuration”)
- Change the cluster state to deactivated (see Deactivating a Cisco SME Cluster, page 4-21)
- Purge (permanently delete) a Cisco SME cluster (see Purging a Cisco SME Cluster, page 4-22)

Note

You can only purge a cluster that is in the deactivated state.

This section covers the following topics:
Deactivating and Purging a Cisco SME Cluster

Deactivating a Cisco SME Cluster

Deactivating a Cisco SME Cluster deletes the cluster from the switch and retains the keys in the Cisco KMC.

To change the cluster state to Deactivated, follow these steps:

Step 1 Click Clusters in the navigation pane to display the clusters.

Step 2 Select a cluster in the information pane and click Remove.

Note Changes the cluster state to deactivated and retains the keys in the Cisco KMC.

Step 3 Click OK.

Step 4 Refresh Fabric Manager Web Client to view the notification that the cluster has been deactivated.

Caution Do not click Remove again unless you want to permanently delete the cluster configuration information and the master key from the Cisco KMC.
Deactivating and Purging a Cisco SME Cluster

Purging a Cisco SME Cluster

Purging a Cisco SME cluster includes the following steps:

- Delete all cluster elements (tape paths, tape devices, volume groups, tape groups, and switches)
- Delete (unbind) any Cisco SME interfaces that are configured in the cluster
- Change the cluster state to deactivated
- Purge the cluster to remove the cluster and the master keys from the Cisco KMC

**Note**

Only clusters with a status of deactivated can be purged.

To purge a Cisco SME cluster, follow these steps:

**Step 1**
Click **Clusters** in the navigation pane to display the Cisco SME clusters.

**Step 2**
Select an deactivated cluster in the information pane and click **Remove**.

**Step 3**
Click **OK** to delete the cluster.

**Caution**

Do not click **OK** unless you want to permanently delete the cluster configuration information and the master key from the Cisco KMC.

**Step 4**
Refresh the Fabric Manager Web Client to view the notification that the cluster has been purged.
Viewing Cisco SME Cluster Details

To view cluster details, click the cluster name and the cluster detail page displays.

You can use the links across the top of the information pane to navigate within the cluster.

This section covers the following topics:

- Viewing Cluster States, page 4-23
- Viewing Members in a Cluster, page 4-24
- Viewing and Modifying Transport Settings in Cluster Detail Page, page 4-24
- Viewing and Modifying Key Management Servers Settings, page 4-27

Viewing Cluster States

Cisco SME clusters can be in one of the following cluster states:

- Online—The Cisco SME cluster is available on the switches and is reachable from the Fabric Manager Server.
Viewing Cisco SME Cluster Details

To view the cluster status, follow these steps:

Step 1  Click Clusters in the navigation pane to view a list of all Cisco SME clusters and their status.

Step 2  Alternately, click Clusters in the navigation pane, and then click a cluster name to view the status of a specific cluster.

Viewing Members in a Cluster

When you view members of a cluster, you see the switches and the interfaces that have been added to a cluster.

To view the Cisco SME interfaces and switches in a cluster, click Members in the navigation pane.

Viewing and Modifying Transport Settings in Cluster Detail Page

To view and modify the transport settings, follow these steps:

Step 1  Select the newly created cluster in the navigation pane to display the cluster detail page.

The transport settings details are displayed when SSL is selected.
The transport settings details are displayed when SSL is Off.

You can also modify the transport settings in the cluster detail page by clicking Modify.
Step 2  Select SSL and choose a Trust Point from the drop-down menu. Click **Apply** to save the settings.
Viewing and Modifying Key Management Servers Settings

To view and modify the primary and secondary key management servers settings, follow these steps:

**Step 1**
Select the cluster in the navigation pane to display the cluster detail page. Click **Modify** to edit the server settings.

**Step 2**
Enter the IP addresses for the primary and/or the secondary servers. Click **Apply** to save the changes. Click **Cancel** to revert back to previous settings.

**Step 3**
Refresh the Fabric Manager Web Client to view the notification that the cluster has been modified.
Viewing Cluster Information Using Fabric Manager Client

To view Cisco SME cluster information using Fabric Manager Client, follow these steps:

**Step 1**
In the Physical Attributes pane, select **End Devices > SME Clusters**.

**Step 2**
Click the **Members** tab to view members in a cluster.
Step 3 Click the **Interfaces** tab to view information about SME interfaces.

