Upgrading the Cisco Nexus Fabric Manager Software

This chapter describes how to upgrade the Cisco Nexus Fabric Manager software. It contains the following sections:

Before You Begin

If you are upgrading the Cisco Nexus Fabric Manager from 1.1(x) to 1.2(3), you must complete all three of the following steps:

- Upgrading the Cisco Nexus Fabric Manager, on page 2.
- Upgrading the Firmware on a Cisco Nexus Fabric Manager Appliance Using the Host Upgrade Utility, on page 4.
- Updating the ESXi LSI MegaRAID SAS Controller, on page 7.

If you are upgrading the Cisco Nexus Fabric Manager from 1.2(x) to 1.2(3) you only need to complete the first step in this guide:

- Upgrading the Cisco Nexus Fabric Manager, on page 2.

Guidelines and Limitations

Before attempting to upgrade the software image, follow these guidelines:

Note Administrators should always review the Release Notes of the new Cisco Nexus Fabric Manager image before upgrading. Release Notes for the Cisco Nexus Fabric Manager can be found at http://www.cisco.com/c/en/us/support/cloud-systems-management/nexus-fabric-manager/products-release-notes-list.html.

Note Upgrading should not be attempted if there is a previously created VRF named "default" in the Cisco Nexus Fabric Manager. In this case, the VRF must be renamed prior to performing the upgrade. Instructions for editing a VRF can be found in the Cisco Nexus Fabric Manager Configuration Guide.

- In the Cisco Nexus Fabric Manager, Release 1.2.x, we have changed the default interface role of a port channel connected to a foreign switch from “switch facing” to “border.” The Cisco Nexus Fabric Manager updates the role of the port channel members correctly, but does not update the role of the port channel itself. If you encounter this specific situation after upgrading, the workaround is to rebuild the port channel by selecting the specific port channel tiles under the **Interfaces** tab and click the **REBUILD** button in the Summary pane.
- Restoring statistics (switch, interfaces, logical port channel, broadcast domains) is not supported. All statistics within the Cisco Nexus Fabric Manager running Release 1.1.x are lost when the software is upgraded to Cisco Nexus Fabric Manager, Release 1.2.x.

Upgrading the Cisco Nexus Fabric Manager

Note To avoid an upgrade script failure due to Unicode translation on a Mac OS, it is recommended that you enter the commands in the terminal window rather than copy-and-paste them from this document.

Before You Begin

1. Download the bundle file from the Cisco Nexus Fabric Manager Download Software page. Make a note of the MD5 checksum.
2. Save the file on a server accessible from the Cisco Nexus Fabric Manager virtual machine.

Step 1 Perform a Cisco Nexus Fabric Manager backup.

a) Log into the Cisco Nexus Fabric Manager UI with your UI credentials.
b) Click **Menu**.
c) Click **System**.
d) Click the **Download** button under **BACKUP & RESTORE** .

Step 2 Export the Cisco Nexus Fabric Manager virtual appliance as an OVA.

a) Log in to the Cisco Nexus Fabric Manager appliance and the vSphere Client.
b) In the **vSphere Client** window, right-click the Cisco Nexus Fabric Manager virtual machine.
c) Choose **Power > Shut Down Guest**.

Wait until the Cisco Nexus Fabric Manager virtual machine is powered off. This is indicated by the green triangle icon to the left of the Cisco Nexus Fabric Manager virtual machine disappearing with only three squares remaining.

d) Choose **File > Export > Export OVF template**.

e) In the **Export OVF Template** window, enter the following information:

- If you prefer, you can change the name in the **Name** field from the default value of the virtual machine name.
- Browse to the directory path where the files is to be saved.
- From the **Format** drop-down list, choose **Single file (OVA)**.

f) In the **vSphere Client** window, right-click the Cisco Nexus Fabric Manager virtual machine.

g) Choose **Power > Power On**.

Step 3 Copy the upgrade bundle file to the Cisco Nexus Fabric Manager VM.

a) In the **vSphere Client** window, right-click the Cisco Nexus Fabric Manager virtual machine.

b) Choose **Open Console**.

c) In the **Console** window, log in with your root credentials.

d) Ensure that the Cisco Nexus Fabric Manager has a route to the remote server where the upgrade bundle is located. .

