

Aplicación de un parche de imagen ESXI no personalizado en un clúster Hyperflex

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Actualizar mediante CLI](#)

[Actualización mediante interfaz de usuario de HX Connect](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el proceso para aplicar parches a un nodo de ESXI Hyperflex con una imagen HX no personalizada a través de la interfaz de línea de comandos (CLI) o de HX Connect.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Hiperflex
- ESXI

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- HyperFlex Connect 5.0.2d
- Clúster estándar Hyperflex
- vCenter 8.0
- VMware ESXI, versión 7.0.3 (23794027)
- VMware ESXI, 7.0.3 build-24585291 (parche de destino)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco no siempre proporciona un paquete HyperFlex independiente para cada nueva versión de parche de VMware ESXi. Con las actualizaciones críticas de ESXi es posible aplicarlas manualmente con cualquiera de los métodos presentados en este artículo. Sin embargo, HyperFlex no recomienda actualizar ESXi con VMware Update Manager (VUM) o VMware Lifecycle Manager (vLCM), ya que puede causar problemas con determinados paquetes de instalación de HyperFlex vSphere (VIB).

Los parches no personalizados solo se pueden aplicar para las mismas versiones de ESXi. Si utiliza ESXi 7.0 u3, solo puede aplicar parches de 7.0u3+ y no puede actualizar de 7.0u3 a 8.0u2 u 8.0u3, ni actualizar de 8.0u2x a 8.0u3x con imágenes no personalizadas.

Antes de aplicar cualquier parche, asegúrese de que la versión actual de la plataforma de datos HyperFlex (HXDP) es compatible con la versión de ESXi que tiene pensado instalar. El gráfico de compatibilidad es el siguiente:

Versión	Servidores VMware ESXi versión HX
6.0(1x)	7 U3, 8 U2
5.5(2a)	7 U3, 8 U2, 8 U3
5.5(1 bis)	7 U3
5.0(2)	7 U3

Si su versión de HXDP es anterior, actualice primero HXDP y, a continuación, ESXi.

Configurar

Descargar el archivo zip de ESXi desde el [sitio web de Broadcom](#)

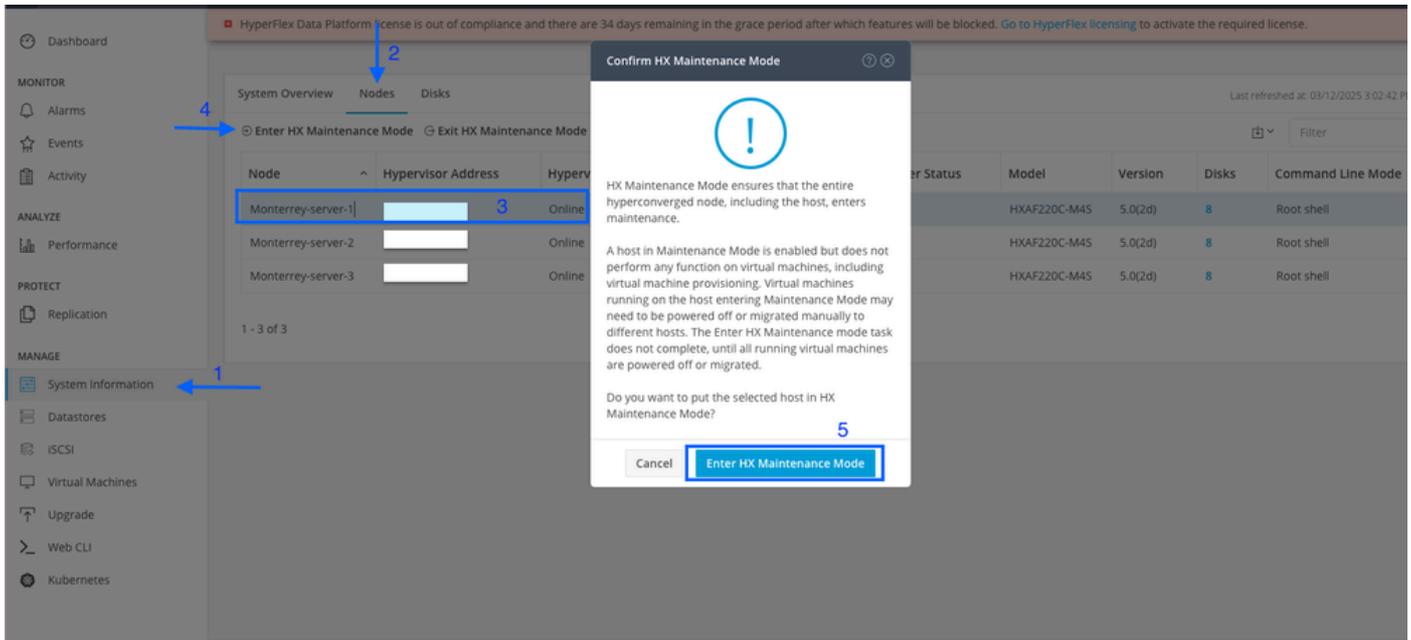
Asegúrese de que el clúster está en línea y en buen estado antes de comenzar con la actividad.

