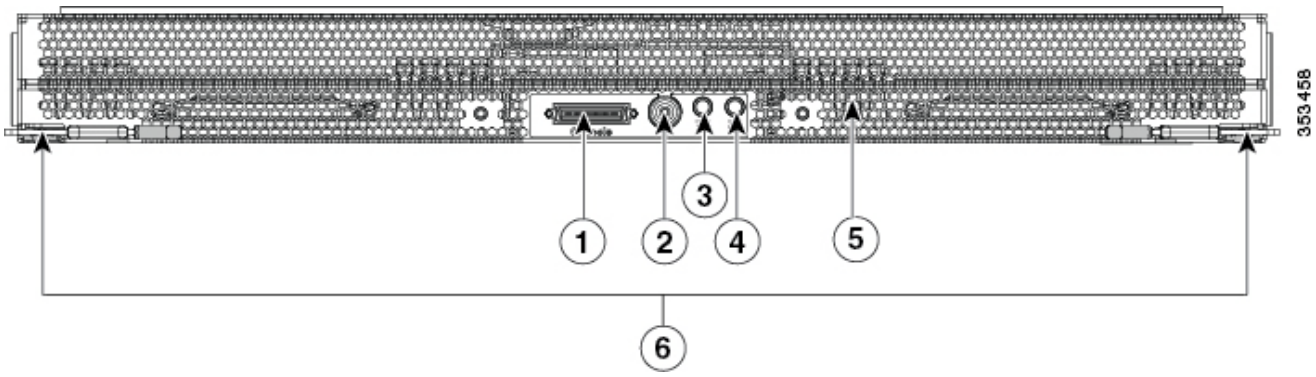
Cisco UCS C3X60 M3 Server Node For Cisco UCS S3260 Storage Server Service Note

This document covers server node installation and replacement of internal server node components.

Cisco UCS C3X60 M3 Server Node Overview

External Features

Figure 1 Cisco UCS C3X60 M3 Server Node Rear-Panel Features



1	KVM cable connector	4	Unit identification button/LED
2	Reset button	5	Server node health LED (behind mesh on server node board)
3	Server node power button/power status LED	6	Ejector levers (two)

External LEDs

Table 1 Cisco UCS C3X60 M3 Server Node External LEDs

LED	Definition of States
Server node power	■ Off—There is no AC power to the server node. ■ Amber—The server node is in standby power mode. Power is supplied only to the Cisco IMC. ■ Green—The server node is in main power mode. Power is supplied to all server node components.
Unit identification	■ Off—The Identification LED is not in use. ■ Blue, blinking—The Identification LED is activated.
Server node health LED	■ Green—The server node is operating normally. ■ Green, blinking—The server is in standby mode or sleep state. ■ Amber—The server node is in a degraded condition. Degraded condition is defined as one or more of the following: — Power supply redundancy lost (power supply unplugged or failed) — SIOC redundancy lost — Faulty or mismatched CPUs — DIMM failure — Failed drive in a RAID configuration ■ Amber, blinking—The server node is in a critical condition. Critical condition is defined as the following: — Boot failure — Fatal CPU and/or bus errors detected — Fatal uncorrectable memory error detected — Both SIOCs failed — Both drives in a RAID configuration failed — Excessive thermal conditions

KVM Cable Connector

This connector allows you to connect a local keyboard, video, and mouse (KVM) cable if you want to perform setup and management tasks locally rather than remotely.

