

# Prácticas recomendadas de administración del firmware de Unified Computing System

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Prácticas recomendadas de administración de imágenes](#)

[Administración de imágenes](#)

[Descarga de imágenes](#)

[Consideraciones sobre el clúster de imágenes](#)

[Eliminación de imagen](#)

[Catálogo de imágenes](#)

[Imágenes en un paquete](#)

[Versión de imagen](#)

[Prácticas recomendadas de actualización del firmware](#)

[Guía rápida](#)

[Componentes](#)

[Imágenes del núcleo y del sistema](#)

[Firmware de UCS Manager](#)

[Firmware del módulo de E/S](#)

[Firmware del servidor](#)

[Actualización directa](#)

[Política de firmware](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## [Introducción](#)

Cisco Unified Computing System (UCS) es una compleja colección de varios componentes de hardware que ejecutan firmware integrado. Este documento describe las prácticas recomendadas para la administración del firmware UCS.

## [Prerequisites](#)

## Requirements

Cisco recomienda:

- Conocimiento práctico del software y el hardware del servidor blade Cisco UCS
- Familiarícese con la GUI de Cisco UCS Manager
- Comprender el impacto y las implicaciones de los diferentes comandos descritos en este documento
- Familiarícese con los componentes y la topología de UCS. Consulte la sección [Diagrama de red](#) para ver un diagrama de una solución típica

Asegúrese de cumplir estos requisitos antes de intentar esta configuración.

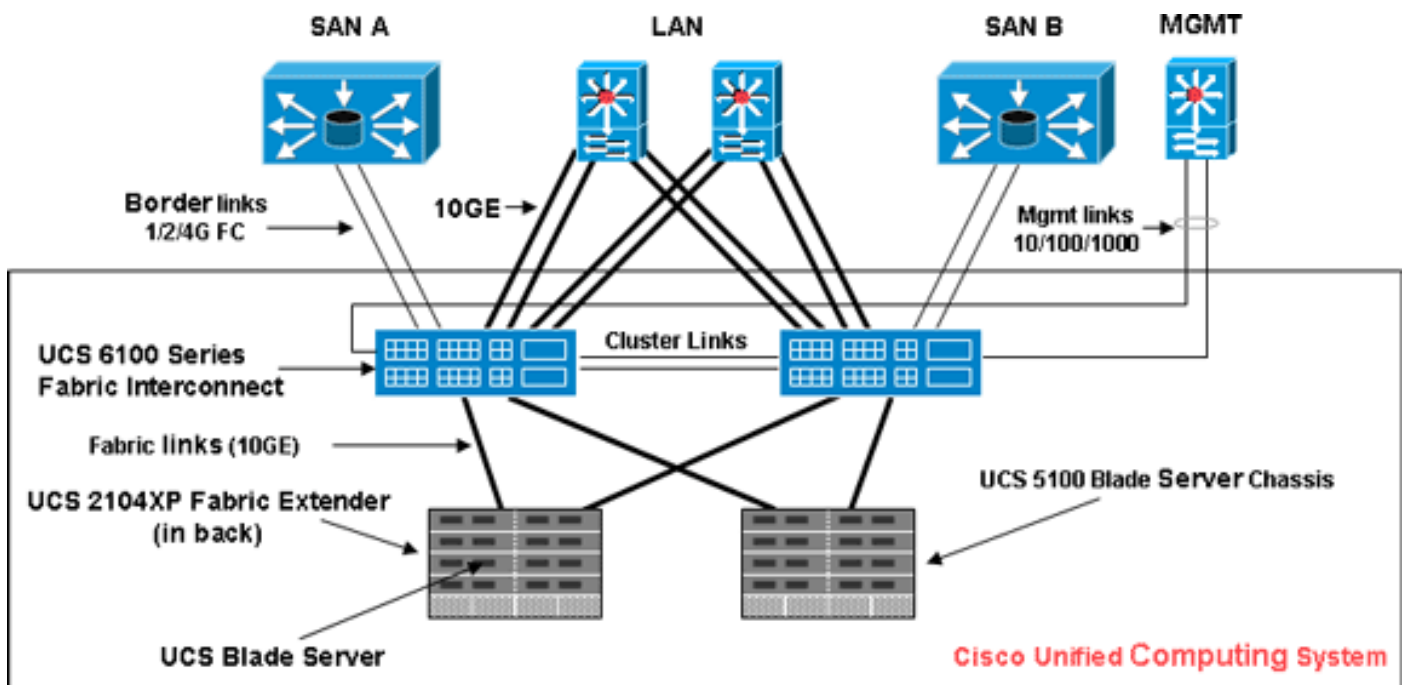
## Componentes Utilizados

La información de este documento se basa en Cisco UCS.