Verifique las versiones iniciales de los VIP de Hyperflex, nenic y nfnic en los nodos ESXi del clúster.

```
esxcli software vib list | egrep -i 'scvmclient|STFSNasPlugin|stHypervisorSvc|nenic|nfnic'
```

Actualizar mediante CLI

Paso 1. En HX Connect, vaya a System Information > Nodes, seleccione uno de los hosts y haga clic en Enter HX Maintenance Mode.

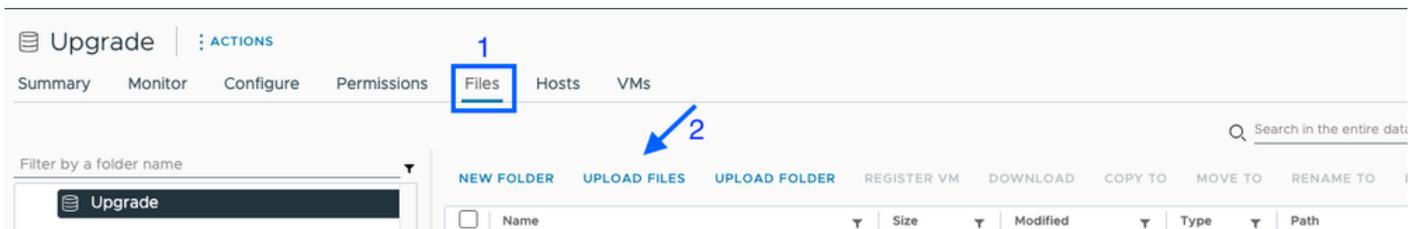


Una vez que el host entra en modo de mantenimiento, continúe con los siguientes pasos.

Paso 2. Transfiera el archivo zip al host.

Puede cargarlo mediante vCenter en un almacén de datos montado.

Navigate hasta el almacén de datos deseado y seleccione Files, luego seleccione UPLOAD FILES y cargue el archivo zip. En la siguiente imagen, se utiliza un almacén de datos llamado Upgrade.



También puede copiar de forma remota y segura el paquete de actualización de ESXI en una carpeta apropiada con espacio suficiente con SCP.

```
scp local_filename user@ESXIServer:/path/where/file/should/go
```

Paso 3. SSH al host de ESXI en modo de mantenimiento y navegue hasta la carpeta del almacén de datos donde se copia el paquete de actualización de ESXI. En este escenario, el archivo está disponible en el almacén de datos Upgrade.

```
[root@Monterrey-server-1:~]cd /vmfs/volumes/Upgrade
```

Puede verificar la versión actual con el comando `vmware -v`

```
[root@Monterrey-server-1:~] vmware -v
VMware ESXi 7.0.3 build-23794027
```

