Guidelines and Prerequisites

Guidelines, and Best Practices for Firmware Upgrades

Before you upgrade the firmware for any endpoint in a Cisco UCS domain, consider the following guidelines, best practices, and limitations:

Configuration Changes and Settings that Can Impact Upgrades

Depending on the configuration of your Cisco UCS domain, the upgrade process may require you to make additional changes.

Default Maintenance Policy Should be Configured for User Acknowledgment

The default maintenance policy is configured to immediately reboot the server when disruptive changes are made to the service profile, such as server firmware upgrades through a host maintenance policy. We recommend that you change the reboot policy setting in the default maintenance policy to **user acknowledgment** to avoid unexpected disruption of server traffic.

When you configure the reboot policy in the default maintenance policy to **user acknowledgment**, the list of disruptive changes are listed with the pending activities. You can then control when the servers are rebooted.

Overlapping FCoE VLAN IDs and Ethernet VLAN IDs Are No Longer Allowed with Cisco UCS Release 2.0 and Higher

Caution In Cisco UCS 1.4 and earlier releases, Ethernet VLANs and FCoE VLANs could have overlapping VLAN IDs. However, starting with Cisco UCS release 2.0, overlapping VLAN IDs are not allowed. If Cisco UCS Manager detects overlapping VLAN IDs during an upgrade, it raises a critical fault. If you do not reconfigure your VLAN IDs, Cisco UCS Manager raises a critical fault and drops Ethernet traffic from the overlapped VLANs. Therefore, we recommend that you ensure there are no overlapping Ethernet and FCoE VLAN IDs before you upgrade to Cisco UCS Release 3.1 and later releases.

Be aware that when an uplink trunk is configured with VLAN ID 1 defined and set as the native VLAN, changing the Ethernet VLAN 1 ID to another value can cause network disruption and flapping on the fabric interconnects, resulting in an HA event that introduces a large amount of traffic and makes services temporarily unavailable.

For a new installation of Cisco UCS Release 3.1 and later releases, the default VLAN IDs are as follows:

- The default Ethernet VLAN ID is 1.
- The default FCoE VLAN ID is 4048.

Note If a Cisco UCS domain uses one of the default VLAN IDs, which results in overlapping VLANs, you can change one or more of the default VLAN IDs to any VLAN ID that is not used or reserved. From release 2.0 and higher, VLANs with IDs from 4030 to 4047 are reserved.

VSANs with IDs in the Reserved Range are not Operational

A VSAN with an ID in the reserved range is not operational after an upgrade. Make sure that none of the VSANs configured in Cisco UCS Manager are in these reserved ranges:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.
- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

If a VSAN has an ID in the reserved range, change that VSAN ID to any VSAN ID that is not used or reserved.

Hardware-Related Guidelines for Firmware Upgrades

The hardware in a Cisco UCS domain can impact how you upgrade. Before you upgrade any endpoint, consider the following guidelines and limitations:

No Server or Chassis Maintenance

Caution Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process completes. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure might corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Avoid Replacing RAID-Configured Hard Disks During or Prior to Upgrade

During or prior to Cisco UCS infrastructure and server firmware upgrades:

- Do not remove, insert or replace any local storage hard disks or SSDs in the servers.
- Ensure that no storage operations are running, including Rebuild, Association, Copyback, BGI, and so on.

Always Upgrade Third-Party Adapters through a Host Firmware Package

You cannot upgrade third-party adapters directly at the endpoints. You must upgrade the firmware on those adapters through a host firmware package.

Configure the Fabric Interconnects

The clustered fabric interconnects provide data path redundancy by design. However, to ensure that data traffic is not disrupted, you must configure redundant Ethernet and storage (FC/FCoE) interfaces within the service profile. You must also ensure that the corresponding Operating System is configured correctly to handle one fabric path outage.

For a standalone configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Firmware- and Software-Related Guidelines for Upgrades

Before you upgrade any endpoint, consider the following guidelines and limitations:

Determine the Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as Cisco adapters and the server CIMC, can be upgraded through either a direct firmware upgrade or a firmware package included in a service profile. The configuration of a Cisco UCS domain determines how you upgrade these endpoints. If the service profiles associated with the servers include a host firmware package, upgrade the adapters for those servers through the firmware package.

Upgrades of an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

If you use Cisco UCS Manager GUI to update the firmware, do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order, and can disrupt communications between the endpoints and the fabric interconnects and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

Determine Available Bootflash and Workspace Partition

The bootflash partition is dedicated solely to firmware images managed by Cisco UCS Manager. To initiate upgrade or downgrade, at least 20 percent of the bootflash partition must be available. When the bootflash partition exceeds 70 percent, faults are raised, but Auto Install proceeds. When the bootflash partition exceeds 80 percent, faults are raised and Auto Install does not proceed.

The workspace partition on the fabric interconnect stores tech support files, core files, and the debug plugin. To initiate upgrade or downgrade, at least 20 percent of the workspace partition must be available.

Checking the Available Space on a Fabric Interconnect provides detailed information about monitoring the available storage on these partitions.

Determine the Impact of Activation for Adapters and I/O Modules

During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

If a server is not associated with a service profile, the activated firmware remains in the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot or reset an unassociated server to activate the firmware.

When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data patch is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between the fabric interconnect and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches the firmware in the fabric interconnect and then activates the firmware and reboots the I/O module again.

