Achieve Automated, End-to-End Firmware Management with Cisco UCS Manager

What You Will Learn

This document describes the operational benefits and advantages of firmware provisioning with Cisco® UCS Manager through features such as host firmware policies and service profiles. The document compares the ease of using Cisco UCS Manager to the current method of manually provisioning firmware on each component of server infrastructure. The benefits include greater utilization of resources and increased business agility because firmware can be managed automatically and from a single pane. This capability allows servers to be accurately repurposed for different functions in minutes rather than hours or days. The document also describes how firmware is managed on servers, switches, and fabric extenders using Cisco UCS Manager.

A Better, Faster, Easier Solution to Server Firmware Operations

Firmware management is an important, yet often overlooked, aspect of computing infrastructure management. To enable a server to be used to support a specific function, its firmware versions and settings must comply with the IT department's best practices. A database server, for example, might require a specific host bus adapter (HBA) firmware revision and settings to access Fibre Channel storage. Similarly, a custom, single-threaded application would see a performance benefit from turning on Intel Turbo Boost mode in the server's BIOS settings.

Firmware updates are necessary to accommodate new versions of firmware that fix bugs and security threats or to support alternate application workloads, different operating systems, or different I/O interfaces installed on servers. Keeping firmware on the myriad components in a server hardware stack up-to-date and available for specific functions is a complex, time-consuming, tedious, and thus error-prone chore. It usually involves multiple administrators who are responsible for using update tools that provision devices—such as HBAs, RAID controllers, network interface cards (NICs), BIOS, and the network data plane—one at a time, manually.

It can often take days to update every component's firmware and settings because until now the process has been manual and has lacked a scripted or automated solution. In addition, after it is begun, this manual firmware updating process is very difficult to undo should administrators decide to revert to original firmware versions. Firmware must be loaded and configured on one component at a time, with each type of firmware typically requiring the use of a component-specific updater. This tedious, complex, and time-consuming activity has prompted many companies to simply buy new servers as new needs arise, putting them into a pool for only a limited set of uses rather than modifying firmware on demand to put servers to use for different functions.

Now Cisco has a better way. Cisco UCS Manager provides two main advantages over past firmware provisioning:

- The capability to group multiple firmware components together in one package
- The capability to apply a firmware package to any compatible server in a single operation

Cisco UCS Manager provides an accurate, easier, faster, more flexible, and centralized solution for managing firmware across the entire hardware stack. Service profiles in Cisco UCS Manager abstract the physical hardware from its software properties. Service profiles allow administrators to associate any compatible firmware with any component of the hardware stack. Simply download the firmware versions needed from Cisco and then, within minutes, totally provision firmware on components within the server, fabric interconnect, and fabric extender based on required network, server, and storage policies per application and operating system.

Competitive benefits of the Cisco Unified Computing System™ firmware solution include the capability to:

- Perform faster, easier firmware provisioning using a policy-based approach that helps ensure compliance with IT standards and nearly eliminates the possibility of errors
- Optimize server environments with the right firmware for every operating system and application
- Repurpose servers as needed (for example, turn a web server into a database manager in minutes, and switch it back, in the same day)
- Scale more easily and add resources more flexibly with automated firmware provisioning
- Reduce capital and operational costs

Cisco UCS Manager Firmware Solution

The Cisco Unified Computing System integrates a low-latency unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multichassis platform in which all resources participate in a unified management domain.

Cisco UCS Manager is an embedded device management system that integrates the components of the Cisco Unified Computing System infrastructure into a single, cohesive entity. It provides the most streamlined, simplified approach to firmware provisioning on all server components that is commercially available today (Figure 1).

Figure 1. Cisco Unified Computing System Provides Complete Firmware Management for the Entire Hardware Stack