Ejecute este comando para ver los detalles del perfil del paquete: `esxcli software sources profile list -d /complete/path/VMware-ESXi...cremallera`

```
[root@Monterrey-server-1:/vmfs/volumes/2f27e295-70f773c4] esxcli software sources profile list -d /vmfs/
Name                               Vendor           Acceptance Level  Creation Time      Modification Time
-----                               -
ESXi-7.0U3s-24585291-standard      VMware, Inc.     PartnerSupported  2025-03-04T00:00:00 2025-03-04T00:00:00
ESXi-7.0U3s-24585291-no-tools      VMware, Inc.     PartnerSupported  2025-03-04T00:00:00 2025-02-21T03:24:14
```

Paso 4. Ejecute este comando para instalar el parche: `esxcli software profile update -d /complete/path/VMware-ESXi...zip -p PackageProfileName` y espere hasta que se muestre el resultado correcto.

```
root@Monterrey-server-1:/vmfs/volumes/2f27e295-70f773c4] esxcli software profile update -d /vmfs/volume
Update Result
  Message: The update completed successfully, but the system needs to be rebooted for the changes to b
  Reboot Required: true
  VIBs Installed: VMware_bootbank_bmca1_7.0.3-0.135.24585291, VMware_bootbank_cpu-microcode_7.0.3-0.13
  VIBs Removed: VMware_bootbank_bmca1_7.0.3-0.125.23794027, VMware_bootbank_cpu-microcode_7.0.3-0.125.
  VIBs Skipped: VMW_bootbank_atlantic_1.0.3.0-8vmw.703.0.20.19193900, VMW_bootbank_bnxtnet_216.0.50.0-
```

Paso 5. Una vez completada la actualización, reinicie el host de ESXi.

Paso 6. SSH en el host y verifique la versión con el comando: `vmware -v`

```
[root@Monterrey-server-1:~] vmware -v
VMware ESXi 7.0.3 build-24585291
```

Paso 7. Salga del nodo del modo de mantenimiento y espere a que el clúster funcione correctamente.

Abra HX-Connect, elija System Information> Nodes, elija el nodo en el modo de mantenimiento y haga clic en Exit HX Maintenance Mode .

Node	Hypervisor Address	Hypervisor Status	Controller Address	Controller Status	Model	Version	Disks	Command Line Mode
Monterrey-server-1		Offline		Offline	HXAF220C-M45	5.0(2d)	8	-
Monterrey-server-2		Online		Online	HXAF220C-M45	5.0(2d)	8	Root shell
Monterrey-server-3		Online		Online	HXAF220C-M45	5.0(2d)	8	Root shell

Espere unos minutos para que el clúster Hyperflex complete la recuperación. El panel de HX Connect muestra el estado operativo, debe ser Online y el estado de la resistencia debe mostrar Healthy.

También desde VCenter, asegúrese de que el servidor puede ver todos los almacenes de datos.

Repita los pasos en todos los nodos que forman parte del clúster, uno a uno.

Actualización mediante interfaz de usuario de HX Connect

Vaya a la ficha Actualizar, seleccione el tipo de actualización de ESXI y cargue el archivo de actualización de ESXI.

Nota: Si su clúster está en la versión 5.5 o 6.0 de HX, debe realizar una actualización combinada seleccionando HX Data Platform y cargando el paquete HX de su versión actual

The screenshot displays the vSphere Upgrade wizard interface. On the left, a navigation sidebar includes sections for MONITOR (Alarms, Events, Activity), ANALYZE (Performance), PROTECT (Replication), and MANAGE (System Information, Datastores, iSCSI, Virtual Machines, Upgrade, Web CLI, Kubernetes). The 'Upgrade' option is highlighted with a blue box and a '1' next to it. The main content area is titled 'Select Upgrade Type' and features a 'Progress' indicator. Under 'Select Upgrade Type', the 'HX Data Platform' option is unchecked, while 'ESXi' is checked and highlighted with a blue box, with a '2' next to it. Below this, a dashed box contains a green progress bar at 52% completion, with the text 'Current version: 7.0.3' and 'Current hypervisor details' below it. Further down, the 'UCS Server Firmware' and 'Secure Boot mode' options are unchecked. The 'vCenter Credentials' section shows the 'Username' field populated with 'administrator@esphera.local' and an empty 'Password' field. A blue 'Upgrade' button is located at the bottom right of the main content area.