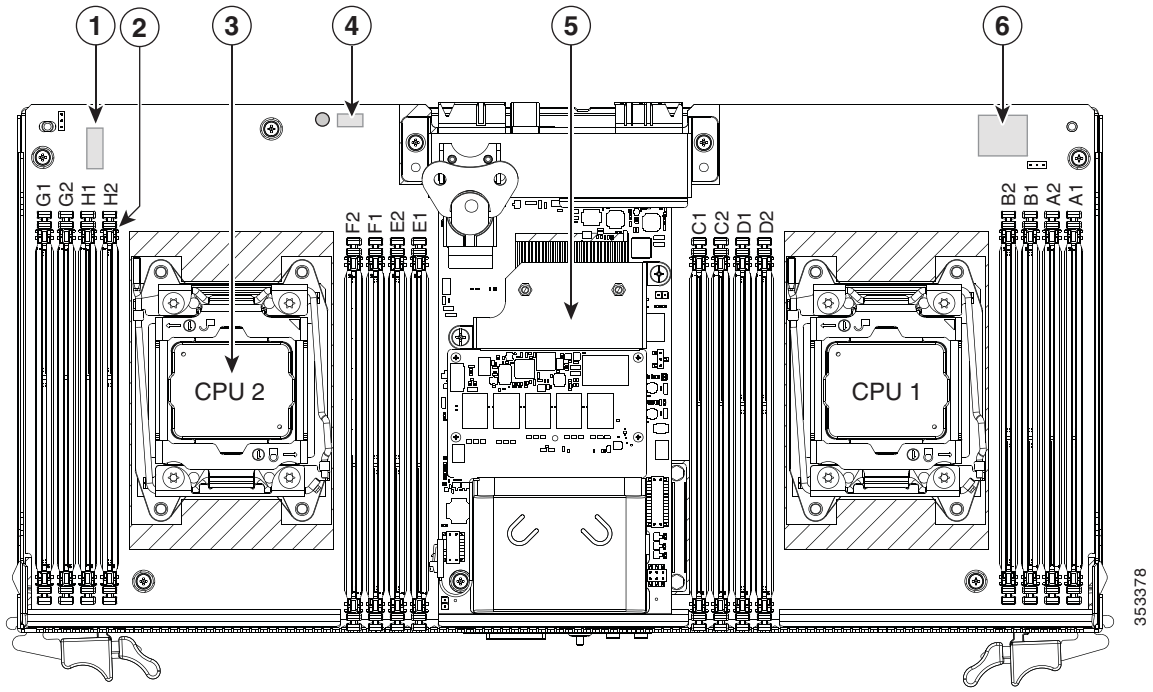
Buttons

- Reset button—You can hold this button down for 5 seconds and then release it to restart the server node controller chipset if other methods of restarting do not work.
- Server node power button/LED—You can press this button to put the server node in a standby power state or return it to full power instead of shutting down the entire system. See also External LEDs, page 2.

- Unit identification button/LED—This LED can be activated by pressing the button or by activating it from the software interface. This aids locating a specific server node. See also External LEDs, page 2.

Internal Component Locations

Figure 2 Cisco UCS C3X60 M3 Server Node Internal Components



1	RTC battery (CR2032)	4	Trusted platform module (TPM) socket
2	DIMMs (8 sockets for each CPU, 16 total)	5	Cisco modular RAID controller card with SuperCap power module (backup) attached
3	CPUs and heat sinks (two)	6	Internal USB port for USB thumb-drive

Removing or Installing a C3X60 M3 Server Node

Shutting Down a C3X60 M3 Server Node

You can invoke a graceful shutdown or a hard shutdown of a server node by using either the Cisco Integrated Management Controller (Cisco IMC) interface, or the power button that is on the face of the server node.

Shutting Down a Server Node By Using the Cisco IMC GUI

To use the Cisco IMC GUI to shut down the server node, follow these steps:

1. Use a browser and the management IP address of the system to log in to the Cisco IMC GUI.
2. In the **Navigation** pane, click the **Chassis** menu.
3. In the **Chassis** menu, click **Summary**.
4. In the toolbar above the work pane, click the **Host Power** link.

   The Server Power Management dialog opens. This dialog lists all servers that are present in the system.
5. In the **Server Power Management** dialog, select one of the following buttons for the server that you want to shut down:

CAUTION: To avoid data loss or damage to your operating system, you should always invoke a graceful shutdown of the operating system. Do not power off a server if any firmware or BIOS updates are in progress.

- Shut Down—Performs a graceful shutdown of the operating system.
- Power Off—Powers off the chosen server, even if tasks are running on that server.

It is safe to remove the server node from the chassis when the Chassis Status pane shows the Power State as Off for the server node that you are removing.

The physical power button on the server node face also turns amber when it is safe to remove the server node from the chassis.

Shutting Down a Server Node By Using the Power Button on the Server Node

To use the physical server node power button to shut down a server node, follow these steps:

1. Check the color of the server node power status LED (see Figure 1):

- Green—The server node is powered on. Go to step 2.
- Amber—the server node is powered off. It is safe to remove the server node from the chassis.

2. Invoke either a graceful shutdown or a hard shutdown:

CAUTION: To avoid data loss or damage to your operating system, you should always invoke a graceful shutdown of the operating system. Do not power off a server if any firmware or BIOS updates are in progress.

- Graceful shutdown—Press and release the **Power** button. The software performs a graceful shutdown of the server node.
- Emergency shutdown—Press and hold the **Power** button for 4 seconds to force the power off the server node.

When the server node power button turns amber, it is safe to remove the server node from the chassis.

C3X60 M3 Server Node Mixing Rules

The system is orderable with different preconfigured C3X60 M3 server nodes. Some server nodes cannot be mixed with others in the same system. Note the following rules that refer to the orderable server node PIDs.