Disable Call Home before Upgrading to Avoid Unnecessary Alerts (Optional)

When you upgrade a Cisco UCS domain, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to the service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, alerts will be generated by the upgrade-related component, restarts and notifications will be sent out based on your Call Home configuration.

Fabric Interconnect Traffic Evacuation

Fabric interconnect traffic evacuation, introduced in Release 2.2(4), is the ability to evacuate all traffic that flows through a fabric interconnect from all servers attached to it through an IOM or FEX, while upgrading a system.

Upgrading the subordinate fabric interconnect in a system disrupts the traffic that is active on the fabric interconnect. This traffic fails over to the primary fabric interconnect. You can use fabric evacuation as follows during the manual upgrade process:

1. Stop all the traffic that is active through a fabric interconnect by configuring **Admin Evac Mode** as **On**.
2. For vNICs configured with failover, verify that the traffic has failed over by using Cisco UCS Manager or tools such as vCenter.
3. Upgrade the subordinate fabric interconnect.
4. Restart all the stopped traffic flows by configuring **Admin Evac Mode** as **Off**.
5. Change the cluster lead to the subordinate fabric interconnect.
6. Repeat steps 1 to 4 and upgrade the other fabric interconnect.

Note

- Fabric interconnect traffic evacuation is supported only in a cluster configuration.
- You can evacuate traffic only from the subordinate fabric interconnect.
- The IOM or FEX backplane ports of the fabric interconnect on which evacuation is configured will go down, and their state will appear as **Admin down**. During the manual upgrade process, to move these backplane ports back to the **Up** state and resume traffic flow, you must explicitly configure **Admin Evac Mode** as **Off**.

Fabric Evacuation with Auto Install

Starting with Cisco UCS Manager Release 3.1(3), you can use fabric evacuation during Auto Install. While initiating Auto Install, when you enable fabric evacuation and then begin Auto Install, the following sequence of events occur:

1. The subordinate fabric interconnect (FI-B) is evacuated and activated.
2. Failover occurs and the primary fabric interconnect (FI-A) becomes the subordinate fabric interconnect. FI-B now becomes the cluster lead.
3. FI-A is now evacuated and activated.

If you use fabric evacuation with Auto Install, and fabric evacuation was enabled on the fabric interconnect before Auto Install, fabric evacuation is disabled after Auto Install is complete.

Ensure that you do not initiate Auto Install with fabric evacuation enabled on the primary fabric interconnect. If fabric evacuation was manually enabled on the primary fabric interconnect before Auto Install, it must be manually disabled before initiating Auto Install.

Note

- Fabric interconnect traffic evacuation is supported only in a cluster configuration.
- You can evacuate traffic only from the subordinate fabric interconnect.
- The IOM or FEX backplane ports of the fabric interconnect on which evacuation is configured will go down, and their state will appear as **Admin down**. These backplane ports will move back to **Up** state after Auto Install is complete.

Stopping Traffic on a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified Fabric Interconnect.
Step 2	UCS-A /fabric-interconnect # **stop server traffic** [**force**]	Stops all the traffic that is active through the specified Fabric Interconnect. Use the **force** option to evacuate a Fabric Interconnect irrespective of its current evacuation state.
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to stop all traffic that is active through Fabric Interconnect B:

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # stop server traffic
Warning: Enabling fabric evacuation will stop all traffic through this Fabric Interconnect
 from servers attached through IOM/FEX. The traffic will fail over to the Primary Fabric
Interconnect for fail over vnics.
UCS-A /fabric-interconnect # commit-buffer
```

Restarting Traffic on a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified Fabric Interconnect.
Step 2	UCS-A /fabric-interconnect # **start server traffic**	Restarts traffic through the specified Fabric Interconnect.

	Command or Action	Purpose
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to restart traffic through Fabric Interconnect B:

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # start server traffic
Warning: Resetting fabric evacuation will cause server traffic that failed over to the
Primary Fabric Interconnect to fail back to this Fabric Interconnect.
UCS-A /fabric-interconnect # commit-buffer
```

Verifying Fabric Evacuation

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show service-profile circuit server** *server-id*	Shows the network circuit information for the service profile associated with the specified server.

Example

This example shows the VIF paths before fabric evacuation.

Note

- VIF at Fabric Interconnect A shows that traffic is initially active through the Fabric interconnect.
- VIF at Fabric Interconnect B is passive before evacuation.

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------ ----------- ----------
 ---------- ---------
               692 eth0            Up          Active     Active        Primary     0/0
     1/15       Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------ ----------- ----------
```

```
 ---------- ---------
              693 eth0            Up          Active     Passive       Backup      0/0
     1/15       Ether
UCS-A#
```

This example shows the VIF paths after Fabric Interconnect A is evacuated.

Note

- After fail over, the VIF state at Fabric Interconnect A goes into error.
- VIF at Fabric Interconnect B takes over as active.

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------- ----------- ----------
 ---------- ---------
              692 eth0            Error       Error      Active        Primary     0/0
     0/0        Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------- ----------- ----------
 ---------- ---------
              693 eth0            Up          Active     Passive       Backup      0/0
     1/15       Ether
UCS-A#
```

Displaying the Status of Evacuation at a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified Fabric Interconnect.
Step 2	UCS-A /fabric-interconnect # **show detail**	Displays details about the specified Fabric Interconnect.