Example:
To verify connectivity to the remote server enter the **ping** command.

```
# ping 209.165.200.230
```

e) Copy the bundle and the checksum files to the Cisco Nexus Fabric Manager virtual machine using a transfer protocol. You can use SCP, FTP, or HTTP.

Example:

```
# scp username@209.165.200.230:/path/to/nfm-1.3.1.bundle .
```

Note Do not exclude the period at the end of the command.

f) Calculate the checksum of the bundle file by entering the following command:

```
# md5sum nfm-1.3.1.bundle
```

g) Compare the calculated checksum value displayed on the screen with the one from the Cisco Nexus Fabric Manager Download Software page.

Note If they do not match, the bundle file is corrupted and must be downloaded again. Do not proceed with the upgrade if the bundle file is corrupted.

Step 4 Perform the upgrade.

a) In the **Console** window, start the bundle upgrade by entering the following command:

```
# bash +x ./nfm-1.3.1.bundle -u
```

Note The upgrade takes a few minutes to complete. During this time the Cisco Nexus Fabric Manager UI is not functional.

If the following messages are displayed, the upgrade was successful.

```
Self Extracting...done

Installing...done
```

If the following messages are displayed, the upgrade failed. Contact the Technical Assistance Center (TAC).

```
Self Extracting...done

Installing...failed. Check /var/log/esmOVA-install.log and/or /var/log/upgrade.log
```

Note The 1.3(1) and 1.2(3) releases involve a kernel update. You must reboot the Cisco Nexus Fabric Manager VM to load the new kernel. The reboot can be run from the same command line where the **upgrade** command was entered. The command is **shutdown -r now**.

b) When the upgrade completes successfully, close and reopen your browser and clear the browser cache.
c) Log in to the Cisco Nexus Fabric Manager UI with your UI credentials.
d) Click the drop-down arrow next to your username, click **About** and verify the running Cisco Nexus Fabric Manager version.

Step 5 Save a new Cisco Nexus Fabric Manager backup.

a) Log in to the Cisco Nexus Fabric Manager UI with your UI credentials.
b) Click **Menu**.
c) Click **System**.
d) Click the **Download** button under **BACKUP & RESTORE** .

Upgrading the Firmware on a Cisco Nexus Fabric Manager Appliance Using the Host Upgrade Utility

The following procedure describes upgrading the firmware on the Cisco Nexus Fabric Manager appliance. This procedure is the same as the procedure used for Cisco UCS C-Series Servers.

Step 1 Download the Host Upgrade Utility (HUU) ISO file.

a) Navigate to the following URL: http://www.cisco.com/cisco/software/navigator.html
b) In the center column of the **Downloads Home** pane, choose **Servers – Unified Computing**.
c) In the right-hand column, choose **UCS C-Series Rack-Mount Standalone Server Software**.
d) In the right-hand column, choose **UCS C220-M4 Rack Server Software**.
e) In the **Select a Software Type** window, choose **Unified Computing System (UCS) Server Firmware**.
f) In the left-hand column, expand **All Releases**, expand **2.0**, and choose 2.0(10f).
g) Click **Download** to download the `ucs-c220m4-huu-2.0.10f.iso` file.
h) In the **End User License Agreement** dialog box, click **Accept License Agreement**.

The download begins.

Step 2 Prepare the ISO for a remote upgrade using the KVM Console.

a) Use a browser to connect to the Cisco Integrated Management Controller (CIMC) GUI software on the Cisco Nexus Fabric Manager appliance server that you are upgrading.
Both Adobe Flash and Java are needed for this operation. Verify that your browser supports both.

b) In the **Address** field of the browser, enter the CIMC IP address for the Cisco Nexus Fabric Manager appliance and enter your username and password.

c) Click **Launch KVM Console** on the toolbar to launch the KVM Console.

d) In the **Cisco Virtual KVM Console** menu bar, click **Virtual Media > Activate Virtual Devices** and click **Accept** if prompted.

e) In the **Virtual Media - Map CD/DVD** dialog box, browse to the `ucs-c220m4-huu-2.0.10f.iso` file.

f) Click **Map Device**.

g) In the **Virtual Media** pane, verify that the `ucs-c220m4-huu-2.0.10f.iso` file is checked.
Wait for mapping to complete.