The information in this document was created from the devices in a specific lab environment. Todos los dispositivos utilizados en este documento comenzaron con una configuración predeterminada. If your network is live, make sure that you understand the potential impact of any command.

## Diagrama de la red

Esta imagen muestra una topología típica de Cisco UCS:



## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Prácticas recomendadas de administración de imágenes

## [Administración de imágenes](#)

Estas son algunas prácticas recomendadas que debe tener en cuenta al administrar imágenes:

- Antes de realizar actualizaciones de firmware, utilice las interfaces de administración de imágenes de UCS Manager para descargar las imágenes relevantes a la fabric interconectada.
- Cisco UCS Manager mantiene un inventario de las imágenes de firmware disponibles.
- Las imágenes se almacenan en la partición `/bootflash` en la Fabric Interconnect.
- La partición `/bootflash` está dedicada exclusivamente a las imágenes de firmware administradas por UCS Manager.
- Cada Fabric Interconnect se suministra precargado con un paquete de firmware.
- Los errores se producen cuando la partición `/bootflash` supera el 70% y el 90% de la capacidad.
- Cada imagen representa un paquete de firmware individual específico de un componente de hardware. Por ejemplo: Imagen IOM, imagen BMC, imagen de UCS Manager, etc.
- Se agrupan varias imágenes para formar un paquete de imágenes.
- Un paquete de imágenes está diseñado sólo para facilitar la distribución y descarga.
- A diferencia de una imagen individual, los paquetes de imágenes no tienen versiones.
- Cisco publica tanto imágenes individuales como paquetes de imágenes.

## [Descarga de imágenes](#)

Estas son algunas prácticas recomendadas que debe tener en cuenta al descargar imágenes:

- Cisco UCS Manager le permite descargar imágenes individuales y paquetes de imágenes.
- Puede utilizar estos cuatro protocolos para transferir imágenes a Cisco UCS: SCP, FTP, SFTP y TFTP.
- La descarga de imágenes se puede iniciar desde la CLI y la GUI de UCS. Para descargar la imagen a través de la CLI, utilice el comando **download image** en el **modo de firmware de alcance**. En la GUI, haga clic en **Installed Firmware** en Equipment.
- Se crea una tarea de descarga que se puede utilizar para monitorear el progreso de la descarga; utilice el comando **show download-task**.
- Cuando descarga un paquete, el paquete se desempaqueta y se extraen imágenes individuales de él.
- La misma imagen se puede descargar varias veces.
- Se pueden reiniciar las tareas de descarga fallidas (o exitosas). En la CLI, utilice el comando **restart** en el modo **scope download-task** o ejecute el mismo comando **download** de nuevo para iniciar el proceso de descarga. En la GUI, haga clic en el enlace **Restart** bajo Download Task para reanudar el proceso de descarga.
- Las tareas de descarga se pueden eliminar en cualquier momento. Cuando elimina una tarea de descarga, las imágenes descargadas no se eliminan.

## [Consideraciones sobre el clúster de imágenes](#)

Se deben tener en cuenta consideraciones especiales al descargar imágenes en una configuración de clúster de alta disponibilidad de UCS con varias Fabric Interconnects.

Estas son algunas prácticas recomendadas que debe tener en cuenta al descargar imágenes a un clúster de alta disponibilidad:

- En un clúster de Fabric Interconnect, las imágenes de ambos Fabric Interconnects se sincronizan automáticamente.
- Cuando descarga imágenes o paquetes durante la configuración del clúster, las imágenes se descargan automáticamente en ambos Fabric Interconnects agrupados.
- Cuando dos Fabric Interconnects previamente separados se unen para formar un clúster, todas las imágenes se sincronizan desde el Fabric Interconnect primario hasta el secundario.
- Si las imágenes se eliminan del fabric interconnect primario cuando el subordinado está inactivo, las imágenes se quitarán del subordinado cuando vuelva a funcionar.