- Do not mix a C3X60 M3 server node and a C3X60 M4 server node in the same Cisco UCS S3260 system. An M4 server node can be identified by the “M4 SVRN” label on the rear panel.
- Single-node systems:
  - Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1.
  - Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.

NOTE: Whichever bay a server node is installed to, it must have a corresponding SIOC. That is, a server node in bay 1 must be paired with a SIOC in SIOC slot 1; a server node in bay 2 must be paired with a SIOC in SIOC bay 2.

- Do not mix UCSC-C3X60-SVRN1 with any other server nodes.
- Do not mix server nodes from line 2 below with server nodes from line 3.
- You can mix server nodes within line 2 below.
- You can mix server nodes within line 3 below.

1. UCSC-C3X60-SVRN1
2. UCSC-C3X60-SVRN2; UCSC-C3X60-SVRN3; UCSC-C3X60-SVRN4; UCSC-C3X60-SVRN5
3. UCSC-C3X60-SVRN6; UCSC-C3X60-SVRN7

Replacing a C3X60 M3 Server Node

The server node is accessed from the rear of the system, so you do not have to pull the system out from the rack.

CAUTION: Before you replace a server node, export and save the Cisco IMC configuration from the node if you want that same configuration on the new node. You can import the saved configuration to the new replacement node after you install it.

1. Optional—Export the Cisco IMC configuration from the server node that you are replacing so that you can import it to the replacement server node. If you choose to do this, use the procedure in Exporting Cisco IMC Configuration From a Server Node, page 6, then return to the next step.

NOTE: You do not have to power off the chassis in the next step. Replacement with chassis powered on is supported if you shut down the server node before removal.

2. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
3. Remove a server node from the system:
   a. Grasp the two ejector levers and pinch their latches to release the levers (see Figure 1).
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.
4. Install a server node:
   a. With the two ejector levers open, align the new server node with the empty bay. Note these configuration rules:
   — Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1
   — Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.
   b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.
   c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.
5. Power on the server node.
6. Perform initial setup on the new server node to assign an IP address and your other preferred network settings. See Initial System Setup in the Cisco UCS S3260 Storage Server Installation and Service Guide.
7. Optional—Import the Cisco IMC configuration that you saved in step 1. If you choose to do this, use the procedure in Importing Cisco IMC Configuration To a Server Node, page 7.

Exporting Cisco IMC Configuration From a Server Node

This operation can be performed using either the GUI or CLI interface of the Cisco IMC. The example in this procedure uses the CLI commands. For more information see *Exporting a Cisco IMC Configuration* in the CLI and GUI guides here: Configuration Guides.

1. Log in to the IP address and CLI interface of the server node that you are replacing.
2. Enter the following commands as you are prompted:

```
Server# scope cimc
Server /cimc# scope import-export
Server /cimc/import-export# export-config <protocol> <ip-address> <path-and-filename>
```

3. Enter the user name, password, and pass phrase.

This sets the user name password, and pass phrase for the file that you are exporting. The export operation begins after you enter a pass phrase, which can be anything that you choose.

To determine whether the export operation has completed successfully, use the show detail command. To abort the operation, type CTRL+C.

The following is an example of an export operation. In this example, the TFTP protocol is used to export the configuration to IP address 192.0.2.34, in file /ucs/backups/cimc5.xml.

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:xxxx
Password:****
Passphrase:***
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
Operation: EXPORT
Status: COMPLETED
Error Code: 100 (No Error)
Diagnostic Message: NONE
```

Importing Cisco IMC Configuration To a Server Node

This operation can be performed using either the GUI or CLI interface of the Cisco IMC. The example in this procedure uses the CLI commands. For more information see *Importing a Cisco IMC Configuration* in the CLI and GUI guides here: Configuration Guides.

1. SSH into the CLI interface of the new server node.
2. Enter the following commands as you are prompted:

```
Server# scope cimc
Server /cimc# scope import-export
Server /cimc/import-export# import-config <protocol> <ip-address> <path-and-filename>
```

3. Enter the user name, password, and pass phrase.

   This should be the user name, password, and pass phrase that you used during the export operation. The import operation begins after you enter the pass phrase.

   The following is an example of an import operation. In this example, the TFTP protocol is used to import the configuration to the server node from IP address 192.0.2.34, from file /ucs/backups/cimc5.xml.

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:xxxx
Password:****
Passphrase:***
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
Operation: Import
Status: COMPLETED
Error Code: 100 (No Error)
Diagnostic Message: NONE
```