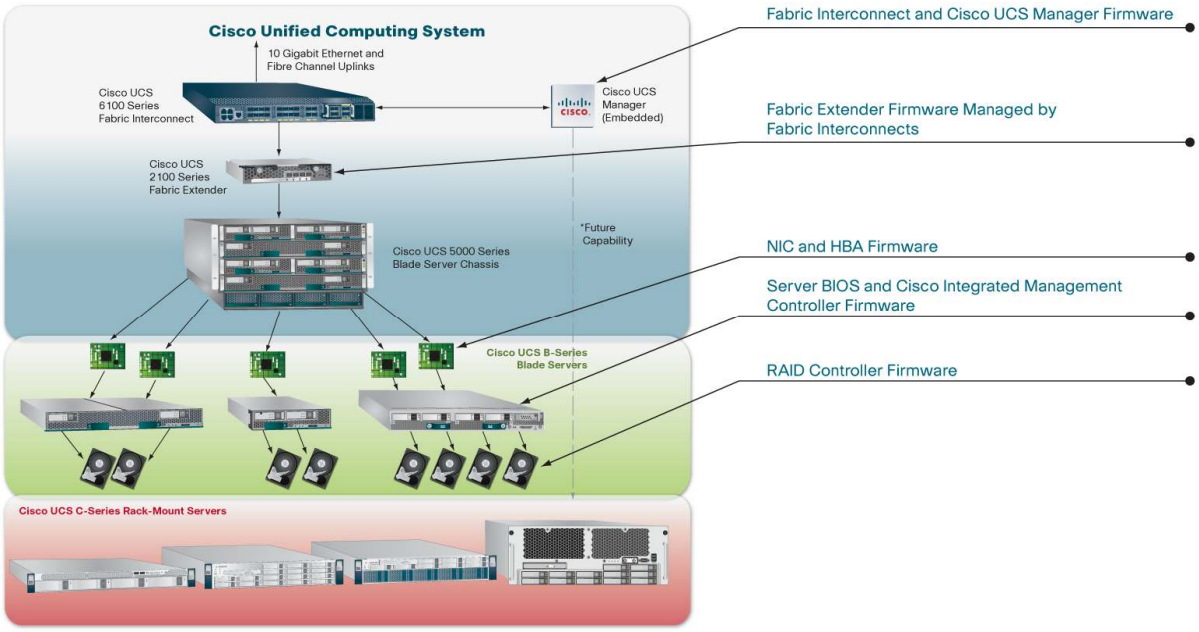


Figure 1 shows the Cisco Unified Computing System infrastructure, with various devices, components, and their related firmware, including:

- Cisco UCS 6100 Series Fabric Interconnects with 10 Gigabit Ethernet and Fibre Channel uplinks
- Cisco UCS Manager
- Cisco UCS 2100 Series Fabric Extenders
- Cisco UCS 5100 Series Blade Server Chassis, containing Cisco UCS B-Series Blade Servers with NICs, HBAs, and RAID controllers

Cisco UCS C-Series Rack-Mount Servers with a future migration path to the Cisco Unified Computing System and the Cisco UCS Manager firmware update solution

Firmware Policies and Service Profiles

Cisco UCS Manager has introduced a simplified, flexible process for firmware provisioning: Component firmware packages are grouped into a firmware policy, the firmware policy can be a part of one or more service profiles, and service profiles containing firmware packages are applied to physical servers. Two crucial process improvements make this simplified workflow possible:

- The capability to quickly choose and modify firmware policies from a central repository of firmware
- The capability to use these firmware policies (which specify a set of compatible versions) in service profiles to specify a complete, comprehensive set of firmware for all of a server's components

Different firmware policies or packages may be required to support different operating systems or applications. These firmware policies define an internally consistent, compliant set of firmware for the hardware stack. For example, there could be a firmware policy for specific server components running applications in Red Hat Linux, Microsoft Windows 2008, or other operating environments. After a firmware policy is created, an administrator can specify the desired firmware policy in a service profile. A service profile includes firmware revisions and settings plus the server's LAN and SAN requirements such as quality of service (QoS) and uplink specifications for upstream LAN and SAN switches and VLAN and VSAN membership. Other service profile information includes BIOS settings such as boot order and the RAID level on a blade's disk drives.