## Eliminación de imagen

Estas son algunas de las prácticas recomendadas a tener en cuenta al eliminar imágenes:

- Puede utilizar la GUI de UCS Manager o la CLI para eliminar las imágenes no usadas.
- La eliminación de la imagen es asíncronica. Cuando el administrador quita una imagen, el objeto se marca como "Eliminado". El proceso de eliminación realizado en segundo plano.
- En el caso de un clúster HA, las imágenes se eliminan automáticamente en ambas Fabric Interconnects.
- Los paquetes son de sólo lectura y no se pueden eliminar.
- Puede eliminar varias imágenes en la GUI o CLI de UCS Manager: Seleccione varias imágenes en la GUI. Ejecute el comando **delete image** en la CLI. Puede eliminar por *tipo* o *versión*. Por ejemplo, este comando elimina todas las imágenes con versión 1.1(0.47):  
`delete image version 1.1(0.47)`

## Catálogo de imágenes

Cisco UCS Manager ofrece dos vistas diferentes del catálogo de imágenes de firmware y su contenido disponible en Fabric Interconnect. Las dos vistas son paquetes e imágenes.

A continuación, se muestran algunas prácticas recomendadas para paquetes e imágenes:

- UCS Manager mantiene el inventario de todas las imágenes disponibles.
- El catálogo de imágenes contiene una lista de imágenes y paquetes.
- Un paquete es un objeto de sólo lectura que se crea cuando se descarga.
- Un paquete no ocupa espacio en disco. Representa una lista o colección de imágenes que fueron desempaquetadas como parte de la descarga del paquete.
- No se puede eliminar un paquete. Los paquetes se depuran automáticamente cuando se eliminan todas las imágenes que forman parte del paquete.
- Cuando se descarga una imagen individual, el nombre del paquete es el mismo que el nombre de la imagen.
- Puede utilizar los comandos **show image** y **show package** para ver el contenido de un catálogo.
- El comando **show image** está disponible en cada ámbito de punto final. Se aplican los filtros correspondientes. Por ejemplo, el comando **show image** en el ámbito IOM muestra todas las imágenes IOM disponibles.
- El comando **show system firmware extend** muestra las versiones de firmware que se ejecutan

en todos los terminales.

- El comando **show <terminal> firmware** muestra todos los detalles del firmware para ese terminal. Por ejemplo, el comando **show server firmware** muestra los detalles del firmware de todos los servidores del sistema.

## Imágenes en un paquete

La vista de paquetes le proporciona una representación de sólo lectura de los paquetes que se han descargado en la Fabric Interconnect. De forma predeterminada, esta vista se ordena por imagen, no por el contenido de la imagen. Para las imágenes de paquete, puede utilizar esta vista para ver qué imágenes de componentes existen en cada paquete descargado.

Un paquete se compone de estas imágenes:

- Imágenes del núcleo y del sistema Fabric-Interconnect
- imagen de UCS Manager
- imagen de firmware IOM
- imagen del firmware BMC
- Firmware del adaptador de red (UCS CNA M71KR)
- Firmware del adaptador de cara al host (aplicable únicamente al adaptador UCS CNA M71KR)ROM de opción QLogicROM de opción Emulexfirmware Emulex
- ROM de opción LSI
- firmware LSI
- BIOS

## Versión de imagen

- El esquema de versiones de NX-OS es similar al de otras familias de software de NX-OS. Por ejemplo: 4.0(0)N1.1
- Otros componentes de UCS siguen el formato de software estándar (X.Y.Z). Por ejemplo: 1.0.0.X es una versión o versión principal y se utiliza para las principales versiones de funciones o cambios arquitectónicos.Y es una versión o versión secundaria.Z es una versión o versión de corrección de errores.

## Prácticas recomendadas de actualización del firmware

### Guía rápida

Puede utilizar cualquiera de estos métodos para actualizar el firmware:

- [Actualización directa](#): actualización directa en los terminales.
- [Política de firmware](#): actualiza los componentes del servidor a través de perfiles de servicio que incluyen una política de paquete de firmware de host y una política de paquete de firmware de administración.

Cisco UCS Manager separa el proceso de actualización directa en fases para garantizar que puede enviar el firmware a un componente mientras el sistema se ejecuta sin que ello afecte al tiempo de actividad del servidor ni de otros componentes. Dado que no es necesario reiniciar el servidor hasta después de activar la actualización del firmware, puede realizar esa tarea de la

noche a la mañana o durante otras ventanas de mantenimiento.