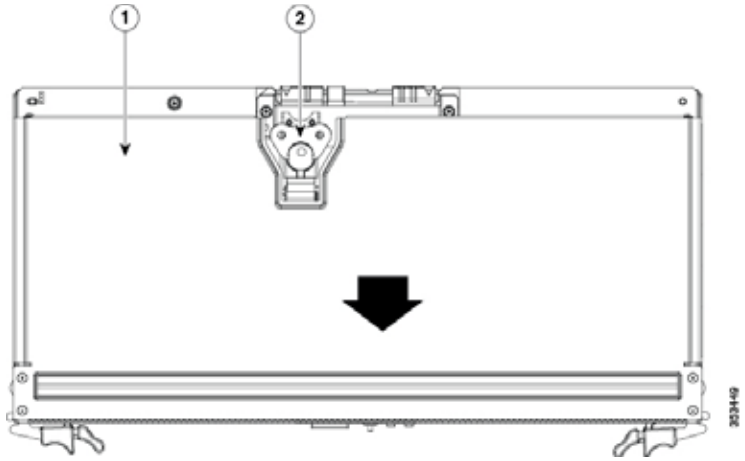
Replacing C3X60 M3 Server Node Internal Components

Removing a C3X60 M3 Server Node Top Cover

NOTE: You do not have to slide the system out of the rack to remove the server node from the rear of the system.

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers and pinch their latches to release the levers (see Figure 1).
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.
3. Remove the cover from the server node:
   a. Lift the latch handle to an upright position (see Figure 3).
   b. Turn the latch handle 90-degrees to release the lock.
   c. Slide the cover toward the rear (toward the rear-panel buttons) and then lift it from the server node.
4. Replace the server node cover:
   a. Set the cover in place on the server node, offset about one inch toward the rear. Pegs on the inside of the cover must set into the tracks on the server node base.
   b. Push the cover forward until it stops.
   c. Turn the latch handle 90-degrees to close the lock.
   d. Fold the latch handle flat.
5. Reinstall a server node:
   a. With the two ejector levers open, align the new server node with the empty bay.
   b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.
   c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.
6. Power on the server node.

Figure 3 Cisco UCS C3X60 M3 Server Node Top Cover



1	Server node top cover	2	Latch handle (shown in closed, flat position)

C3X60 M3 Internal Diagnostic LEDs

There are internal diagnostic LEDs on the edge of the server node board. These LEDs can be viewed while the server node is removed from the chassis, up to 30 seconds after AC power is removed.

There are fault LEDs for each DIMM, each CPU, the RAID card, and each system I/O controller (SIOC).

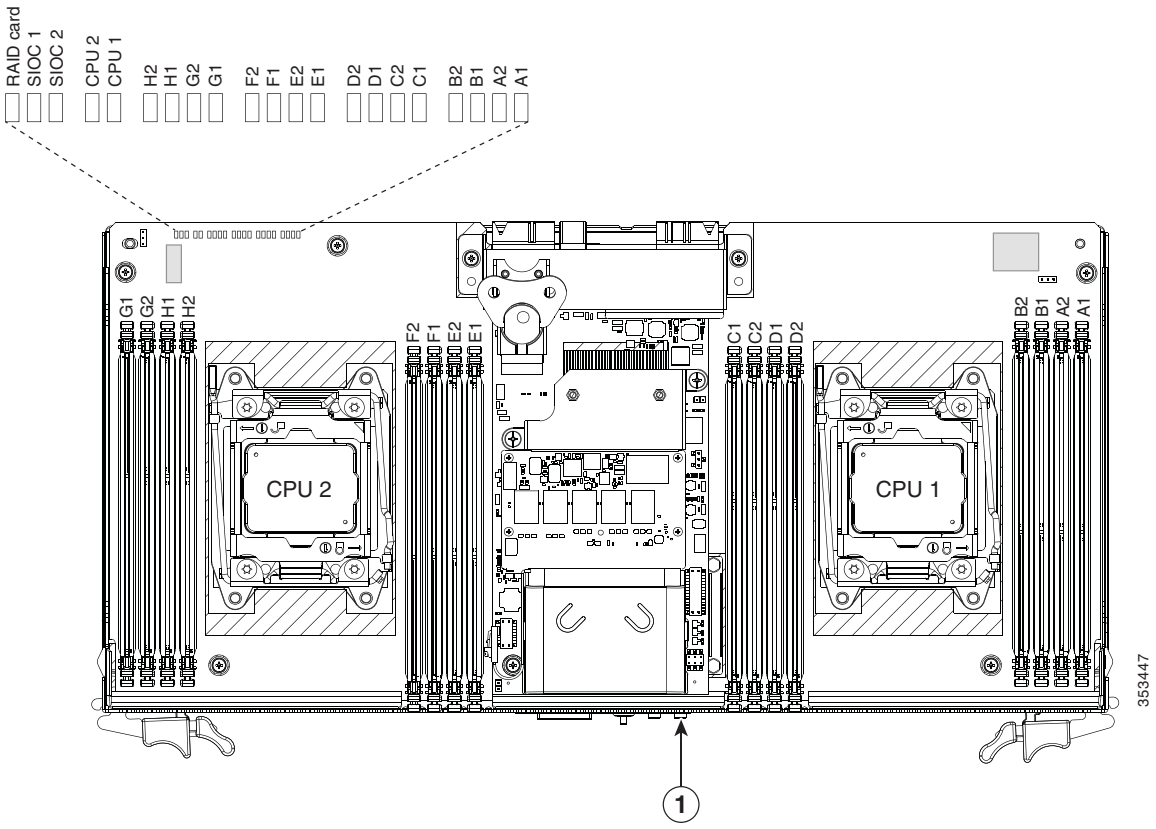
1. Shut down and remove the server node from the system as described in Shutting Down a C3X60 M3 Server Node, page 4.