Example

This example shows how to display the detailed status of a Fabric Interconnect.

Note Admin Evacuation and Oper Evacuation show the status of evacuation at the Fabric Interconnect.

```
 UCS-A /fabric-interconnect # show detail

Fabric Interconnect:
    ID: B
    Product Name: Cisco UCS 6248UP
    PID: UCS-FI-6248UP
    VID: V01
    Vendor: Cisco Systems, Inc.
    Serial (SN): SSI171400HG
    HW Revision: 0
    Total Memory (MB): 16165
    OOB IP Addr: 10.193.32.172
    OOB Gateway: 10.193.32.1
    OOB Netmask: 255.255.255.0
    OOB IPv6 Address: ::
    OOB IPv6 Gateway: ::
    Prefix: 64
    Operability: Operable
    Thermal Status: Ok
    Admin Evacuation: On
    Oper Evacuation: On
    Current Task 1:
    Current Task 2:
    Current Task 3:
```

Secure Firmware Update

Cisco UCS Manager, Release 3.1(2) introduces secure firmware update, which enables you to update the adapter firmware securely for third-party Intel network and storage adapters. Only server administrators can upgrade or downgrade firmware for the adapters. OS administrators with root privileges are not allowed to downgrade the adapter firmware.

The following Cisco UCS servers support secure firmware update:

Secure Firmware Update Supported Network Adapters and Storage Disks

Supported Storage Disks on Cisco Blade Servers

The following Intel NVMe storage disks support secure firmware update on a Cisco UCS B200 M4 server that has the UCSB-LSTOR-PT storage controller.

Storage Disks
UCS-PCI25-8003
UCS-PCI25-16003
UCS-PCI25-40010
UCS-PCI25-80010

Note Secure firmware update is not supported on a Cisco UCS B200 M4 server for the following:

- NVMe disks with SAS storage controllers.
- A combination of NVMe disks and HDDs present on a Cisco UCS B200 M4 server.
- Network adapters.

Supported Network Adapters and Storage Disks on Cisco Rack Servers

The following Intel network adapters support secure firmware update on Cisco UCS C460, C240, and C220 M4 servers:

Table 1: Supported Network Adapters

Network Adapters
UCSC-PCIE-IQ10GF
UCSC-PCIE-ID10GF
UCSC-PCIE-ID40GF

The following Intel NVMe storage disks support secure firmware update on the Cisco UCS C460 M4 server, Cisco UCS C240 M4 Server, and Cisco UCS C220 M4 Server:

Table 2: Supported NVMe Storage Disks

NVMe Storage Disks	Description
UCS-PCI25-8003	P3600 2.5"
UCS-PCI25-16003	P3600 2.5"
UCS-PCI25-40010	P3700 2.5"
UCS-PCI25-80010	P3700 2.5"
UCSC-F-I80010	P3700 HHHL
UCSC-F-I160010	P3700 HHHL
UCSC-F-I20003	P3600 HHHL

Guidelines for Secure Firmware Support on Cisco UCS Servers

Cisco UCS Manager Release 3.1(2) introduces support for secure firmware update.

Important Ensure that CIMC is running Version 2.0(13) or later and Cisco UCS Manager is running Release 3.1(2) or later releases. Secure firmware update cannot be done when the CIMC is running a version earlier than 2.0(13) and Cisco UCS Manager is running a release earlier than Release 3.1(2).

Guidelines for Blade Servers

For secure firmware update on Cisco UCS B200 M4 servers, do the following:

- For Cisco UCS B200 M4 servers, upgrade the Cisco UCS Manager infrastructure software bundle and B-Series server software bundle to Cisco UCS Manager Release 3.1(2) or a later release.
- Install the UCSB-LSTOR-PT storage controller and insert the NVMe disks on a Cisco UCS B200 M4 server.
- Reacknowledge the server. Refer to the *Reacknowledging a Blade Server* section in the *Cisco UCS Manager Infrastructure Management Guide, Release* .

Guidelines for Rack Servers

For secure firmware update on Cisco UCS C460, C240, C220 M4 servers, do the following:

- For the supported Cisco UCS M4 servers, upgrade the Cisco UCS Manager infrastructure software bundle and C-Series server software bundle to Cisco UCS Manager Release 3.1(2) or a later release.
- Reacknowledge the Cisco UCS servers. Refer to the *Reacknowledging a Rack Server* section in the *Cisco UCS Manager Infrastructure Management Guide, Release* .

Cautions, and Guidelines for Upgrading with Auto Install

Before you use Auto Install to upgrade the firmware for any endpoint in a Cisco UCS domain, consider the following cautions, guidelines, and limitations:

Note These guidelines are specific to Auto Install and are in addition to those listed in Guidelines, and Best Practices for Firmware Upgrades, on page 1.

State of the Endpoints

Before you begin an upgrade, all affected endpoints must be as follows:

- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- For all endpoints to be upgraded, verify that they are in an Operable state.
- For all servers to be upgraded, verify that all the servers have been discovered and that discovery did not fail. Install Server Firmware will fail if any server endpoints cannot be upgraded.

- For each server to be upgraded, check the running firmware version on the storage controller and local disks, and verify that they are in the **Ready** state.