---

**Viewing Cluster Information Using Device Manager**

To view Cisco SME cluster information using Device Manager, follow these steps:

---

**Step 1** In the Interface menu, select **SME Clusters**.

**Step 2** Select the **Clusters** tab to view the cluster name, state, and Master IP address.

**Step 3** Select the **Members** tab to view the cluster name, switch, fabric name, and whether or not the cluster/fabric is local.
Cluster Quorum and Master Switch Election Overview

This section describes the Cisco SME cluster quorum and the process for electing the master switch in a cluster. The section includes the following topics:

- Cluster Quorum, page 4-31
- Master Switch Election, page 4-31

In this section, the term switch is used to describe a Cisco MDS 9000 Family switch that is part of a Cisco SME cluster. In addition, the following terms are used in this section.

Node ID
Every switch in a cluster has a node ID. Cisco SME assigns a node ID to every new switch as it is added to the cluster. The switch where the cluster is created is assigned the node ID of 1. This is the master switch. When a new switch is added to the cluster, it is assigned the next available higher node ID. For example, when a second switch is added to the cluster it gets the node ID of 2 and the third switch gets the node ID of 3, and so on.

Cluster View
The cluster view is the set of switches that are part of the operational cluster.
Cluster Quorum

For a cluster to be operational, it must include more than half the number of configured switches in the cluster view. In an N-node cluster, N/2 + 1 nodes form a cluster quorum.

If N is even, the cluster quorum requires N/2 nodes and also, the presence of the switch with the lowest node ID.

The quorum logic ensures that in the event of cluster partitions, at most one partition can be operational. All other switches are nonoperational. This guarantees the consistency of the cluster.

Master Switch Election

When a cluster is created, the switch on which the cluster is created becomes the cluster master switch. When the master switch fails or is rebooted, another switch takes over as the master switch. The master election logic uses the node ID and the latest cluster configuration to determine which switch in the cluster will become the master switch. The master election logic is describe as follows:

- If the master switch fails in an operational cluster, the switch with the next lowest node ID takes over as the master switch. Note that in an operational cluster, all the switches run the same cluster configuration.

- When the previous master switch comes back online and joins the cluster, it does not immediately become the master.

- When all the switches of a cluster are coming up, the switch that has the latest cluster configuration becomes the master switch. If there are multiple switches with the same configuration, the switch with the lowest node ID is chosen to be the master switch.

- Once a master switch is chosen and the cluster is operational (there is a quorum), even if a switch with a lower node ID joins the cluster at a later time, the master switch does not change.

For example, there are three switches S1, S2, and S3 with node IDs 1, 2, and 3, respectively. If switches S2 and S3 form a quorum then switch S2 becomes the master switch. Even if switch S1 with the node ID of 1 comes up and joins the cluster at a later time, switch S2 continues to be the master. However, if switch S2 goes down for any reason, switch S1 will become the master switch.

Two-Switch Cluster Scenarios

According to the cluster quorum logic (see the “Cluster Quorum” section on page 4-31), a cluster with two configured switches can be operational if both switches are operational or the switch with the lowest node ID is operational.

In the latter case, the switch with the lowest node ID is the master of the one-switch cluster. The other switch could have failed or simply lost connectivity to the operational switch. In either case, the switch with the higher node ID would become nonoperational. If the node with the lower node ID failed, the other switch cannot form an operational cluster.

The examples that follow describe these scenarios. The first three examples consider single switch failures.

1. Assume that in a two-switch cluster with switches S1 (node ID 1) and S2 (node ID 2), S1 is the master (the master has the lower node ID).
Cluster Quorum and Master Switch Election Overview

Send documentation comments to mdsfeedback-doc@cisco.com

When the switches lose connectivity between them, the master switch S1 continues to be operational since it has the lower node ID and can form an \((N/2)\) switch cluster. Switch S2 becomes non-operational.

2. Assume that in a two-switch cluster with switches S1 (node ID 1) and S2 (node ID 2), S2 is the master (note that the master has the higher node ID because it has the latest configuration when both the switches came online).

When the switches lose connectivity between them, switch S2 becomes non-operational and S1 takes over as the master to form a 1-switch cluster. This is consistent with the quorum logic in a two-switch cluster \((N/2\) with lowest node ID).

3. Assume that in a two-switch cluster with switches S1 (node ID 1) and S2 (node ID 2). If S1 fails (regardless of which switch was the master), S2 will also become non-operational as long as S1 is down.

When S1 comes up, S1 and S2 will form a two-switch cluster.

The next set of examples describe reboots of both switches (S1 with node ID 1 and S2 with node ID 2).

