Unified Computing System Firmware Management Best Practices

Document ID: 110511

Contents

Introduction

Cisco Unified Computing System (UCS) is a complex collection of various hardware components that run embedded firmware. This document describes best practices for UCS firmware management.

Prerequisites

Requirements

Cisco recommends that you:

- Have a working knowledge of Cisco UCS blade server software and hardware
- Be familiar with Cisco UCS Manager GUI
- Understand the impact and implications of the different commands described in this document
- Be familiar with the UCS components and topology. Refer to the Network Diagram section for a diagram of a typical solution

Ensure that you meet these requirements before you attempt this configuration.

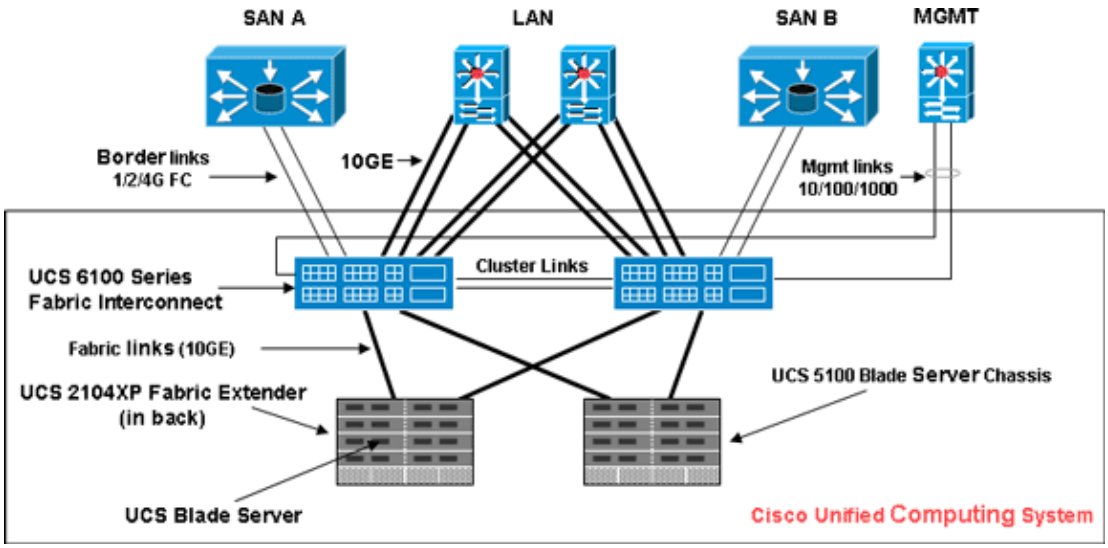
Components Used

The information in this document is based on Cisco UCS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a default configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This image shows a typical Cisco UCS topology:



Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Image Management Best Practices

Image Management

Here are some best practices to consider when you manage images:

- Before you perform firmware updates, use the UCS Manager image management interfaces in order to download relevant images to the fabric interconnect.
- Cisco UCS Manager maintains an inventory of available firmware images.
- Images are stored in `/bootflash` partition in the fabric interconnect.
- The `/bootflash` partition is dedicated solely to firmware images managed by the UCS Manager.
- Each fabric interconnect ships preloaded with one firmware package.
- Faults are raised when the `/bootflash` partition exceeds 70% and 90% capacity.
- Each image represents an individual firmware package specific to one hardware component. For example: IOM image, BMC image,UCS manager image, and so on.
- Multiple images are bundled together to form an image package.
- An image package is meant only for ease of distribution and download.
- Unlike an individual image, image packages do not have versions.

- Cisco publishes both individual images and image packages.

Image Download

Here are some best practices to consider when you download images:

- Cisco UCS Manager allows you to download both individual images and image packages.
- You can use these four protocols in order to transfer images to the Cisco UCS: SCP, FTP, SFTP, and TFTP.
- Image download can be initiated from the UCS CLI and GUI.
    - In order to download the image via the CLI, use the **download image** command in **scope firmware** mode.
    - In the GUI, click **Installed Firmware** under Equipment.
- A download task is created that can be used to monitor the download progress; use the **show download−task** command.
- When you download a package, the package is unpacked, and individual images are extracted from it.
- The same image can be downloaded multiple times.
- A failed (or successful) download tasks can be restarted.
    - In the CLI, use the **restart** command in **scope download−task** mode or execute the same download command again in order to start the download process.
    - In the GUI, click the **Restart** link under Download Task in order to resume the download process.
- Download tasks can be deleted at any time. When you delete a download task, downloaded images are not deleted.

Image Cluster Considerations

Special considerations must be taken into account when you download images in a UCS high−availability cluster configuration with multiple fabric interconnects.