After the ISO file appears as a mapped remote device, continue to Step 3.

Step 3 Gracefully shut down the Cisco Nexus Fabric Manager appliance and the vSphere Client.

a) Log in to the Cisco Nexus Fabric Manager appliance and the vSphere Client.

b) In the vSphere Client window, right-click the Cisco Nexus Fabric Manager virtual machine.

c) Choose **Power > Shut Down Guest** .
Wait until the Cisco Nexus Fabric Manager virtual machine is powered off. This is indicated by the green triangle icon to the left of the Cisco Nexus Fabric Manager virtual machine disappearing with only three squares remaining.

Step 4 Return to the CIMC browser window and power cycle the Cisco Nexus Fabric Manager appliance.

a) In the **CIMC** window, click the **Power Cycle Server** button.

b) In the **KVM** window, continuously press the **F6** key when prompted, to open the **Boot Menu** screen.

c) In the **Boot Menu** screen, choose **Cisco vKVM-Mapped vDVD1.22** and press **Enter**.

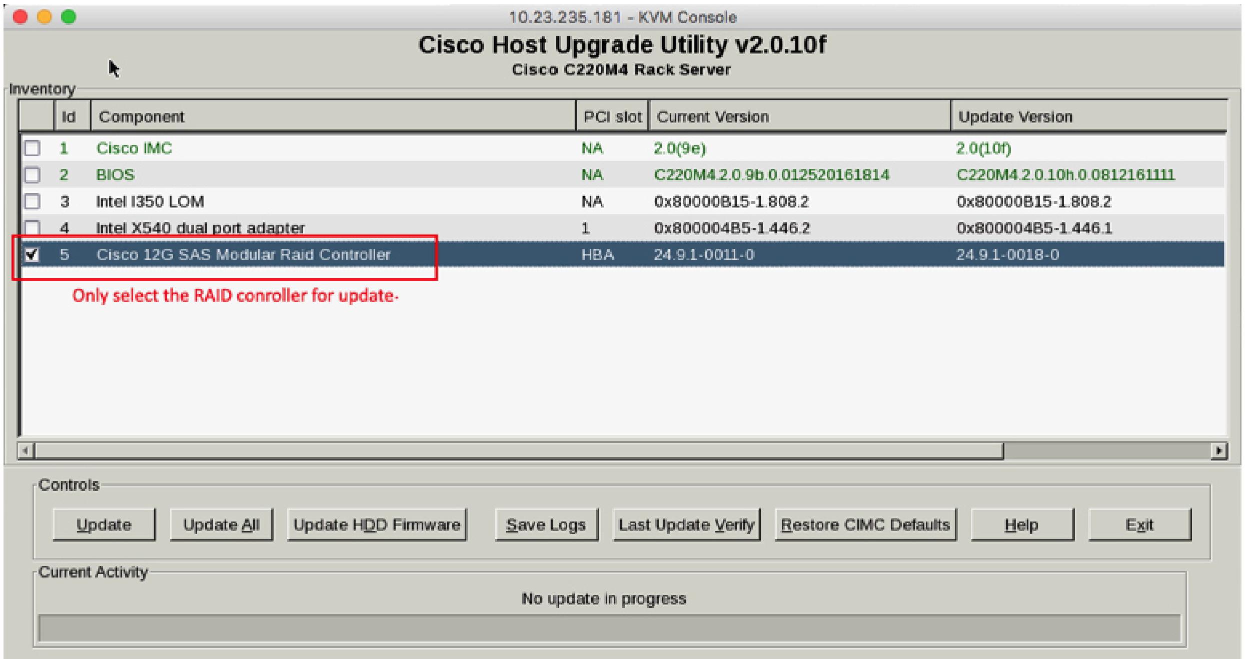
Note If you are prompted to dismount a drive, click **No**, and continue.

The CIMC HUU can take some time to load, discover, and update.

Step 5 Read the Cisco End User License Agreement (EULA) and click **I agree** after the HUU boots.
After you accept the EULA, the **Cisco Host Upgrade Utility** window appears with a list of all the components that are available for update.

Step 6 Check the **Cisco 12G SAS modular RAID Controller** check box.

Note Do not select any other options for upgrade – only the **Cisco 12G SAS RAID Controller**.