Una vez cargado el archivo, introduzca las credenciales de vCenter y haga clic en Actualizar.

Select Upgrade Type Progress

HX Data Platform ⓘ

ESXi ⓘ

ESXi-7.0U3s-24585291-standard file is uploaded

Current version: 7.0.3 [Current hypervisor details](#) [Bundle details](#)

UCS Server Firmware ⓘ

Secure Boot mode ⓘ

vCenter Credentials

Username: administrator@vsphere.local Password: [masked]

[Upgrade](#)

La primera etapa consiste en validar la actualización. Si Distributed Resource Scheduler (DRS) está habilitado, las VM se trasladan automáticamente a otros hosts.

Select Upgrade Type Progress

Validating upgrade

Monterrey Warning

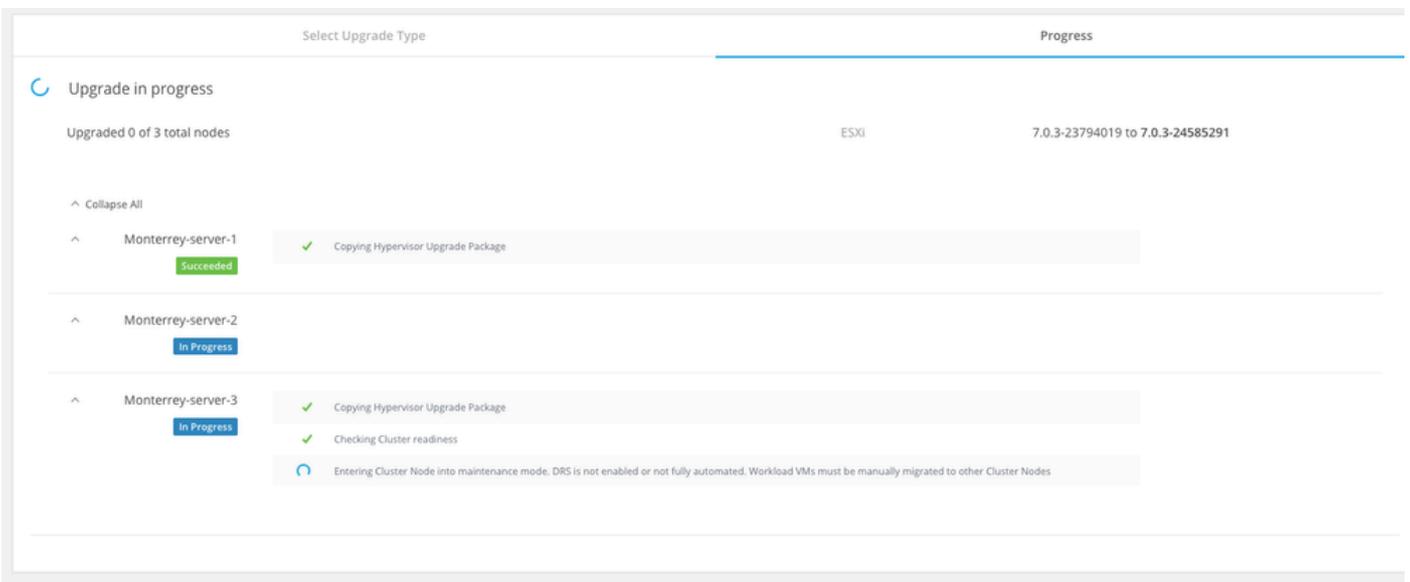
- ✓ Checking cluster state
- ✓ Checking if cluster rebalance is in progress
- ✓ Checking if all nodes are online and connected to vCenter
- ✓ Checking if all controller VMs have enough free space in root partition
- ✓ Checking if all controller VMs have disks mounted correctly
- ✓ Checking ESX Host Version on Cluster Nodes with NVMe Disks
- ✓ Validating if all nodes have same HyperFlex version.
- ✓ Querying Hypervisor bundle details during upgrade
- ✓ Checking if ESXi upgrade is required
- ⚠ Checking vCenter configuration
WARNING: The current cluster Monterrey has DRS disabled. Host evacuation will need to be performed manually through vCenter for each host during the upgrade. This process is non-disruptive as VMs are evacuated using manual vMotion tasks. Please configure DRS for a fully automated experience and retry.
- ✓ Checking ESXi nodes have enough space to upload upgrade bundle

[Cancel](#) [Retry](#) [Skip Validations](#)

Haga clic en Omitir validaciones y la actualización se iniciará automáticamente.