NOTE: You do not have to remove the server node cover to view the LEDs on the edge of the board.

2. Press and hold the server node unit identification button (see Figure 4) within 30 seconds of removing the server node from the system.

   A fault LED that lights amber indicates a faulty component.

Figure 4 Cisco UCS C3X60 M3 Server Node Internal Components



1	Unit identification button		

Replacing DIMMs Inside the C3X60 M3 Server Node

There are 16 DIMM sockets on the server node board.

CAUTION: DIMMs and their sockets are fragile and must be handled with care to avoid damage during installation.

CAUTION: Cisco does not support third-party DIMMs. Using non-Cisco DIMMs in the system might result in system problems or damage to the motherboard.

NOTE: To ensure the best system performance, it is important that you are familiar with memory performance guidelines and population rules before you install or replace the memory.

For additional information about troubleshooting DIMM memory issues, see the document Troubleshoot DIMM Memory in UCS.

DIMM Performance Guidelines and Population Rules

- DIMM Sockets, page 11
- DIMM Population Rules, page 12
- Memory Mirroring Mode, page 12
- Lockstep Channel Mode, page 12

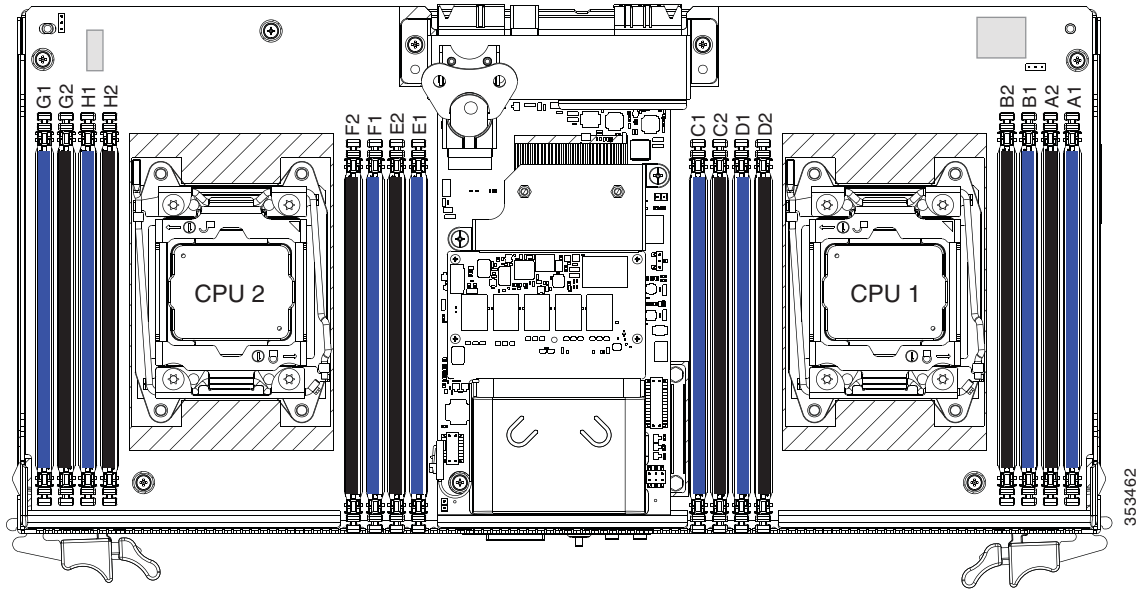
DIMM Sockets

Figure 5 shows the DIMM sockets and how they are numbered on a C3X60 M3 server node board.

- A server node has 16 DIMM sockets (8 for each CPU).
- Channels are labeled with letters as shown in Figure 5.