Estas etapas se producen cuando se actualiza manualmente el firmware:

- *Actualizar*: durante esta etapa, el sistema envía la versión de firmware seleccionada al componente. El proceso de actualización sobrescribe el firmware en la ranura de copia de seguridad del componente.
- *Activar*: durante esta etapa, el sistema configura la ranura de respaldo como activa y reinicia el terminal. Cuando se reinicia el punto final, la ranura de respaldo se convierte en la ranura activa y la ranura activa se convierte en la ranura de respaldo. El firmware en la nueva ranura activa se convierte en la versión de inicio y en la versión en ejecución. Si el componente no puede arrancar desde el firmware de inicio, de forma predeterminada aparece la versión de copia de seguridad y provoca una alarma.

Estas son algunas prácticas recomendadas que se deben tener en cuenta para las actualizaciones de firmware:

- Muchos de los componentes de UCS pueden almacenar más de una imagen de firmware.
- La imagen con la que se inicia el punto final se denomina *versión en ejecución*.
- La otra imagen no activa se denomina la *versión de respaldo*.
- La imagen con la que el punto final se iniciaría la próxima vez se denomina la *versión inicial*.
- UCS Manager proporciona operaciones *de actualización* para enviar una nueva versión del firmware para reemplazar la imagen de respaldo.
- UCS Manager proporciona operaciones *de activación* para cambiar la versión en ejecución a una nueva versión.
- Para algunos extremos, puede utilizar la opción *set-startup* durante la activación para configurar la imagen de inicio del componente sin reiniciar el dispositivo. El siguiente reinicio dará como resultado el arranque del componente a la imagen de software seleccionada.
- Para el firmware de Fabric Interconnect y Cisco UCS Manager, no se necesita ninguna actualización, ya que la imagen ya está presente de forma local.
- El firmware de LSI, la opción ROM, el firmware del adaptador orientado al host y el BIOS no se pueden actualizar directamente como otros componentes. Estos componentes sólo se pueden actualizar mediante políticas de firmware asociadas al perfil de servicio.
- Cisco UCS Manager proporciona interfaces para actualizar y activar. No se ha realizado ningún pedido de reinicios de terminales durante la activación.
- Si bien las actualizaciones se pueden ejecutar simultáneamente, Cisco recomienda que las activaciones de software y firmware se emitan en un orden lógico y metódico.
- El firmware que se activa debe pasar las comprobaciones de compatibilidad; de lo contrario, la activación falla.

## Componentes

Cisco UCS Manager admite actualizaciones para estos componentes:

- Fabric Interconnect: Imagen del núcleo, imagen del sistema, Cisco UCS Manager
- Chasis: IOM
- Servidor: BIOS, BMC, adaptadores, LSI

## Imágenes del núcleo y del sistema

Estas son las mejores prácticas a considerar para las imágenes del núcleo y del sistema:

- La activación de la imagen del núcleo y del sistema interrumpe la conectividad de la red de servidores blade y de E/S de la aplicación, ya que la fabric interconectada debe restablecerse una vez que se haya completado la activación.
- En una configuración de clúster, cada Fabric Interconnect se puede activar independientemente del otro.
- Después de la activación, la fabric interconectada y todas las IOM conectadas a ella se restablecen automáticamente.
- Aunque las imágenes del núcleo y del sistema se pueden activar por separado, Cisco recomienda activarlas juntas para reducir el tiempo de inactividad.

## Firmware de UCS Manager

A continuación se indican las prácticas recomendadas que se deben tener en cuenta para el firmware de UCS Manager:

- UCS Manager en ambos fabric interconnects debe ejecutar la misma versión.
- La activación de UCS Manager reduce la administración durante un breve período. Todas las conexiones del shell virtual (VSH) se desconectan.
- En una configuración de clúster, se activa UCS Manager en ambos Fabric Interconnects.
- La actualización de UCS Manager no afecta a la E/S de la aplicación del servidor, ya que no es necesario restablecer los Fabric Interconnects.
- Si UCS Manager se actualiza mientras la persona subordinada está inactiva, la fabric interconectada subordinada se actualiza automáticamente cuando vuelve a estar en línea.