Recommendations for the Default Host Firmware Policy

After you upgrade Cisco UCS Manager, a new host firmware policy named "default" is created, and is assigned to all service profiles that did not already include a host firmware policy. The default host firmware policy is blank. It does not contain any firmware entries for any components. This default policy is also configured for an immediate reboot rather than waiting for user acknowledgment before rebooting the servers.

During the upgrade of server firmware, you can modify the default host firmware policy to add firmware for the blade and rack-mount servers in the Cisco UCS domain. To complete the upgrade, all servers must be rebooted.

Every service profile that is assigned to the default host firmware policy reboots the associated server according to the maintenance policy included in the service profile. If the maintenance policy is set to immediate reboot, you cannot cancel the upgrade or prevent the servers from rebooting after you complete the configuration in the **Install Server Firmware** wizard. We recommend that you verify the maintenance policy associated with these service profiles to ensure that they are set for a timed reboot or for user acknowledgment.

Note If you are upgrading from a release prior to 2.1(2a), you may be impacted by CSCup57496. After manually upgrading the CIMC and associating a service profile, remove the Management Firmware pack to activate the firmware of CIMC. For more information, please refer to https://tools.cisco.com/bugsearch/bug/CSCup57496. This is not applicable to Cisco UCS Mini.

Time, Date, and Time Zone on Fabric Interconnects Must Be Identical

To ensure that the fabric interconnects in a cluster configuration are in sync, you must ensure that they are configured for the same date, time, and time zone. We recommend that you configure an NTP server and the correct time zone in both fabric interconnects. If the date, time or time zone in the fabric interconnects are out of sync, the Auto Install might fail.

Cannot Upgrade Infrastructure and Server Firmware Simultaneously

You cannot upgrade the infrastructure firmware at the same time as you upgrade server firmware. We recommend that you upgrade the infrastructure firmware first and then upgrade the server firmware. Do not begin the server firmware upgrade until the infrastructure firmware upgrade is completed.

Required Privileges

Users must have the following privileges to upgrade endpoints with Auto Install:

Privileges	Upgrade Tasks User Can Perform
admin	• Run Install Infrastructure Firmware • Run Install Server Firmware • Add, delete, and modify host firmware packages
Service profile compute (ls-compute)	Run Install Server Firmware

Privileges	Upgrade Tasks User Can Perform
Service profile server policy (ls-server-policy)	Add, delete, and modify host firmware packages
Service profile config policy (ls-config-policy)	Add, delete, and modify host firmware packages

Impact of Host Firmware Packages on Install Server Firmware

Because Install Server Firmware uses host firmware packages to upgrade the servers, you do not have to upgrade all servers in a Cisco UCS domain to the same firmware versions. However, all servers which have associated service profiles that include the host firmware packages you selected when you configured Install Server Firmware are upgraded to the firmware versions in the specified software bundles.

Effect of Using Install Server Firmware on Servers Whose Service Profiles Do Not Include a Host Firmware Package

If you use Install Server Firmware to upgrade server endpoints on servers that have associated service profiles without host firmware packages, Install Server Firmware uses the default host firmware package to upgrade the servers. You can only update the default host firmware package through Install Server Firmware.

If you want to upgrade the CIMC or adapters in a server with an associated service profile that has previously been updated through the default host firmware package in Install Server Firmware, you must use one of the following methods:

- Use Install Server Firmware to modify the default host firmware package and then upgrade the server through Install Server Firmware.
- Create a new host firmware package policy, assign it to the service profile associated with the server, and then upgrade the server through that host firmware package policy.
- Disassociate the service profile from the server and then directly upgrade the server endpoints.

Upgrading Server Firmware on Newly Added Servers

If you add a server to a Cisco UCS domain after you run Install Server Firmware, the firmware on the new server is not automatically upgraded by Install Server Firmware. If you want to upgrade the firmware on a newly added server to the firmware version used when you last ran Install Server Firmware, you must manually upgrade the endpoints to upgrade the firmware on that server. Install Server Firmware requires a change in firmware version each time. You cannot rerun Install Server Firmware to upgrade servers to the same firmware version.

Note After you finish the upgrade, you can use the **Firmware Auto Sync Server** policy in Cisco UCS Manager to automatically update newly discovered servers.

Cautions, and Guidelines Limitations for Managing Firmware in Cisco UCS Central

Before you start managing Cisco UCS Manager firmware from Cisco UCS Central, consider the following cautions, guidelines and limitations:

- The firmware policies you define for a domain group will be applied to any new Cisco UCS Domain added to this domain group. If a firmware policy is not defined in the domain group, Cisco UCS Domain will inherit the policy from the parent domain group.
- The global policies will remain global in Cisco UCS Manager even when Cisco UCS Manager loses connection with Cisco UCS Central. If you want to apply any changes to any of the policies that are global in Cisco UCS Manager, you must change the ownership to local from global.
- When you create a host firmware package from Cisco UCS Central, it must be associated to a service profile to deploy updates in Cisco UCS domains.
- When you modify a host firmware package in Cisco UCS Central, the changes are applied to Cisco UCS domains during the next maintenance schedule associated with the host firmware update.
- The host firmware maintenance policies you define in Cisco UCS Central apply to the org-root in Cisco UCS domains. You cannot define separate host maintenance policies for sub organizations in a Cisco UCS Domain from Cisco UCS Central.
- Any server with no service profile association will get upgraded to the default version of the host firmware pack. Since these servers do not have a maintenance policy, they will reboot immediately.
- If you specify a maintenance policy in Cisco UCS Central and enable user acknowledgment and do not specify a schedule, you can acknowledge the pending task only from Cisco UCS Manager. To acknowledge pending activities from Cisco UCS Central, you must schedule maintenance using global schedulers and enable user acknowledgment.
- When you schedule a maintenance policy in Cisco UCS Central and enable user acknowledgment, that task will be displayed on the pending activities tab at the time specified in the schedule.
- You can view the pending activity for a maintenance policy only from the domain group section.
- Make sure to enable user acknowledgment for any firmware schedule to avoid any unexpected reboot in the Cisco UCS domains.