Here are some best practices to consider when you download images to an HA cluster:

- In a fabric interconnect cluster, images on both fabric interconnects are automatically synced.
- When you download images or packages during cluster setup, images are automatically downloaded to both clustered fabric interconnects.
- When two previously separated fabric interconnects join to form a cluster, all images are synced from the primary fabric interconnect to the secondary.
- If images are deleted from the primary fabric interconnect when the subordinate is down, the images will be removed from the subordinate when it comes back up.

Image Delete

Here are some best practices to consider when you delete images:

- You can use the UCS Manager GUI or the CLI in order to remove unused images.
- Image deletion is asynchronous. When the administrator removes an image, the object is marked as Deleted." The delete process performed in the background.
- In the case of an HA cluster, images are automatically deleted on both fabric interconnects.
- Packages are read only, and they cannot be deleted.
- You can delete multiple images in either the UCS Manager GUI or CLI:

- Select multiple images in GUI.
- Execute the **delete image** command in the CLI.

  You can delete by *type* or *version*. For example, this command deletes all images versioned as 1.1(0.47):

  ```
  delete image version 1.1(0.47)
  ```

Image Catalog

Cisco UCS Manager provides two different views of the catalog of firmware images and their contents available on the fabric interconnect. The two views are packages and images.

Here are some best practices to consider for packages and images:

- The UCS Manager maintains inventory of all available images.
- The image catalog contains a list of images and packages.
- A package is a read−only object that is created when it is downloaded.
- A package does not occupy disk space. It represents a list or collection of images that were unpacked as part of the package download.
- A package cannot be deleted. Packages are automatically purged when all the images that are part of the package are removed.
- When an individual image is downloaded, the package name is the same as the image name.
- You can use the **show image** and **show package** commands in order to view the contents of a catalog.
- The **show image** command is available at each endpoint scope. Corresponding filters are applied.

  For example, the **show image** command under IOM scope displays all available IOM images.
- The **show system firmware expand** command displays firmware versions that run on all endpoints.
- The **show** <*endpoint*> **firmware** command displays all firmware details for that endpoint.

  For example, the **show server firmware** displays firmware details for all servers in the system.

Images in a Package

Package view provides you with a read−only representation of the packages that have been downloaded onto the fabric interconnect. By default this view is sorted by image, not by the contents of the image. For bundle images, you can use this view to see which component images exist in each downloaded bundle.

A package is comprised of these images:

- Fabric−interconnect kernel and system images
- UCS Manager image
- IOM firmware image
- BMC firmware image
- Network−facing adapter firmware (UCS CNA M71KR)
- Host−facing adapter firmware (applicable for UCS CNA M71KR adapter only)
  - QLogic option ROM
  - Emulex option ROM
  - Emulex firmware
- LSI option ROM
- LSI firmware
- BIOS

Image Versioning

- The NX−OS versioning scheme is similar to that of other NX−OS software family. For example: 4.0(0)N1.1
- Other UCS components follow the standard software format (X.Y.Z). For example: 1.0.0.

    - X is a major version or release and is used for major feature releases or architectural changes.
    - Y is a minor version or release.
    - Z is a bug fix version or release.

Firmware Update Best Practices

At a Glance

You can use either of these methods to update the firmware:

- Direct update Direct update at the endpoints.
- Firmware policy Updates to server components through service profiles that include a host firmware package policy and a management firmware package policy.

Cisco UCS Manager separates the direct update process into stages to ensure that you can push the firmware to a component while the system runs without affecting uptime on the server or other component. Because you do not need to reboot the server until after you activate the firmware update, you can perform that task overnight or during other maintenance windows.

These stages occur when you manually update firmware:

- *Update* During this stage, the system pushes the selected firmware version to the component. The update process overwrites the firmware in the backup slot on the component.
- *Activate* During this stage, the system sets the backup slot as active and reboots the endpoint. When the endpoint is rebooted, the backup slot becomes the active slot, and the active slot becomes the backup slot. The firmware in the new active slot becomes the startup version and the running version.

  If the component cannot boot from the startup firmware, it defaults to the backup version and raises an alarm.

Here are some best practices to consider for firmware updates:

- Many of the components in UCS can store more than one firmware image.
- The image with which the endpoint is booted is called the *running* version.
- The other non−active image is called the *backup* version.
- The image with which the endpoint would boot next time is called the *startup* version.
- The UCS Manager provides *update* operations to push a new version of the firmware to replace the backup image.
- The UCS Manager provides *activate* operations to change the running version to a new version.
- For some endpoints, you can use the *set−startup* option during activation in order to set the component boot image without resetting the device. The next reset will result in the component booting to the selected software image.
- For the fabric interconnect firmware and Cisco UCS Manager, no update is needed as the image is already present locally.
- LSI firmware, option ROM, host−facing adapter firmware, and BIOS cannot be updated directly like other components. These components can be updated only through firmware policies associated with the service profile.