10.23.235.181 - KVM Console

Cisco Host Upgrade Utility v2.0.10f

Cisco C220M4 Rack Server

Inventory

	Id	Component	PCI slot	Current Version	Update Version
☐	1	Cisco IMC	NA	2.0(9e)	2.0(10f)
☐	2	BIOS	NA	C220M4.2.0.9b.0.012520161814	C220M4.2.0.10h.0.0812161111
☐	3	Intel I350 LOM	NA	0x80000B15-1.808.2	0x80000B15-1.808.2
☐	4	Intel X540 dual port adapter	1	0x800004B5-1.446.2	0x800004B5-1.446.1
☑	5	Cisco 12G SAS Modular Raid Controller	HBA	24.9.1-0011-0	24.9.1-0018-0

Only select the RAID conroller for update.

Current Activity

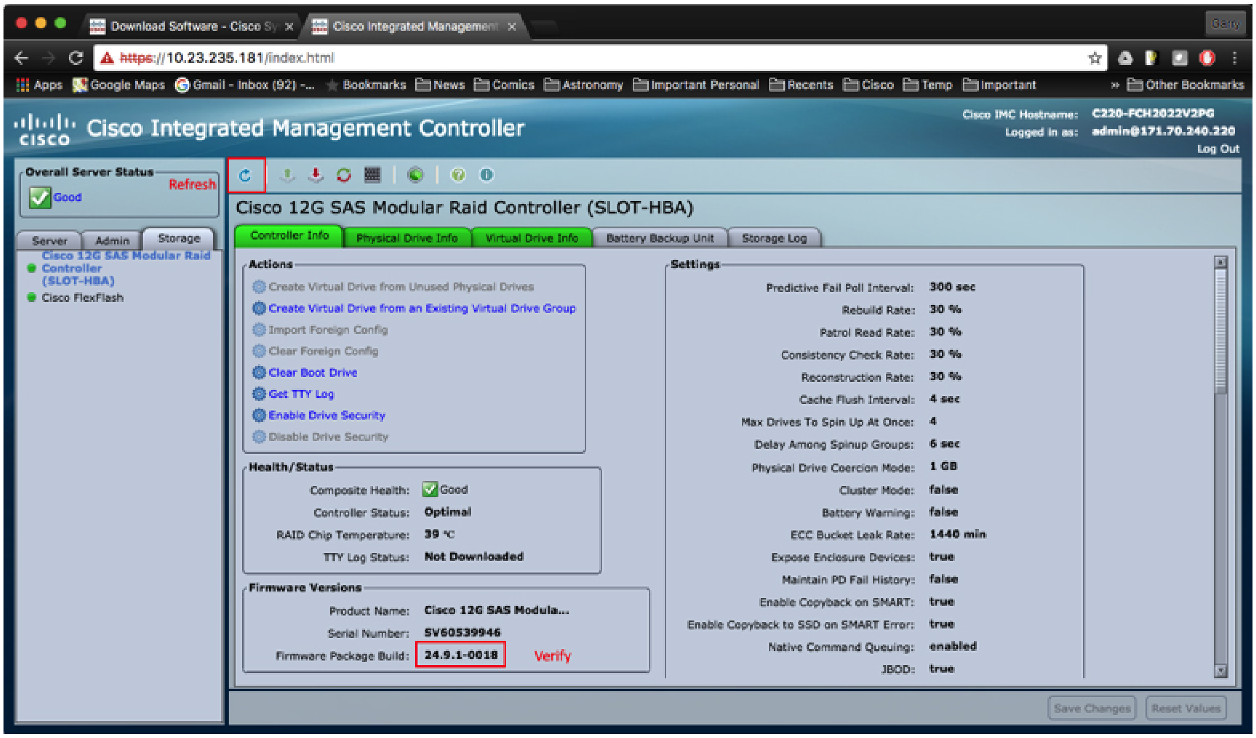
No update in progress

Step 7 Click **Update**.
This initiates the update and the status of the update is displayed in the **Update Status** column. You can also view a more detailed log of a series of activities and statuses that are involved while updating the firmware in the **Execution Logs** section.

Step 8 Click **Exit**.
This reboots the appliance, loading the updated version of the RAID controller.