Note For more information on managing firmware in Cisco UCS Central, see the Firmware Management chapters in the *Cisco UCS Central Administration Guide* and *Cisco UCS Central CLI Reference Manual*.

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS domain must be fully functional and all processes must be complete before you begin a firmware upgrade or downgrade on those endpoints. You cannot upgrade or downgrade an endpoint that is not in a functional state.

For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. An incomplete process, such as an FSM that has failed after the maximum number of retries, can cause the upgrade or downgrade on an endpoint to fail. If an FSM is in progress, Cisco UCS Manager queues up the update and activation and runs them when the FSM has completed successfully.

Before you upgrade or downgrade firmware in a Cisco UCS domain, complete the following tasks:

- Review the Release Notes.
- Review the relevant Hardware and Software Interoperability Matrix to ensure that the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade.
- Back up the configuration into an All Configuration backup file.
- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that the data path is up and running. For more information, see the Verification that the Data Path is Ready, on page 29 section.
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that the Cisco UCS domain does not include any critical or major faults. If such faults exist, you must resolve them before you upgrade the system. A critical or major fault may cause the upgrade to fail.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.
- If you want to integrate a rack-mount server into the Cisco UCS domain, follow the instructions in the appropriate C-Series Rack-Mount Server Integration Guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.
- For Cisco UCS domains that are configured for iSCSI boot, do the following before you upgrade to Cisco UCS, Release 3.1(1) or higher:
  - Ensure that all iSCSI vNICs used across multiple service profiles have unique initiator names.
  - If any iSCSI vNICs have the same initiator name within a service profile, Cisco UCS reconfigures the service profile to have a single unique initiator name.
  - Make the corresponding IQN initiator name changes on any network storage devices to ensure that the boot LUNs are visible to the new IQN.

Pre-Upgrade Validation Checks

Ensure that you complete the following pre-upgrade validation checks before installing firmware:

Create Backup Files

When you perform a backup through Cisco UCS Manager, you take a snapshot of all or part of the system configuration and export the file to a location on your network. You can perform a backup while the system is up and running. The backup operation only saves information from the management plane. It does not have any impact on the server on network traffic.

Cisco recommends that you create the following backup files before beginning a Cisco UCS firmware upgrade:

- **All Configuration** backup file—An XML backup of all the system and logical configuration
- **Full State** backup file—A binary snapshot of the entire system

Creating an All Configuration Backup File

This procedure assumes that you do not have an existing backup operation for an All Configuration backup file.

Before you begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **create backup** *URL* **all-configuration enabled**	Creates an enabled All Configuration backup operation that runs as soon as you enter the **commit-buffer** command. The **all-configuration** option backs up the server, fabric, and system related configuration. Specify the URL for the backup file using one of the following syntax: • **ftp:**// *username***@***hostname* / *path* • **scp:**// *username*@*hostname* / *path* • **sftp:**// *username*@*hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path*
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

Example

The following example uses SCP to create an All Configuration backup file on the host named host35 and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config.bak all-configuration
enabled
```

```
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

Configuring the Full State Backup Policy

Before you begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **scope backup-policy default**	Enters the all configuration export policy mode.
Step 3	UCS-A /org/backup-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	Specifies the hostname, IPv4 or IPv6 address of the location where the backup policy is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 4	UCS-A /org/backup-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 5	UCS-A /org/backup-policy # **set user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 6	UCS-A /org/backup-policy # **set password**	After you press **Enter**, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.

	Command or Action	Purpose
Step 7	UCS-A /org/backup-policy # **set remote-file** *filename*	Specifies the full path to the backup file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
Step 8	UCS-A /org/backup-policy # **set adminstate** {**disable** | **enable**}	Specifies the admin state for the policy. This can be one of the following: • **enable**—Cisco UCS Manager exports the backup file using the schedule specified in the **Schedule** field. • **disable**—Cisco UCS Manager does not export the file.
Step 9	UCS-A /org/backup-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Specifies the frequency with which Cisco UCS Manager exports the backup file.
Step 10	UCS-A /org/backup-policy # **set descr** *description*	Specifies a description for the backup policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Step 11	UCS-A /org/backup-policy # **commit-buffer**	Commits the transaction.