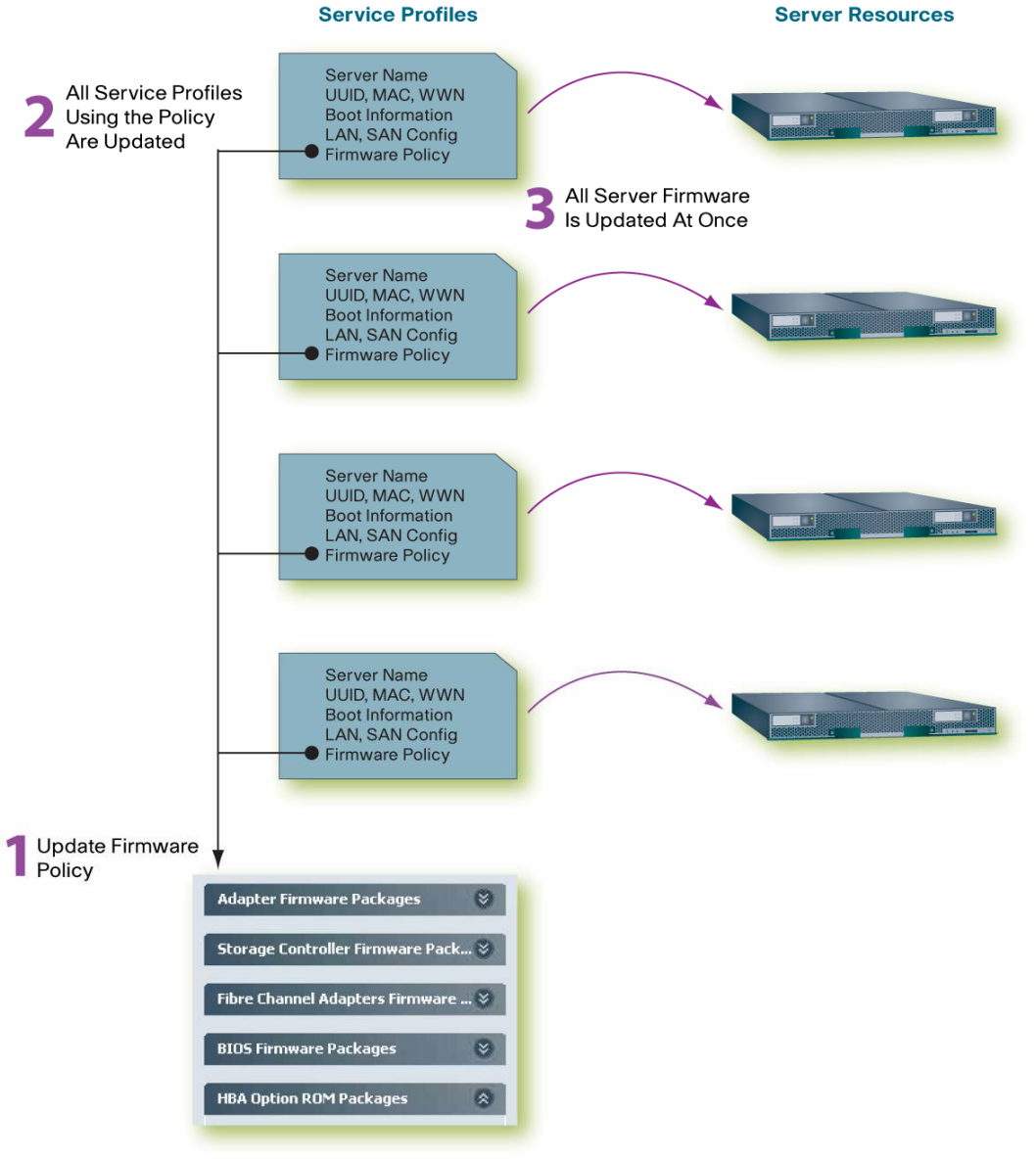
Using Cisco Unified Computing System firmware policies and service profiles, any server can be reprovisioned within minutes. Companies no longer have to buy new servers to dedicate to specific functions to avoid firmware provisioning. This easier, faster approach to firmware management can significantly reduce server expenditures, increase application availability through the introduction of fewer errors and less server downtime, and increase an organization's capability to use server resources to handle multiple tasks.

Best Practices for Updating Firmware

A service profile typically references a firmware policy that dictates the firmware revisions for all components of the hardware stack. For instance, Figure 2 shows four servers, each with unique identities and settings specified by their service profiles. Each service profile references the same firmware policy, so all four servers have identical sets of firmware applied to them.