## Firmware del módulo de E/S

A continuación se indican las prácticas recomendadas que se deben tener en cuenta para el firmware del módulo de E/S (IOM):

- Al igual que otros componentes de UCS, cada módulo de E/S almacena dos imágenes (una imagen en ejecución y una imagen de copia de seguridad).
- La operación de actualización reemplaza la imagen de copia de seguridad de IOM con la nueva versión de firmware.
- La operación de activación degrada la imagen de inicio actual a una imagen de copia de seguridad. Se coloca una nueva imagen de inicio y el sistema se configura para arrancar desde esta imagen de copia de seguridad.
- La opción *set-startup* se puede utilizar para establecer solamente la imagen activa; no se produce un reinicio. Este proceso se puede utilizar para actualizar varios módulos de E/S y, a continuación, restablecerlos simultáneamente. Si se actualiza y se activa la fabric interconectada, la fabric interconectada reinicia el módulo de E/S correspondiente, lo que reduce el tiempo de inactividad.
- Es muy importante que la IOM y la fabric interconectada sean compatibles entre sí.
- Si el software que se ejecuta en Fabric Interconnect detecta un IOM que ejecuta una versión incompatible, realiza una actualización automática del IOM para llevarlo a la misma versión que el software del sistema Fabric Interconnect.
- UCS Manager genera un error para indicar esta situación. Además, el estado de detección de

- IOM muestra *Actualización automática* mientras la actualización automática está en curso.
- El comando **show firmware [detail]** en el ámbito IOM muestra las versiones de firmware de ejecución, copia de seguridad y inicio.
  - En la GUI de UCS, puede ver el firmware en cada nivel de chasis en la ficha Firmware instalado.

## Firmware del servidor

A continuación se indican las prácticas recomendadas que se deben tener en cuenta para el firmware del módulo de E/S (IOM):

- Hay dos métodos para actualizar el firmware del servidor: [Actualización directa](#): método manual para instalar el firmware del servidor en cada extremo del componente del servidor. El método de actualización directa sólo está disponible para BMC (orientado a la red del adaptador). [Política de firmware](#): permite la instalación automática del firmware del servidor en un punto final dado cuando un perfil de servicio se enlaza a ese servidor. El método de política de firmware es lógico y se utiliza con un perfil de servicio, que se puede aplicar a cualquier servidor.
- Si un firmware está configurado para actualizarse con un perfil de servicio, no se permite la actualización directa.
- La actualización directa no está disponible para BIOS, firmware LSI, ROM de opción y firmware de adaptador orientado al host. Estos componentes solo se pueden actualizar mediante la política de firmware (a través de un perfil de servicio).
- El firmware del servidor BMC es muy similar al CMC en el que almacena dos imágenes: ejecución y copia de seguridad.
- El comando **update firmware** en el ámbito BMC reemplaza el firmware de copia de seguridad por una nueva versión.
- El comando **activar firmware** en el BMC configura la imagen de respaldo como la imagen en ejecución y la versión anterior en ejecución como la versión de respaldo.
- El comando **show firmware [detail]** en scope BMC muestra los detalles del firmware.

## Actualización directa

Estas son las prácticas recomendadas que se deben tener en cuenta para la actualización directa:

- El firmware orientado a la red de UCS CNA M71KR también almacena dos imágenes: ejecución y copia de seguridad.
- El comando **update firmware** en el adaptador de alcance reemplaza el firmware de copia de seguridad por una nueva versión.
- El comando **activar firmware** en el adaptador de alcance configura la imagen de respaldo como la imagen en ejecución y la versión en ejecución anterior como la versión de respaldo.
- El comando **show firmware [detail]** en el adaptador de alcance muestra los detalles del firmware.
- UCS CNA M71KR incluye firmware orientado al host que se actualiza únicamente a través del método de política de firmware.

## Política de firmware



Puede actualizar el firmware a través de los perfiles de servicio del firmware del servidor y del adaptador, incluido el BIOS del servidor. Debe definir estas políticas e incluirlas en el perfil de servicio asociado a un servidor:

- Se admiten dos políticas: Paquete de host de firmware: BIOS, firmware LSI, ROM de opción LSI, ROM de opción Qlogic, firmware Emulex y ROM de opción Emulex Paquete de administración de firmware: BMC
- Los paquetes de firmware se pueden crear en los niveles de la organización, al igual que cualquier otra política de gestión.
- Cada paquete de firmware puede contener elementos de paquete que representan el firmware por componente del sistema.
- Los perfiles de servicio tienen dos propiedades: una propiedad para cada tipo de paquete de firmware. Si esas propiedades se establecen en un nombre de paquete válido, las asociaciones activan y el firmware del paquete se aplica al servidor.
- Se puede utilizar el mismo nombre de paquete de firmware para varios perfiles de servicio. El cambio en la versión de cualquiera de los elementos del paquete provoca la reasociación de todos los perfiles de servicio afectados para aplicar la nueva versión.

## [Verificación](#)

Actualmente no hay ninguna verificación específica para esta configuración

## [Troubleshoot](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## [Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)