Example

The following example shows how to configure the full state backup policy for a weekly backup and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # scope backup-policy default
UCS-A /org/backup-policy # set hostname host35
UCS-A /org/backup-policy* # set protocol scp
UCS-A /org/backup-policy* # set user UserName32
UCS-A /org/backup-policy* # set password
Password:
UCS-A /org/backup-policy* # set remote-file /backups/full-state1.bak
UCS-A /org/backup-policy* # set adminstate enable
UCS-A /org/backup-policy* # set schedule weekly
UCS-A /org/backup-policy* # set descr "This is a full state weekly backup."
UCS-A /org/backup-policy* # commit-buffer
UCS-A /org/backup-policy #
```

Configure Cisco Smart Call Home for Firmware Upgrade

Cisco Smart Call Home is a web application that leverages the Call Home feature of Cisco UCS. Smart Call Home offers proactive diagnostics and real-time email alerts of critical system events, which results in higher network availability and increased operational efficiency. Smart Call Home is a secure connected service

offered by Cisco Unified Computing Support Service and Cisco Unified Computing Mission Critical Support Service for Cisco UCS. The *Cisco UCS Manager Administration Management Guide* provides detailed information about configuring Smart Call Home.

When you upgrade firmware, Cisco UCS Manager restarts the components to complete the upgrade process. This restart can trigger email alerts. Disabling Smart Call Home will avoid creating such alerts and automatic support cases with TAC during the firmware upgrade process.

Disabling Smart Call Home

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope callhome**	Enters monitoring call home mode.
Step 3	UCS-A /monitoring/callhome # **disable**	Enables Call Home.
Step 4	UCS-A /monitoring/callhome # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example disables Smart Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Fault Suppression During Firmware Upgrade

Fault suppression allows you to suppress SNMP trap and Call Home notifications during a planned maintenance time. You can create a fault suppression task to prevent notifications from being sent whenever a transient fault is raised or cleared.

Faults remain suppressed until the time duration has expired, or the fault suppression tasks have been manually stopped by the user. After the fault suppression has ended, Cisco UCS Manager will send notifications for any outstanding suppressed faults that have not been cleared.

Enabling fault suppression for any component during firmware upgrade suppresses the faults related to that component until the time duration has expired, or until the component comes back up after upgrade. For example, if fabric interconnect faults are configured to be suppressed during firmware upgrade, no faults triggered by the fabric interconnect going down during upgrade will be displayed.

Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect

It is essential to ensure that port configurations and services that go down when the fabric interconnect reboots are re-established after the fabric interconnect comes back up.

Starting with Cisco UCS Manager Release 3.1, Cisco UCS Manager displays any service that is not re-established after the last reboot of a fabric interconnect. Cisco UCS Manager creates a baseline of the outstanding faults before a fabric interconnect is to be rebooted. After the fabric interconnect reboots and comes up, you can view the new faults generated since the last baseline to identify the services that went down because of the fabric reboot.

When a specific interval of time has passed after Cisco UCS Manager created a baseline of the outstanding faults, baselining is cleared and all faults show up as new faults. This interval is called "baseline expiration interval". Modifying Baseline Expiration Interval for Faults, on page 20, provides detailed information about modifying a baseline expiration interval in Cisco UCS Manager.

Cisco recommends that you resolve service-impacting faults before you continue with the fabric interconnect reboot or evacuation.

Modifying Baseline Expiration Interval for Faults

You can modify a baseline expiration interval in Cisco UCS Manager.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope fault policy**	Enters monitoring fault policy mode.
Step 3	UCS-A /monitoring/fault-policy # **show**	Displays the details of the fault policy.
Step 4	UCS-A /monitoring/fault-policy # **set baseline-expiration-interval** {*days hours minutes seconds*}	Modifies the baseline expiration interval. The default baseline expiration interval is 24 hours. **Note** After the baseline-expiration-interval expires, all faults are shown as new faults.
Step 5	UCS-A /monitoring/fault-policy* # **commit**	Commits the transaction.
Step 6	UCS-A /monitoring/fault-policy # **show**	Displays the details of the fault policy.

Example

This example shows how to modify the baseline expiration interval for faults:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- ------------------------------- -----------------------
----------------------------------------
    Retain       00:00:20:00    00:01:00:00                     10
10:00:00:12
```

```
UCS-A /monitoring/fault-policy # set baseline-expiration-interval 0 2 24 0
UCS-A /monitoring/fault-policy* # commit
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- ------------------------------ -----------------------
-----------------------------------------
    Retain       10:00:00:00    01:01:01:01                    10
00:02:24:00
UCS-A /monitoring/fault-policy #
```

Viewing Faults Generated During the Upgrade of a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **show new-faults**	Shows the faults generated after baselining and because of the reboot of the fabric interconnect during upgrade.
Step 3	UCS-A /monitoring # **show baseline-faults**	Shows the faults baselined before the reboot of the fabric interconnect during upgrade.

Example

This example shows how to view faults generated at various stages of the upgrade process:

Faults before reboot of the primary fabric interconnect:

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

Faults after reboot of the primary fabric interconnect:

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
```

```
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server 1
/ 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state is
down
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

To view faults generated because of reboot of the primary fabric interconnect:

```
UCS-A /monitoring # show new-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server 1
/ 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state is
down
```

To view faults before reboot of the primary fabric interconnect:

```
UCS-A# show baseline-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

Verifying the Operability of a Fabric Interconnect

If your Cisco UCS domain is running in a high availability cluster configuration, you must verify the operability of both fabric interconnects.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect #**show**	Displays information about the fabric interconnect. Verify that the operability of the fabric interconnects is in the Operable state. If the operability is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

Example

The following example displays that the operability for both fabric interconnects is in the Operable state:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    A  192.168.100.10  192.168.100.20  255.255.255.0   Operable

UCS-A /fabric-interconnect # exit
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    B  192.168.100.11  192.168.100.20  255.255.255.0   Operable
```

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the operational state and leadership role for both fabric interconnects in a high availability cluster. Verify that both fabric interconnects (A and B) are in the Up state and HA is in the Ready state. If the fabric interconnects are not in the Up state

	Command or Action	Purpose
		or HA is not in the Ready state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*. Also note which fabric interconnect has the primary role and which has the subordinate role; you will need to know this information to upgrade the firmware on the fabric interconnects.