- Cisco UCS Manager provides interfaces to update and activate. There is no ordering for endpoint resets during the activation.
- While updates can be issued simultaneously, Cisco recommends that software and firmware activations be issued in a logical, methodical order.
- Firmware that is activated must pass compatability checks; otherwise, the activation fails.

Components

Cisco UCS Manager supports update for these components:

- Fabric interconnect: Kernel image, system image, Cisco UCS Manager
- Chassis: IOM
- Server: BIOS, BMC, adapters, LSI

Kernel and System Images

Here are best practices to consider for kernel and system images:

- Kernel and system image activation is disruptive to application I/O and blade network connectivity as the fabric interconnect needs to be reset after activation is complete.
- In a cluster setup, each fabric interconnect can be activated independently of the other.
- After activation, fabric interconnect and all the IOMs connected to it are automatically reset.
- Although kernel and system images can be activated separately, Cisco recommends that you activate them together to reduce downtime.

UCS Manager Firmware

Here are best practices to consider for UCS Manager firmware:

- UCS Manager on both fabric interconnects must run the same version.
- UCS Manager activation brings down management for a brief period. All the virtual shell (VSH) connections are disconnected.
- In a cluster setup, UCS Manager on both fabric interconnects are activated.
- UCS Manager update does not affect server application I/O as fabric interconnects do not need to be reset.
- If UCS Manager is updated while subordinate is down, subordinate fabric interconnect automatically updates when it comes back online.

I/O Module Firmware

Here are best practices to consider for I/O module (IOM) firmware:

- Similar to other UCS components, each I/O module stores two images (a running image and a backup image).
- The update operation replaces the backup image of IOM with the new firmware version.
- The activate operation demotes the current startup image to a backup image. A new startup image is put in its place, and the system is configured to boot from this backup image.
- The *set−startup* option can be used to set only the active image; a reset does not occur. This process can be used to upgrade multiple I/O modules and then simultaneously reset them. If the fabric interconnect is updated and then activated, the fabric interconnect reboots the corresponding I/O Module, reducing the downtime.
- It is very important for the IOM and fabric interconnect to be compatible with each other.

- If the software that runs on the fabric interconnect detects an IOM that runs an incompatible version, it performs an automatic update of the IOM to bring it to the same version as the fabric interconnect system software.
- UCS Manager raises fault to indicate this situation. In additon, the discovery state of IOM displays *Auto updating* while the automatic update is in progress.
- The **show firmware [detail]** command at IOM scope shows running, backup, and startup firmware versions.
- In the UCS GUI, you can view the firmware at each chassis level on the Installed Firmware tab.

Server Firmware

Here are best practices to consider for I/O module (IOM) firmware:

- There are two methods to update the server firmware:
    - ♦ Direct update Manual method for installing server firmware at each server component endpoint. The direct update method is available only for BMC (adapter−network facing).
    - ♦ Firmware policy Results in automatic installation of the server firmware at a given endpoint when a service profile is bound to that server. The firmware policy method is logical and used with a service profile, which can be applied to any server.
- If a firmware is set to update with a service profile, direct update is not permitted.
- Direct update is not available for BIOS, LSI firmware, option ROM, and host−facing adapter firmware. These components can be updated only through firmware policy (via a service profile).
- The BMC server firmware is very similar to CMC in which it stores two images: running and backup.
- The **update firmware** command at scope BMC replaces the backup firmware with new version.
- The **activate firmware** command at scope BMC configures the backup image as the running image and the previous running version as the backup version.
- The **show firmware [detail]** command at scope BMC displays firmware details.

Direct Update

Here are best practices to consider for direct update:

- Network−facing firmware of UCS CNA M71KR also stores two images: running and backup.
- The **update firmware** command at scope adapter replaces the backup firmware with new version.
- The **activate firmware** command at scope adapter configures the backup image as the running image and the previous running version as the backup version.
- The **show firmware [detail]** command at scope adapter displays firmware details.
- UCS CNA M71KR includes host−facing firmware that is updated only through the firmware policy method.

Firmware Policy

You can update firmware through the service profiles on the server and adapter firmware, including the BIOS on the server. You must define these policies and include them in the service profile associated with a server:

- Two policies are supported:
    - ♦ Firmware Host pack BIOS, LSI Firmware, LSI option ROM, Qlogic option ROM, Emulex firmware, Emulex option ROM
    - ♦ Firmware Management Pack BMC
- Firmware packs can be created at the organization levels just like any other management policy.
- Each firmware pack can contain pack items that represent firmware per system component.

- Service profiles have two properties: one property for each type of firmware pack. If those properties are set to a valid pack name, associations trigger and firmware from the pack is applied to the server.
- The same firmware pack name can be used for multiple service profiles. Change in version of any of the pack items triggers reassociation of all the affected service profiles to apply the new version.

Verify

There is currently no specific verify for this configuration

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Aug 03, 2009 Document ID: 110511