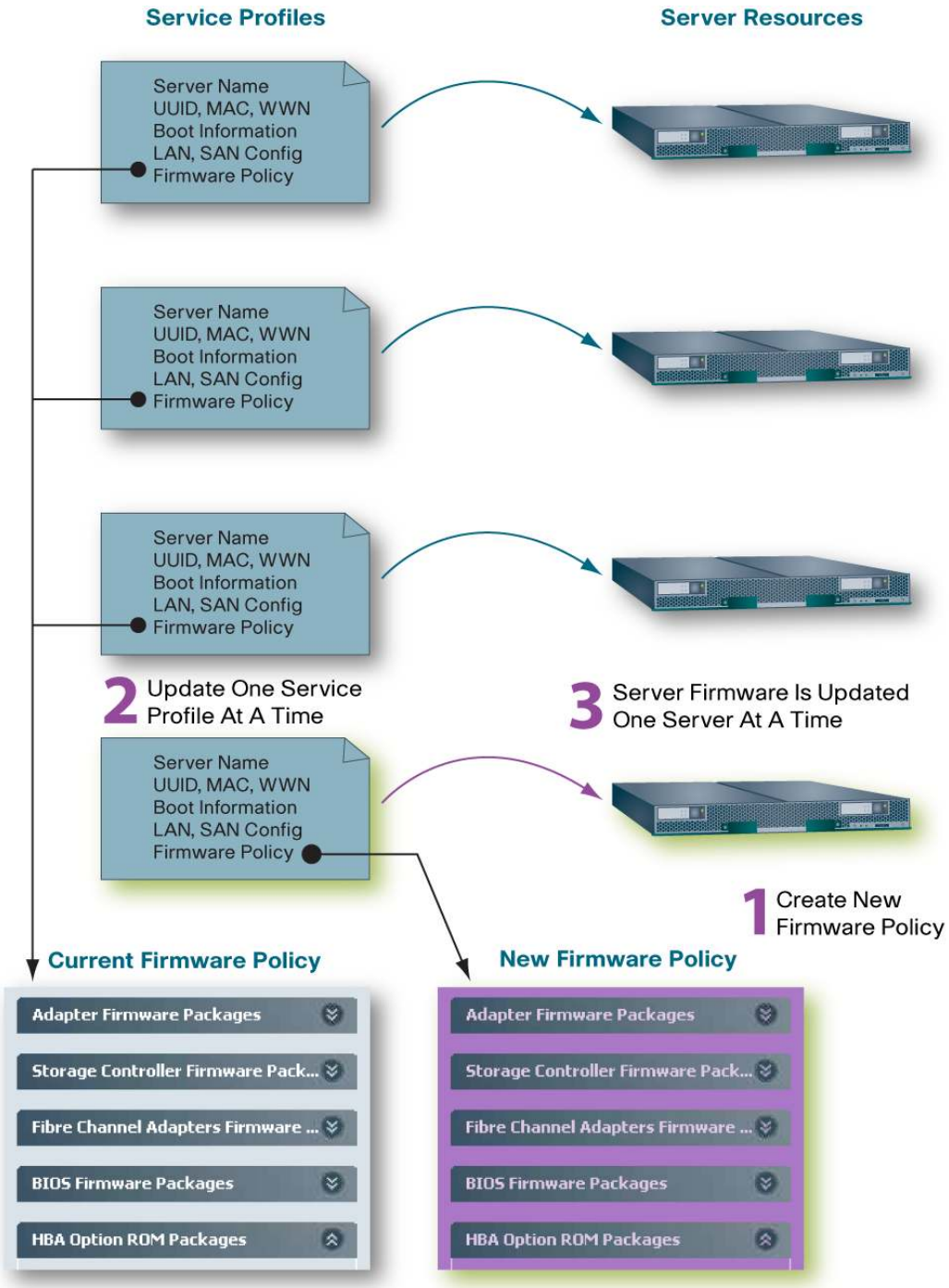
Firmware settings can be updated in two ways: all at once, or one at a time. To accomplish the former, an administrator could choose to update a firmware policy specified by multiple service profiles, resulting in an immediate update to all servers, with no other human intervention. Everything works together, is updated simultaneously, and remains consistent.

Figure 2. Assigning Service Profiles to Multiple Servers at Once



To remain compliant as new firmware becomes available, a best practice for updating firmware using Cisco UCS Manager is to create a new firmware policy and then associate it with the service profile of selected servers one at a time so that the new policy can be tested first before all servers are reprovisioned (Figure 3).