  For example, channel A = DIMM sockets A1, A2.
- Each channel has two DIMM sockets. The blue socket in a channel is always socket 1.

Figure 5 Cisco UCS C3X60 M3 DIMM and CPU Numbering



DIMM Population Rules

Observe the following guidelines when installing or replacing DIMMs:

- For optimal performance, spread DIMMs evenly across both CPUs and all channels.
- Populate the DIMM sockets of each CPU identically. Populate the blue DIMM 1 sockets first, then the black DIMM 2 slots. For example, populate the DIMM slots in this order:
  1. A1, E1, B1, F1, C1, G1, D1, H1
  2. A2, E2, B2, F2, C2, G2, D2, H2
- Observe the DIMM mixing rules shown in Table 2.

Table 2 DIMM Mixing Rules

DIMM Parameter	DIMMs in the Same Channel	DIMMs in the Same Bank
DIMM Capacity: RDIMM = 8 or 16 GB	You can mix different capacity DIMMs in the same channel (for example, A1, A2).	You can mix different capacity DIMMs in the same bank. However, for optimal performance DIMMs in the same bank (for example, A1, B1, C1, D1) should have the same capacity.
DIMM Speed: 1600- or 1866-MHz	You can mix speeds, but DIMMs will run at the speed of the slowest DIMMs/CPUs installed in the channel.	You can mix speeds, but DIMMs will run at the speed of the slowest DIMMs/CPUs installed in the bank.
DIMM Type: RDIMMs	You cannot mix DIMM types in a channel.	You cannot mix DIMM types in a bank.

Memory Mirroring Mode

When you enable memory mirroring mode, the memory subsystem simultaneously writes identical data to two channels. If a memory read from one of the channels returns incorrect data due to an uncorrectable memory error, the system automatically retrieves the data from the other channel. A transient or soft error in one channel does not affect the mirrored data, and operation continues.

Memory mirroring reduces the amount of memory available to the operating system by 50 percent because only one of the two populated channels provides data.

Lockstep Channel Mode

When you enable lockstep channel mode, each memory access is a 128-bit data access that spans four channels.

Lockstep channel mode requires that all four memory channels on a CPU must be populated identically with regards to size and organization. DIMM socket populations within a channel do not have to be identical but the same DIMM slot location across all four channels must be populated the same.

For example, DIMMs in sockets A1, B1, C1, and D1 must be identical. DIMMs in sockets A2, B2, C2, and D2 must be identical. However, the A1-B1-C1-D1 DIMMs do not have to be identical with the A2-B2-C2-D2 DIMMs.

Replacing DIMMs

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers and pinch their latches to release the levers (see Figure 1).

b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.

c. Pull the server node straight out from the system.

3. Remove the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.

4. Locate the faulty DIMM and remove it from the socket on the riser by opening the ejector levers at both ends of the DIMM socket.

5. Install a new DIMM:

NOTE: Before installing DIMMs, refer to the population guidelines. See DIMM Performance Guidelines and Population Rules, page 11.

a. Align the new DIMM with the socket on the riser. Use the alignment key in the DIMM socket to correctly orient the DIMM.

b. Push the DIMM into the socket until it is fully seated and the ejector levers on either side of the socket lock into place.

6. Replace the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.

7. Install a server node:

a. With the two ejector levers open, align the new server node with the empty bay.

— Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1

— Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.

b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.

c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.

8. Power on the server node.

Replacing CPUs and Heatsinks Inside the C3X60 M3 Server Node

Two CPUs are inside each server node. Although CPUs are not spared separately for this server node, you might need to move your CPUs from a faulty server node to a new server node.

CPU Configuration Rules

- A server node must have two CPUs to operate. See Figure 5 for the C3X60 M3 server node CPU numbering.

Replacing CPUs and Heatsinks

CAUTION: CPUs and their motherboard sockets are fragile and must be handled with care to avoid damaging pins during installation. The CPUs must be installed with heatsinks and their thermal pads to ensure proper cooling. Failure to install a CPU correctly might result in damage to the system.