Step 9 After the appliance reboots, return to the CIMC browser to verify that the correct firmware version is loaded.

a) Click the **Refresh** icon.
b) Click the **Storage** tab.
c) Click the **Controller Info** tab.
d) In the **Firmware Versions** pane, verify that the **Product Name** is Cisco 12G SAS Modular RAID controller and the **Firmware Package Build** is version 24.9.1-0018.



Cisco IMC Hostname: C220-FCH2022V2PG
Logged in as: admin@171.70.240.220

Cisco 12G SAS Modular Raid Controller (SLOT-HBA)

Health/Status

Composite Health: Good
Controller Status: Optimal
RAID Chip Temperature: 39 °C
TTY Log Status: Not Downloaded

Firmware Versions

Product Name: Cisco 12G SAS Modula...
Serial Number: SV60539946
Firmware Package Build: 24.9.1-0018

Settings

Predictive Fail Poll Interval: 300 sec
Rebuild Rate: 30 %
Patrol Read Rate: 30 %
Consistency Check Rate: 30 %
Reconstruction Rate: 30 %
Cache Flush Interval: 4 sec
Max Drives To Spin Up At Once: 4
Delay Among Spinup Groups: 6 sec
Physical Drive Coercion Mode: 1 GB
Cluster Mode: false
Battery Warning: false
ECC Bucket Leak Rate: 1440 min
Expose Enclosure Devices: true
Maintain PD Fail History: false
Enable Copyback on SMART: true
Enable Copyback to SSD on SMART Error: true
Native Command Queuing: enabled
JBOD: true

Updating the ESXi LSI MegaRAID SAS Controller

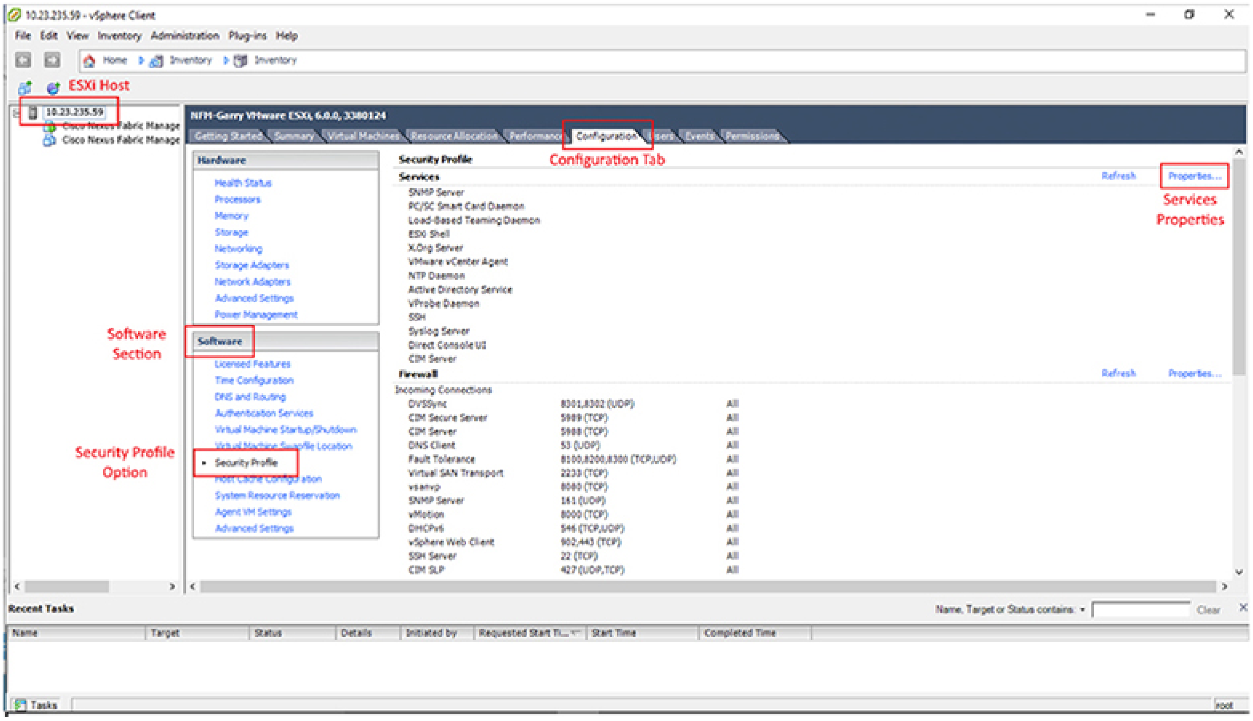
Before You Begin

You must have upgraded the firmware on the Cisco Nexus Fabric Manager appliance.