Figure 3. Changing Server Policies One at a Time for a Service Profile and Associated Server

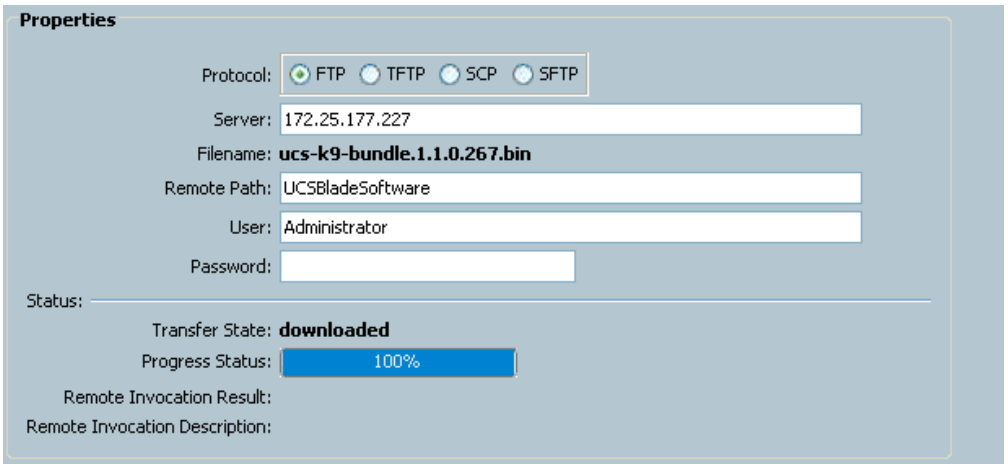


This approach is less disruptive because multiple servers are not being taken offline for firmware changes at the same time. Instead, the administrator can choose which servers to update. If the server does not operate properly with the revised policy referenced from the service profile, the administrator can immediately roll back to the previous firmware policy before correcting errors in the new policy and reprovisioning the server a second time.

How to Create and Associate a Service Profile with a Blade Server Step by Step

First, download the firmware from Cisco to a local file. Then upload that file securely to the Cisco UCS 6100 Series Fabric Interconnect using FTP, Trivial File Transfer Protocol (TFTP), Secure Copy Protocol (SCP), or Secure FTP (SFTP). This places the package into a firmware library where an inventory of available firmware images is maintained (Figure 4).

Figure 4. Downloading Firmware from Cisco to the Cisco UCS 6100 Series Fabric Interconnect



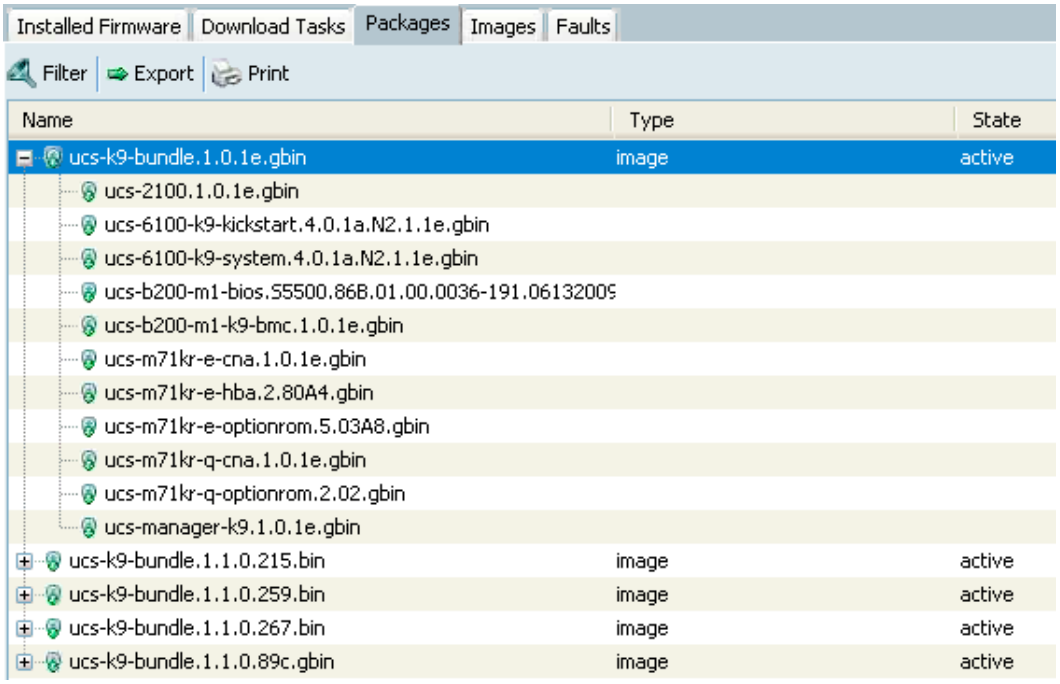
Before performing firmware updates on any other part of the server infrastructure, the Cisco UCS Manager Image Management interface should be used to download relevant images to the server and fabric extender. This operation is performed manually as these devices seldom require firmware upgrades. Images are stored in the /bootflash partition in the server, which is dedicated solely to firmware images managed by Cisco UCS Manager. Each Cisco UCS 6100 Series interconnect ships preloaded with one firmware package. Faults are raised when the /bootflash partition exceeds 70 and 90 percent capacity.