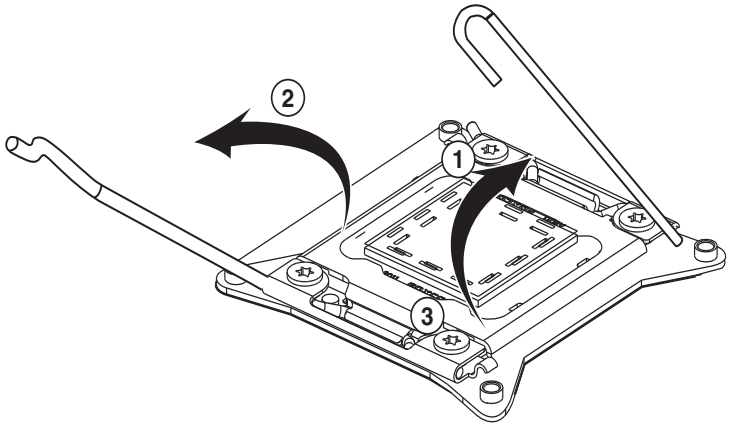
CAUTION: The Pick-and-Place tools used in this procedure are required to prevent damage to the contact pins between the motherboard and the CPU. Do not attempt this procedure without the required tools, which are included with each CPU option kit. If you do not have the tool, you can order a spare (Cisco PID UCS-CPU-EP-PNP).

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers and pinch their latches to release the levers (see Figure 1).
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.
3. Remove the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.
4. Use a Number 2 Phillips-head screwdriver to loosen the four captive screws that secure the heatsink, and then lift it off of the CPU.

   NOTE: Alternate loosening each screw evenly to avoid damaging the heatsink or CPU.
5. Unclip the first CPU retaining latch that is labeled with the  icon, and then unclip the second retaining latch that is labeled with the  icon. See Figure 6.

   NOTE: You must hold the first retaining latch open before you can lift the second retaining latch.
6. Open the hinged CPU cover plate. See Figure 6.

Figure 6 Cisco UCS C3X60 M3 Server Node CPU Socket Retaining Latches



1	CPU retaining latch,	3	Hinged CPU cover plate
2	CPU retaining latch,		

7. Remove the old CPU:

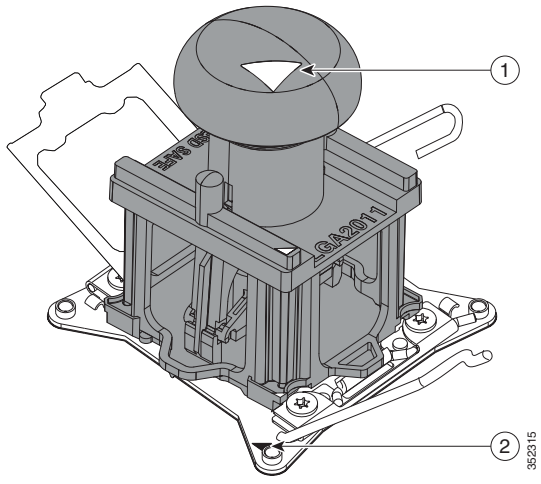
   a. Set the Pick-and-Place tool on the CPU in the socket, aligning the arrow on the tool with the registration mark on the socket (the small triangular mark). See Figure 7.

   b. Press the top button on the tool to grasp the installed CPU.

   c. Lift the tool and CPU straight up.

   d. Press the top button on the tool to release the old CPU on an antistatic surface.

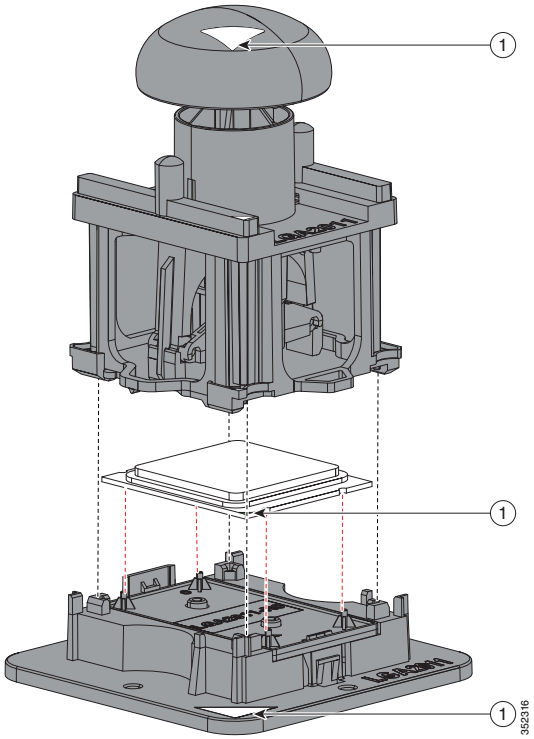
Figure 7 Pick and Place Tool on CPU Socket



1	Arrow mark on tool	2	Registration mark on CPU socket

8. Insert the new CPU into the Pick-and-Place tool:
   a. Remove the new CPU from the packaging and place it on the pedestal that is included in the kit. Align the registration mark on the corner of the CPU with the arrow on the corner of the pedestal (see Figure 8).
   b. Press down on the top button of the tool to lock it open.
   c. Set the Pick-and-Place tool on the CPU pedestal, aligning the arrow on the tool with the arrow on the corner of the pedestal. Make sure that the tabs on the tool are fully seated in the slots on the pedestal.
   d. Press the side lever on the tool to grasp and lock in the CPU.
   e. Lift the tool and CPU straight up off the pedestal.