Supervise el proceso de actualización.

Nota: Si DRS está desactivado, vMotion envía las VM manualmente para continuar el proceso de actualización.



The screenshot shows the vSphere Upgrade Progress page. The page is divided into two tabs: "Select Upgrade Type" and "Progress". The "Progress" tab is active, showing the upgrade status for three nodes: Monterrey-server-1, Monterrey-server-2, and Monterrey-server-3. The upgrade is for ESXi version 7.0.3-23794019 to 7.0.3-24585291. Monterrey-server-1 is "Succeeded", Monterrey-server-2 is "In Progress", and Monterrey-server-3 is "In Progress".

Node Name	Status	Progress Details
Monterrey-server-1	Succeeded	Copying Hypervisor Upgrade Package
Monterrey-server-2	In Progress	
Monterrey-server-3	In Progress	Copying Hypervisor Upgrade Package Checking Cluster readiness Entering Cluster Node into maintenance mode. DRS is not enabled or not fully automated. Workload VMs must be manually migrated to other Cluster Nodes

Espere hasta que se complete la actualización en todos los nodos del clúster.

UPGRADE STATUS

Success

Upgraded on 03/12/2025 2:48:30 PM [View Activity for details](#)

UPGRADE VERSION

ESXi

7.0.3-23794019 to 7.0.3-24585291

X

CLUSTER UPGRADE ELIGIBILITY

Verificación

Puede verificar la versión instalada de ESXI desde HX Connect en la pestaña Información del sistema.

MONITOR

- Alarms
- Events
- Activity

ANALYZE

- Performance

PROTECT

- Replication

MANAGE

- System Information
- Datastores
- iSCSI
- Virtual Machines
- Upgrade
- Web CLI
- Kubernetes

Monterrey ONLINE

License Type: Reserved

License Status:

vCenter:

Uptime: 194 days, 23 hours, 21 minutes, 8 seconds

Hypervisor: 7.0.3-24585291

HXDP Version: 5.0.2d-42558

Total Capacity:

Available Capacity:

Data Replication Factor:

Hyperconverged Nodes

Node	Hypervisor	HyperFlex Controller	Disk Overview (7 in use)
Monterrey-server-1 HXAF220C-M4S	Online 7.0.3-24585291	Online 5.0.2d-42558	
Monterrey-server-2 HXAF220C-M4S	Online 7.0.3-24585291	Online 5.0.2d-42558	
Monterrey-server-3 HXAF220C-M4S	Online 7.0.3-24585291	Online 5.0.2d-42558	

Desde vCenter puede ver la versión de ESXI en el Resumen del servidor.