Firmware package downloads can be initiated from Cisco UCS Manager using the GUI. To download the firmware using the command-line interface (CLI), use the Download Image command in Scope Firmware mode. In the GUI, in the Equipment section, click Installed Firmware. A download task is created than can be used to monitor the download progress using the Show Download Task command.

When a package is downloaded, it is unpacked, and individual images are extracted from it.

Firmware is available in bundles for groups of server components or individually for single components. The firmware catalog for the Cisco UCS 6100 Series includes drop-down menus that show different firmware versions that can be specified as different server workloads are deployed (Figure 5). Firmware can be viewed from the catalog as bundles or individual images.

Figure 5. Firmware Bundles or Packages in the Cisco Unified Computing System Firmware Library

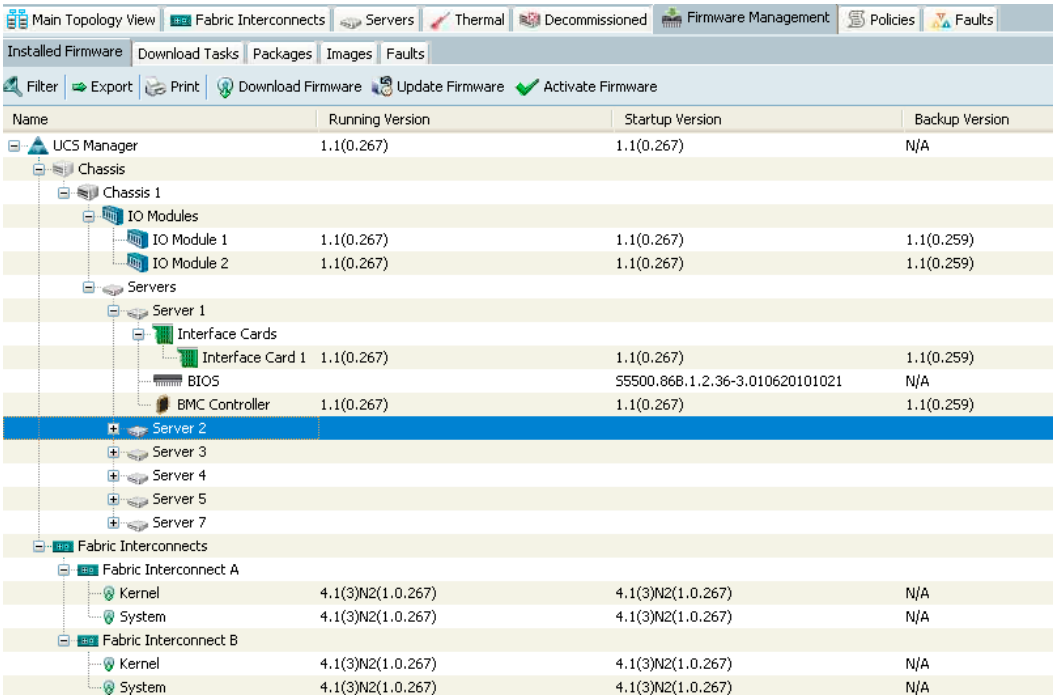


Here are the contents of a sample firmware bundle:

- Fabric interconnect kernel and system images
- Cisco UCS Manager image
- I/O module (IOM) firmware image
- Baseboard management controller (BMC) firmware image
- Network-facing adapter firmware for the Cisco UCS M71KR Converged Network Adapter (CNA)
- Host-facing adapter firmware for the Cisco UCS M71KR CNA including firmware for the integrated Emulex or QLogic HBA
- QLogic option ROM
- Emulex option ROM
- Emulex firmware
- LSI option ROM
- LSI firmware
- BIOS

Currently installed firmware images for the different components of each server can be viewed on the Image tab of the Cisco UCS Manager firmware library (Figure 6).