Step 1 Enable SSH on the ESXi hypervisor.

a) Open the VMware vSphere client.
If VMware vSphere is not already installed, you can download VMware vSphere from https://my.vmware.com/en/web/vmware/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/6_0

b) Choose the ESXi host in the **vSphere Client** window as seen in the following figure.



Security Profile

Services

SNMP Server
PC/SC Smart Card Daemon
Load-Based Teaming Daemon
ESXi Shell
X.Org Server
VMware vCenter Agent
NTP Daemon
Active Directory Service
VProbe Daemon
SSH
Syslog Server
Direct Console UI
CIM Server

Firewall

Incoming Connections

DVSSync	8301,8302 (UDP)	All
CIM Secure Server	5989 (TCP)	All
CIM Server	5988 (TCP)	All
DNS Client	53 (UDP)	All
Fault Tolerance	8100,8200,8300 (TCP,UDP)	All
Virtual SAN Transport	2233 (TCP)	All
vsanvp	8080 (TCP)	All
SNMP Server	161 (UDP)	All
vMotion	8000 (TCP)	All
DHCPv6	546 (TCP,UDP)	All
vSphere Web Client	902,443 (TCP)	All
SSH Server	22 (TCP)	All
CIM SLP	427 (UDP,TCP)	All

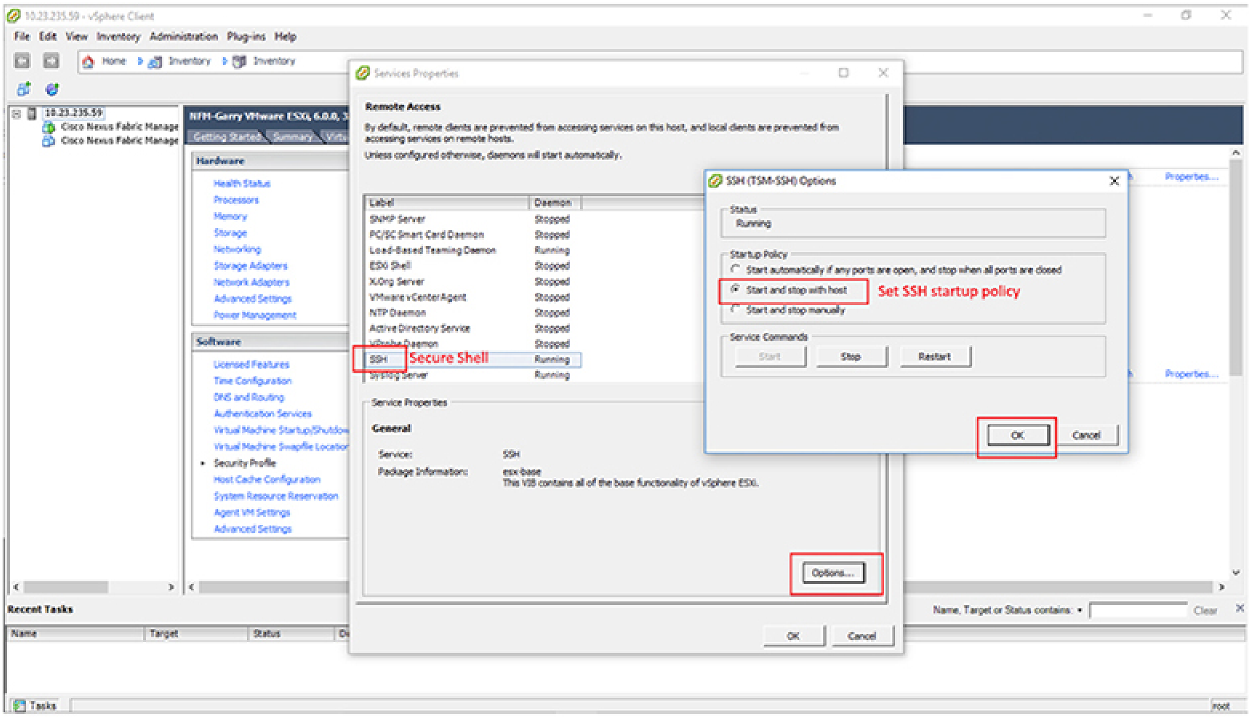
Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time

c) Click the **Configuration** tab.

d) In the **Software** area, choose **Security Profile**.

e) In the **Services** area, choose **Properties**.

f) In the **Services Properties** window, choose SSH and click the **Options** button.