10.0.20.100 | ACTIONS

Summary Monitor Configure Permissions VMs Datastores

Host Details



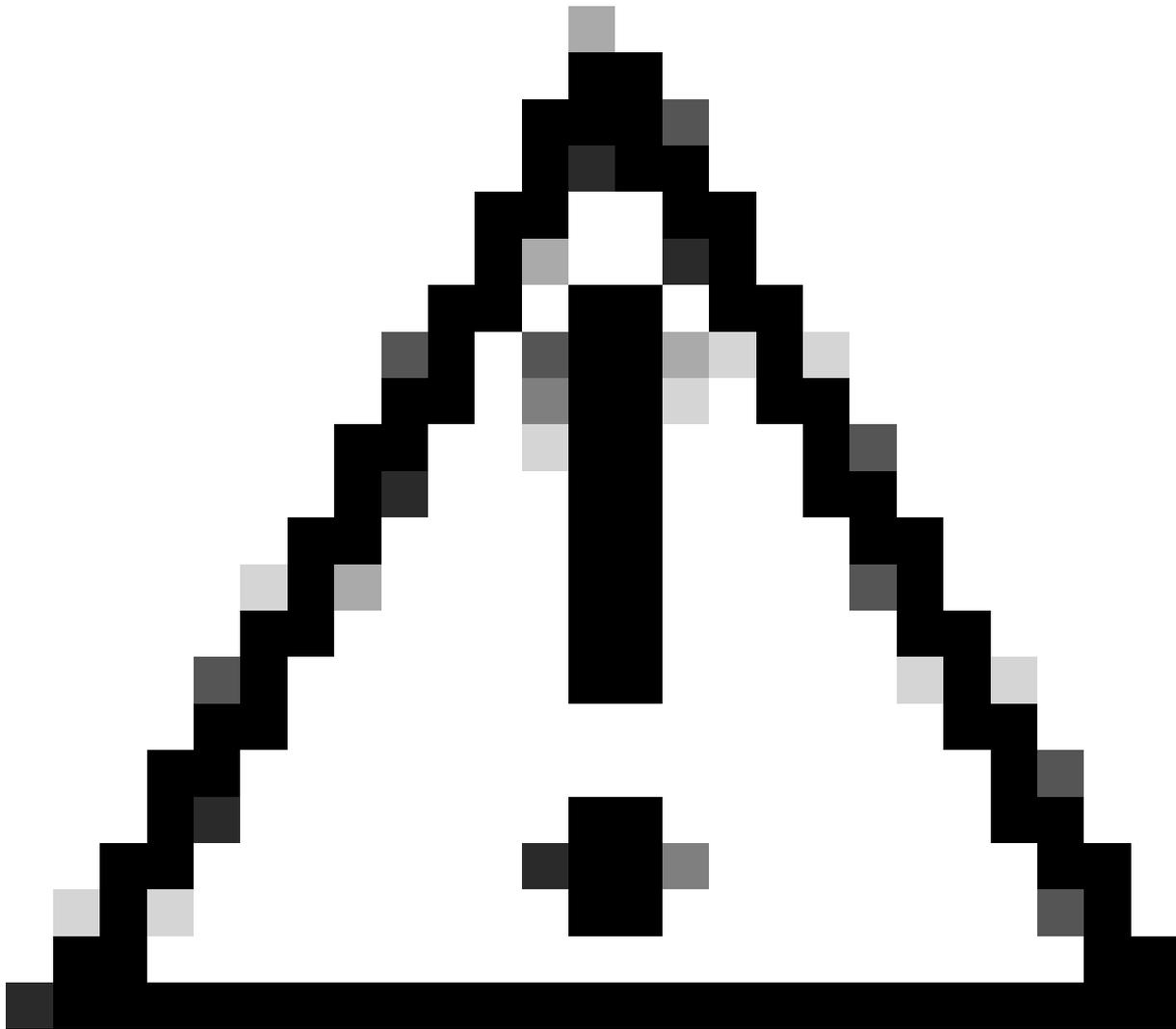
Hypervisor:	VMware ESXi, 7.0.3, 24585291
Model:	HXAF220C-M4S
Processor Type:	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz
Logical Processors:	48
NICs:	8
Virtual Machines:	7
State:	Connected
Uptime:	22 hours

Dado que la imagen de ESXI no es personalizada, debe confirmar que los VIP de Hyperflex aún se muestran intactos en los servidores.

SSH en cada host de ESXI después de que se haya completado el parche y antes de comenzar con el siguiente nodo y verifique los VIP de Hyperflex con el comando: `esxcli software vib list | egrep -i 'scvmclient|STFSNasPlugin|stHypervisorSvc'`

Nota: En las versiones ESXi 7.0 U3, vmware-esx-STFSNasPlugin cambió a CIS-ESX-STFSNasPlugin
En las versiones ESXi 8.0 U1, stHypervisorSvc cambió a sthypervisorsvc.

```
[root@Monterrey-server-1:~] esxcli software vib list | egrep -i 'scvmclient|STFSNasPlugin|stHypervisorS
CIS-ESX-STFSNasPlugin      4.5.1-11                CIS      VMwareAccepted  2023-10
scvmclient                  5.5.1-38                CIS      VMwareAccepted  2023-11
stHypervisorSvc            4.5.1-11                CIS      VMwareAccepted  2023-10
```



Precaución: En ciertos escenarios, la imagen no personalizada puede sobrescribir los VIB nenic y nfnic con una versión diferente a las de la imagen personalizada. Debe validar que tenemos las versiones correctas después del parche.