Figure 6. Servers and Their Components with Running, Startup, and Backup Versions of Firmware



Name	Running Version	Startup Version	Backup Version
UCS Manager	1.1(0.267)	1.1(0.267)	N/A
Chassis			
Chassis 1			
IO Modules			
IO Module 1	1.1(0.267)	1.1(0.267)	1.1(0.259)
IO Module 2	1.1(0.267)	1.1(0.267)	1.1(0.259)
Servers			
Server 1			
Interface Cards			
Interface Card 1	1.1(0.267)	1.1(0.267)	1.1(0.259)
BIOS		S5500.86B.1.2.36-3.010620101021	N/A
BMC Controller	1.1(0.267)	1.1(0.267)	1.1(0.259)
Server 2			
Server 3			
Server 4			
Server 5			
Server 7			
Fabric Interconnects			
Fabric Interconnect A			
Kernel	4.1(3)N2(1.0.267)	4.1(3)N2(1.0.267)	N/A
System	4.1(3)N2(1.0.267)	4.1(3)N2(1.0.267)	N/A
Fabric Interconnect B			
Kernel	4.1(3)N2(1.0.267)	4.1(3)N2(1.0.267)	N/A
System	4.1(3)N2(1.0.267)	4.1(3)N2(1.0.267)	N/A

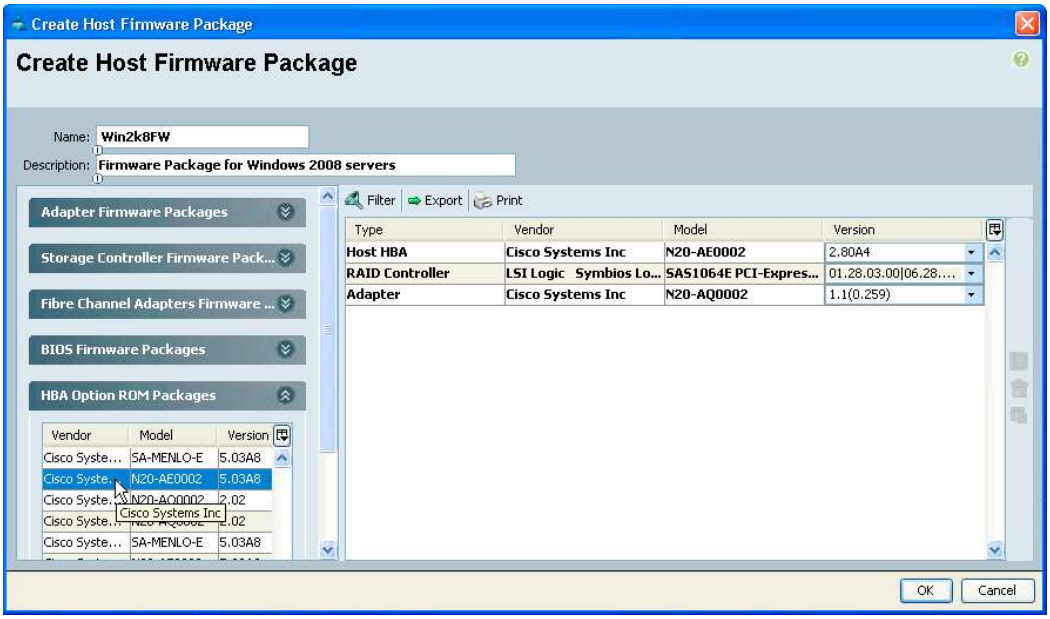
Other tabs and controls allow for the downloading, updating, and activation of firmware versions. All the components—including chasses, IOMs, HBAs, NICs, and interface cards for the services processors—are displayed with all their firmware. This view is a major advantage over approaches that require use of a separate element manager for each individual component.