Example

The following example displays that both fabric interconnects are in the Up state, HA is in the Ready state, fabric interconnect A has the primary role, and fabric interconnect B has the subordinate role:

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

Configuring the Default Maintenance Policy

Some modifications to a service profile or to an updating service profile template can be disruptive and require a reboot of the server. A maintenance policy determines how Cisco UCS Manager reacts when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how Cisco UCS Manager deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with admin privileges
- Automatically at the time specified in a schedule
- When the server boots again

Before you begin

If you plan to configure this maintenance policy for deferred deployment, create a schedule.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCS-A /org # **scope maint-policy default**	Enters the maintenance policy mode for the default maintenance policy.
Step 3	UCS-A /org/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**}	When a service profile is associated with a server, the server needs to be rebooted to complete the association. Specifying the reboot-policy command determines when the reboot occurs for all service profiles that include this maintenance policy. Possible values include: • **immediate**--The server reboots as soon as the change is made to the service profile. • **timer-automatic** --You select the schedule that specifies when maintenance operations can be applied to the server using the **`set scheduler`** command. Cisco UCS reboots the server and completes the service profile changes at the scheduled time. • **user-ack** --The user must explicitly acknowledge the changes by using the **apply pending-changes** command before changes are applied. Cisco recommends that you set the reboot policy of the default maintenance policy to **user-ack**.
Step 4	(Optional) UCS-A /org/maint-policy # **set scheduler** *scheduler-name*	If the reboot-policy property is set to timer-automatic, you must select the schedule that specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.
Step 5	UCS-A /org/maint-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example modifies the reboot policy of the default maintenance policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope maint-policy default
UCS-A /org/maint-policy* # set reboot-policy user-ack
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

Disabling the Management Interface

Before firmware upgrade, you could shut down the management interface of the secondary fabric interconnect. This ensures that any active KVM connections between any server and the management interface will reset. The GUI flow fails over to the primary fabric interconnect and reduces the time that you are disconnected from the GUI.

If Cisco UCS Manager detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault. By default, the management interfaces monitoring policy is enabled. The *Cisco UCS Manager System Monitoring Guide* provides more details about the Management Interfaces Monitoring Policy.

Procedure

Step 1 Enter monitoring mode.

UCS-A# **scope monitoring**

Step 2 Enable or disable the management interfaces monitoring policy.

UCS-A /monitoring # **set mgmt-if-mon-policy admin-state** {**enabled** | **disabled**}

Step 3 UCS-A /monitoring # **commit-buffer**

Commits the transaction to the system configuration.

Step 4 Open a Telnet session to the upstream switch connected to the fabric interconnect.

Step 5 Verify the configuration of the interface to which the fabric interconnect management port is connected, and disable it using the shut command on the switch.

Any KVM session that is open through this interface terminates.

Step 6 Reconnect KVM sessions to ensure that these sessions are not impacted by upgrade of the secondary fabric interconnect.

Example

The following example disables the monitoring interface management policy and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # set mgmt-if-mon-policy admin-state enabled
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Verifying the Status of an I/O Module

If your Cisco UCS is running in a high availability cluster configuration, you must verify the status for both I/O modules in all chassis.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope iom** *iom-id*	Enters chassis I/O module mode for the selected I/O module.
Step 3	UCS-A # **show**	Shows the status of the specified I/O module on the specified chassis. Verify that the overall status of the I/O module is in the Operable state. If the overall status is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*.

Example

The following example displays that the overall status for both I/O modules on chassis 1 is in the Operable state:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             1 Left  A         Operable

UCS-A /chassis/iom # exit
UCS-A /chassis # scope iom 2
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             2 Right B         Operable
```

Verifying the Status of a Server

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / server-id*	Enters chassis server mode for the specified server in the specified chassis.
Step 2	UCS-A /chassis/server # **show status detail**	Shows the status detail of the server. Verify that the overall status of the server is Ok, Unavailable, or any value that does not indicate a failure. If the overall status is in a state that indicates a failure, such as Discovery Failed, the endpoints on that server cannot be upgraded.

Example

The following example displays that the overall status for server 7 on chassis 1 is in the Ok state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show status detail
Server 1/7:
    Slot Status: Equipped
    Conn Path: A,B
    Conn Status: A,B
    Managing Instance: B
    Availability: Unavailable
    Admin State: In Service
    Overall Status: Ok
    Oper Qualifier: N/A
    Discovery: Complete
    Current Task:
```

Verifying the Status of Adapters on Servers in a Chassis

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / server-id*	Enters chassis server mode for the specified server in the specified chassis
Step 2	UCS-A /chassis/server # **show adapter status**	Displays the status of the adapter. Verify that the overall status of the adapter is in the Operable state. If the overall status of the adapter is in any state other than Operable, you cannot upgrade it. However, you can proceed with the upgrade for the other adapters in the Cisco UCS domain.