SSH en cada host de ESXI después de que se haya completado el parche y antes de comenzar con el siguiente nodo y verifique los VIP de Hyperflex con el comando: `esxcli software vib list | egrep -i 'nenic|nfnic'`

```
[root@Monterrey-server-3:~] esxcli software vib list | egrep -i 'nenic|nfnic'
```

nfnic	5.0.0.43-10EM.700.1.0.15843807	CIS	VMwareCertified	2025-02
nenic-ens	1.0.6.0-10EM.700.1.0.15843807	Cisco	VMwareCertified	2023-10
nenic	2.0.10.0-10EM.700.1.0.15843807	Cisco	VMwareCertified	2024-03

Troubleshoot

Si nenic o nfnic se sobrescribieron con una versión diferente, puede instalar las correctas descargando una imagen zip personalizada de ESXI de su misma versión de software.cisco.com. Descomprima la imagen a y desde el directorio vib busque los directorios nenic y nfnic. Extraiga el archivo vib y cárguelo a través de vCenter en un almacén de datos montado en los servidores. Asegúrese de que el clúster está en línea y en buen estado.

Paso 1. En HX Connect, vaya a System Information > Nodes, seleccione uno de los hosts y haga clic en Enter HX Maintenance Mode.

Una vez que el host entra en modo de mantenimiento, continúe con los siguientes pasos.

SSH al host ESXI en modo de mantenimiento y navegue hasta la carpeta del almacén de datos donde se copia el archivo vib de ESXI. En esta situación, el archivo está disponible en el almacén de datos de actualización

```
[root@Monterrey-server-3:~] cd /vmfs/volumes/Upgrade
```

```
[root@Monterrey-server-3:/vmfs/volumes/2f27e295-70f773c4] ls  
CIS_bootbank_nenic_2.0.10.0-10EM.700.1.0.15843807.vib
```

Ejecute este comando para actualizar el vib: `esxcli software vib update -v "/complete/path/vib-file.vib" -f`

```
[root@Monterrey-server-3:/vmfs/volumes/2f27e295-70f773c4] esxcli software vib update -v "/vmfs/volumes/  
Installation Result  
  Message: The update completed successfully, but the system needs to be rebooted for the changes to b  
  Reboot Required: true  
  VIBs Installed: CIS_bootbank_nenic_2.0.10.0-10EM.700.1.0.15843807  
  VIBs Removed: Cisco_bootbank_nenic_1.0.45.0-10EM.700.1.0.15843807  
  VIBs Skipped:
```

Una vez completada la actualización de vib, reinicie el host de ESXi.

SSH en el host y verifique que vib se haya actualizado correctamente con el comando: `esxcli software vib list | egrep -i 'nenic|nfnic'`

Salga del nodo del modo de mantenimiento y espere a que el clúster funcione correctamente.

Abra HX-Connect, elija System Information> Nodes, elija el nodo en el modo de mantenimiento y haga clic en Exit HX Maintenance Mode .

Si el servidor arranca desde la tarjeta SD, puede encontrarse con un problema conocido mientras aplica el parche. "No se puede remediar el host debido a un error mientras se esperaba el proceso untar". Este problema se produce cuando la operación untar de VIB individuales tarda más del tiempo de espera predeterminado de 30 segundos durante el proceso de remediación.

Para los entornos que utilizan la tarjeta SD como la partición OSData, hay posibilidades de que el proceso de desactivación de las herramientas VMware tome una duración ligeramente mayor. Puede consultar [este artículo](#) para resolverlo.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).