When provisioning firmware, the Backup Firmware feature provides a secondary location from which firmware can be loaded. The backup location allows administrators to place the target version of the firmware on the server. This approach enables a fast switchover at the time of the actual upgrade, since nothing needs to be downloaded at that time. In addition, it provides a quick failover mechanism. If a problem occurs with the new target firmware, the system can revert to its original firmware without any additional downloads.

The Backup Firmware feature also gives administrators the option to activate the new firmware during off-peak hours so network processing is not adversely affected. This capability is especially useful with large firmware images, which take a longer time to activate.

With Cisco UCS Manager, server, storage, and network administrators create firmware policies for the range of devices in a server infrastructure based on different operating systems or applications. Creating a policy involves creating a policy name with a list of firmware versions as properties (Figure 7).

Figure 7. Creating Firmware Policies



Policy creation for specific server components (HBA, RAID controller, adapter, etc.) then involves choosing firmware versions using drop-down menus with point-and-click ease.

Policy for a particular server and application then is selected from a service profile (Figure 8). The server defined by the service profile then immediately reboots, and the new service profile becomes active, directing the server components to perform based on the previously defined policies.

Figure 8. Creating Service Profiles with Policies

Service profiles in Cisco UCS Manager can be accessed, created, and modified by external management tools using XML APIs. The API also provides integration with external configuration management databases for inventory population, asset tracking, and granular configuration and state information. Since they reside below the operating system, service profiles can be used in conjunction with existing tools, like those for patch management.

Using service profiles as templates, administrators can quickly deploy new service profiles, replacing dynamic or variable parameters with pointers to specific resource pools. For example, instead of specifying a specific worldwide name (WWN) in a service profile template, the template can include a pointer to a pool of WWNs that are managed by Cisco UCS Manager for that particular service profile. This approach allows the maintenance of different pools for different service profiles.

Conclusion

The Cisco UCS Manager firmware solution brings significant advantages over current, manual or separate firmware provisioning methods. Firmware management for network, SAN, and server components can be handled from one centralized location. With the Cisco Unified Computing System, an enterprise can slide a blade server into a blade chassis and with a few mouse clicks can completely provision the server based on policies defined by subject-matter experts. All other server infrastructure can be similarly provisioned.

Instead of managing server firmware manually, administrators can rely on Cisco UCS Manager to simplify and expedite the process, downloading firmware packages to the Cisco UCS Manager's firmware library, creating policies that dictate firmware revisions for each server component, and then applying those policies by updating service profiles associated with servers one at a time or in a bulk upgrade.

Over time, the complexity of today's servers has made firmware provisioning more complex. Virtualization also introduces operational complexity. While it is easy to add a new virtual machine and move it across a physical infrastructure, network and storage administrators have experienced big increases in change requests, and this increase has been exacerbated by the use of automated live migration of virtual machines.

Cisco UCS Manager brings an orderly, automated, flexible new experience to administrators. The capability to perform faster, easier, and less expensive firmware provisioning enables companies to easily repurpose servers as needed, instead of having to buy more hardware for dedicated tasks to avoid server provisioning delays and complexity. Cisco UCS Manager also facilitates optimization of server environments, making it easier to provide the right firmware for every application and operating system. The solution also allows server environments to scale more easily and add resources more flexibly.

The enhanced firmware provisioning approach used by Cisco UCS Manager is characteristic of the unified approach of the Cisco Unified Computing System. Cisco is dedicated to providing portability of both physical and virtual environments, with server identity, LAN and SAN addressing, I/O configurations, firmware, and network connectivity profiles used to dynamically provision and integrate server and network resources. Such a highly dynamic and stateless environment can be adapted to meet rapidly changing needs in today's data centers, with benefits including just-in-time deployment of new computing resources and simplified, reliable movement of traditional and virtual workloads.

For More Information

- **Cisco Unified Computing System:** http://www.cisco.com/en/US/netsol/ns944/index.html
- **Cisco Unified Computing System introductory video:** http://www.cisco.com/cdc_content_elements/flash/netsol/data_center/ucs_video/pop.html
- **Cisco UCS Manager:** http://www.cisco.com/en/US/products/ps10281/index.html
- **Configuring Cisco UCS Manager:** http://www.cisco.com/en/US/products/ps10281/tsd_products_support_configure.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Printed in USA C11-588010-00 03/10