Example

The following example displays that the overall status for the adapter in server 7 on chassis 1 is in the Operable state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show adapter status
Server 1/1:
    Overall Status
    --------------
    Operable
```

Verification that the Data Path is Ready

The following sections detail the steps to verify that the data path is ready.

Verifying that Dynamic vNICs Are Up and Running

When you upgrade a Cisco UCS that includes dynamic vNICs and an integration with VMware vCenter, you must verify that all dynamic vNICs are up and running on the new primary fabric interconnect. Ensure that the vNICs are up and running before you activate the new software on the former primary fabric interconnect to avoid data path disruption.

Perform this step in the Cisco UCS Manager GUI.

Procedure

Step 1 In the **Navigation** pane, click **VM**.

Step 2 Expand **All** > **VMware** > **Virtual Machines**.

Step 3 Expand the virtual machine for which you want to verify the dynamic vNICs and choose a dynamic vNIC.

Step 4 In the **Work** pane, click the **VIF** tab.

Step 5 On the **VIF** tab, verify that the **Status** column for each VIF is **Online**.

Step 6 Repeat Steps 3 through 5 until you have verified that the VIFs for all dynamic vNICs on all virtual machines have a status of **Online**.

Verifying the Ethernet Data Path

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show int br | grep -v down | wc –l**	Returns the number of active Ethernet interfaces.

	Command or Action	Purpose
		Verify that this number matches the number of Ethernet interfaces that were up prior to the upgrade.
Step 3	UCS-A(nxos)# **show platform fwm info hw-stm | grep '1.' | wc –l**	Returns the total number of MAC addresses. Verify that this number matches the number of MAC addresses prior to the upgrade.

Example

The following example returns the number of active Ethernet interfaces and MAC addresses for subordinate fabric interconnect A so that you can verify that the Ethernet data path for that fabric interconnect is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show int br | grep -v down  | wc -l
86
UCS-A(nxos)# show platform fwm info hw-stm | grep '1.' | wc -l
80
```

Verifying the Data Path for Fibre Channel End-Host Mode

For best results when upgrading a Cisco UCS domain, we recommend that you perform this task before you begin the upgrade and after you activate the subordinate fabric interconnect, and then compare the two results.

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show npv flogi-table**	Displays a table of flogi sessions.
Step 3	UCS-A(nxos)# **show npv flogi-table | grep fc | wc -l**	Returns the number of servers logged into the fabric interconnect. The output should match the output you received when you performed this verification prior to beginning the upgrade.

Example

The following example displays the flogi-table and number of servers logged into subordinate fabric interconnect A so that you can verify that the Fibre Channel data path for that fabric interconnect in Fibre Channel End-Host mode is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                  EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc705    700  0x69000a 20:00:00:25:b5:27:03:01 20:00:00:25:b5:27:03:00 fc3/1
vfc713    700  0x690009 20:00:00:25:b5:27:07:01 20:00:00:25:b5:27:07:00 fc3/1
vfc717    700  0x690001 20:00:00:25:b5:27:08:01 20:00:00:25:b5:27:08:00 fc3/1

Total number of flogi = 3.

UCS-A(nxos)# show npv flogi-table | grep fc | wc -l
3
```

Verifying the Data Path for Fibre Channel Switch Mode

For best results when upgrading a Cisco UCS domain, we recommend that you perform this task before you begin the upgrade and after you activate the subordinate fabric interconnect, and then compare the two results.

Procedure

	Command or Action	Purpose
Step 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	Enters NX-OS mode for the fabric interconnect.
Step 2	UCS-A(nxos)# **show flogi database**	Displays a table of flogi sessions.
Step 3	UCS-A(nxos)# **show flogi database | grep –I fc | wc –1**	Returns the number of servers logged into the fabric interconnect. The output should match the output you received when you performed this verification prior to beginning the upgrade.

Example

The following example displays the flogi-table and number of servers logged into subordinate fabric interconnect A so that you can verify that the Fibre Channel data path for that fabric interconnect in Fibre Channel End-Host mode is up and running:

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc726           800   0xef0003  20:00:00:25:b5:26:07:02 20:00:00:25:b5:26:07:00
vfc728           800   0xef0007  20:00:00:25:b5:26:07:04 20:00:00:25:b5:26:07:00
vfc744           800   0xef0004  20:00:00:25:b5:26:03:02 20:00:00:25:b5:26:03:00
vfc748           800   0xef0005  20:00:00:25:b5:26:04:02 20:00:00:25:b5:26:04:00
vfc764           800   0xef0006  20:00:00:25:b5:26:05:02 20:00:00:25:b5:26:05:00
vfc768           800   0xef0002  20:00:00:25:b5:26:02:02 20:00:00:25:b5:26:02:00
vfc772           800   0xef0000  20:00:00:25:b5:26:06:02 20:00:00:25:b5:26:06:00
```

```
vfc778           800   0xef0001  20:00:00:25:b5:26:01:02 20:00:00:25:b5:26:01:00

Total number of flogi = 8.
UCS-A(nxos)# show flogi database | grep fc | wc -l
8
```