Services Properties

Remote Access

By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.

Unless configured otherwise, daemons will start automatically.

Label	Daemon
SNMP Server	Stopped
PC/SC Smart Card Daemon	Stopped
Load-Based Teaming Daemon	Running
ESXi Shell	Stopped
X.Org Server	Stopped
VMware vCenterAgent	Stopped
NTP Daemon	Stopped
Active Directory Service	Stopped
vSphere Daemon	Stopped
SSH	Running
Syslog Server	Running

Service Properties

General

Service: SSH

Package Information: esx-base
This VIB contains all of the base functionality of vSphere ESXi.

Options... OK Cancel

SSH (TSM-SSH) Options

Status: Running

Startup Policy
- ○ Start automatically if any ports are open, and stop when all ports are closed
- ● Start and stop with host
- ○ Start and stop manually

Service Commands: Start Stop Restart

OK Cancel

g) In the **SSH (TSM-SSH) Options** window, in the **Service Commands** area, click **Start**.

h) Click the **Start and stop with host** radio button.

i) Click **OK**.

j) Click **OK**.

Step 2 Open a terminal window and SSH into the VMware ESXi hypervisor via its IP address.

For example:

```
ssh root@ ESXi_IP_address
```

Step 3 Enter the following command to confirm if you are already using the correct driver.

Note If the driver version is greater than or equal to 6.608.12.00-1OEM.600.0.0.2768847, you are updated. There is no need to continue.

```
[root@localhost:~] esxcli software vib list | grep "^lsi-mr3"
lsi-mr3 6.608.12.00-1OEM.600.0.0.2768847 Avago VMwareCertified 2016-09-20
```

Step 4 Otherwise, download updated lsi-mr3 ESXi 6.0 drivers for the LSI MegaRAID SAS controllers from this location: https://my.vmware.com/web/vmware/details?downloadGroup=DT-ESX60-LSI-LSI-MR3-66081200-1OEM&productId=491

Step 5 Extract the driver file from the `.zip` file and upload it to the host in the root (/) folder using the **scp** command.

Example:

To copy from a local host to the ESXi hypervisor, enter the following command:

```
scp /Users/user/folder_the_file_resides_in/lsi-mr3-6.608.12.00-1OEM.600.0.0.2768847.x86_64.vib
root@ESXi_IP_address:/
```

Step 6 Enter the following command to install the driver.

```
[root@localhost:~] esxcli software vib install -v "/lsi-mr3-6.608.12.00-1OEM.600.0.0.2768847.x86_64.vib"
 --maintenance-mode
```

Step 7 Gracefully shut down the Cisco Nexus Fabric Manager virtual appliance and the vSphere Client.

a) Log in to the Cisco Nexus Fabric Manager appliance and the vSphere Client.
b) In the **vSphere Client** window, right-click the Cisco Nexus Fabric Manager virtual machine.
c) Choose **Power > Shut Down Guest**.
Wait until the Cisco Nexus Fabric Manager virtual machine is powered off. This is indicated by the green triangle icon to the left of the Cisco Nexus Fabric Manager virtual machine disappearing with only three squares remaining.

Step 8 Reboot the host from the VMware vSphere client.

Note The host does not need to be put into maintenance mode. Enter LSI driver update in the **Reason** section.

Step 9 After reboot, SSH into the VMware ESXi hypervisor via its IP address.

```
ex. ssh root@ESXi_IP_address
```

Step 10 Enter the following command to confirm that you have updated the correct driver.

```
[root@localhost:~] esxcli software vib list | grep "^lsi-mr3"
lsi-mr3 6.608.12.00-1OEM.600.0.0.2768847 Avago VMwareCertified 2016-09-20
```