Caution

If you perform any configuration change on a cluster, you must save the running configuration to the startup configuration by entering the `copy running-config startup-config` CLI command on all switches before rebooting them. Otherwise, the cluster may not form correctly after the reboot (see example 6.).

4. After a reboot, if both switches S1 and S2 come up about the same time, a two-switch cluster will be formed.
   a. If the cluster configurations are the same, S1 (with the lower node ID) will become the master.
   b. If the cluster configurations are different, the switch with the latest cluster configuration will become the master.

5. After a reboot, if switch S2 comes up first, it will not be able to form a cluster until S1 also comes up. After that, the algorithm explained in the previous case will be used.

6. After a reboot, if switch S1 comes up first, it will form a one-switch cluster \((N/2\) with lowest node ID). When S2 comes up, it will join the cluster to form a two-switch cluster.

When S2 comes up and if it happens to have the latest cluster configuration in the startup configuration (this can happen if you did not save the running configuration to the startup configuration on S1 but did so on S2), it will not be able to join the cluster formed by S1. You may be required to follow the recovery procedures described in Chapter 9, “Cisco SME Troubleshooting” to bring S2 back into the cluster.

Caution

It is critical that you save the running configuration on all switches before a reboot.

Three-Switch Cluster Scenarios

In a three-switch cluster, the quorum requires two switches to be in the cluster view \((N/2 + 1)\). The examples below explain three scenarios in a three-switch cluster with switches S1 (node ID 1), S2 (node ID 2) and S3 (node ID 3). S1 is the master switch.

1. In a three-switch operational cluster, if switch S3 fails or loses connectivity with the other two switches, then S3 becomes nonoperational. Switches S1 and S2 will form an operational cluster. When S3 comes up again, it will rejoin the cluster.
2. In a three-switch operational cluster, if the master switch S1 fails or loses connectivity with the other two switches, then S1 becomes nonoperational. Switches S2 and S3 will form an operational cluster and S2 will be the master. When S1 comes up again, it will rejoin the cluster. Note that S2 will continue to be the master.

3. If two switches fail, the cluster will become nonoperational.

The examples below describe reboots on all switches in the cluster.

⚠️ Caution

If you perform any configuration change on a cluster, you must save the running configuration to the startup configuration by entering the `copy running-config startup-config` command on all switches before rebooting them. Otherwise, the cluster may not form correctly after the reboot.

4. After a reboot, if all switches come up at about the same time, first a 2-switch cluster will be formed and later the third switch will be added.
   a. If the cluster configurations are the same, S1 (with the lower node ID) will become the master switch and form the 2-switch cluster first; and then add the third switch.
   b. If the cluster configurations are different, the switch that is running the latest configuration will become the master switch and then form a 2-switch cluster; and then add the third switch.

5. After a reboot, if the switches come up one at a time, a 2-switch cluster will be formed after the first two switches are up. Later, when the third switch comes online, it will join the cluster.
   If the third switch happens to be running the latest cluster configuration in the startup configuration (this can happen if you save the running configuration only on this switch but not on the other two), the third switch will not be able to join the cluster. You may be required to follow the recovery procedures described in Chapter 9, “Cisco SME Troubleshooting” to bring this switch back into the cluster.

⚠️ Caution

It is critical that you save the running configuration on all switches before a reboot.

**Four-Switch Cluster Scenarios**

The four-switch cluster scenario is very similar to the examples above. The cluster will be operational if the cluster view has at least three switches (N/2 + 1), or if the cluster view has two switches including the switch with the lowest node ID (N/2 with lowest node ID).

**In-Service Software Upgrade (ISSU) in a Two-Node Cluster**

In-Service Software Upgrade (ISSU) is a comprehensive, transparent software upgrade application that allows you to deploy bug fixes and add new features and services without any disruption to the traffic.

In a cluster comprising of the MDS 9222i switches as nodes, if the nodes are not able to communicate, then the node having the lowest node identifier (node ID) remains in the cluster while the other node leaves the cluster. However, when an ISSU is performed on a node having the lowest node identifier, a complete loss of the cluster results because both the nodes leave the cluster.

This undesirable situation is addressed in a two-node cluster as follows:
The upgrading node sends a message to the other node of the intent to leave the cluster. The upgrading node can either be a master node or a slave node.

The remaining node remains in the cluster and performs the role of the master node if it was a slave node. This node continues to remain in the cluster with the quorum intact.

After the ISSU is completed and the switches boot up, the upgraded node rejoins the cluster as a slave node.

Note

This feature is tied to the internals of ISSU logic and no additional commands need to be executed.