Figure 8 CPU and Pick and Place Tool on Pedestal



1	Arrow marks on CPU and pedestal for alignment		

9. Install a new CPU:
   a. Set the Pick-and-Place tool that is holding the CPU over the empty CPU socket on the motherboard.

NOTE: Align the arrow on the top of the tool with the registration mark (small triangle) that is stamped on the metal of the CPU socket, as shown in Figure 7.

   b. Press the top button on the tool to set the CPU into the socket. Remove the empty tool.
10. Close the hinged CPU cover plate.
11. Clip down the CPU retaining latch with the icon first, then clip down the CPU retaining latch with the icon. See Figure 6.
12. Install a heatsink:

CAUTION: The heatsink must have a new thermal grease on the heatsink-to-CPU surface to ensure proper cooling. New heatsinks have a pre-applied pad of grease. If you are reusing a heatsink, you must remove the old thermal grease and apply grease from a syringe.

a. Do one of the following:

— If you are installing a new heatsink, remove the protective film from the pre-applied pad of thermal grease on the bottom of the new heatsink. Then continue with step 13

— If you are reusing a heatsink, continue with step 12a.

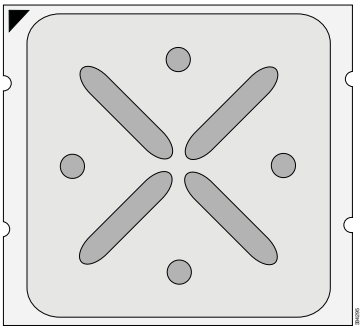
a. Apply an alcohol-based cleaning solution to the old thermal grease and let it soak for a least 15 seconds.

b. Wipe all of the old thermal grease off the old heatsink using a soft cloth that will not scratch the heatsink surface.

c. Apply thermal grease from the syringe that is included with the new CPU to the top of the CPU. Apply about half the syringe contents to the top of the CPU in the pattern that is shown in Figure 9.

NOTE: If you do not have a syringe of thermal grease, you can order a spare (Cisco PID UCS-CPU-GREASE3).

Figure 9 CPU Thermal Grease Application Pattern



13. Align the heatsink captive screws with the motherboard standoffs, and then use a Number 2 Phillips-head screwdriver to tighten the captive screws evenly.

CAUTION: Alternate tightening each screw evenly to avoid damaging the heatsink or CPU.

14. Replace the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.

15. Install a server node:

a. With the two ejector levers open, align the new server node with the empty bay.

— Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1

— Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.

b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.

c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.

16. Power on the server node.

Additional CPU-Related Parts To Order With RMA Replacement Server Nodes

When a return material authorization (RMA) of the server node or CPU is done on a system, there are additional parts that might not be included with the CPU or motherboard spare bill of materials (BOM). The TAC engineer might need to add the additional parts to the RMA to help ensure a successful replacement.

- Scenario 1—You are re-using the existing heatsinks:
  - Heat sink cleaning kit (UCSX-HSCK=)
  - Thermal grease kit for S3260 (UCS-CPU-GREASE3=)
  - Intel CPU Pick-n-Place tool for EP CPUs (UCS-CPU-EP-PNP=)
- Scenario 2—You are replacing the existing heatsinks:
  - Heat sink (UCSB-HS-01-EP=)
  - Heat sink cleaning kit (UCSX-HSCK=)
  - Intel CPU Pick-n-Place tool for EP CPUs (UCS-CPU-EP-PNP=)

A CPU heatsink cleaning kit is good for up to four CPU and heatsink cleanings. The cleaning kit contains two bottles of solution, one to clean the CPU and heatsink of old thermal interface material and the other to prepare the surface of the heatsink.

It is important to clean the old thermal interface material off of the CPU prior to installing the heatsinks. Therefore, when ordering new heatsinks it is still necessary to order the heatsink cleaning kit at a minimum.

Replacing an RTC Battery Inside the Server Node

The real-time clock (RTC) battery retains system settings when the server is disconnected from power. The battery type is CR2032. Cisco supports the industry-standard CR2032 battery, which can be purchased from most electronic stores.

NOTE: When the RTC battery is removed or it completely loses power, settings that were stored in the BMC of the server node are lost. You must reconfigure the BMC settings after installing a new battery.

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers on the node and pinch their latches to release the levers.
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.

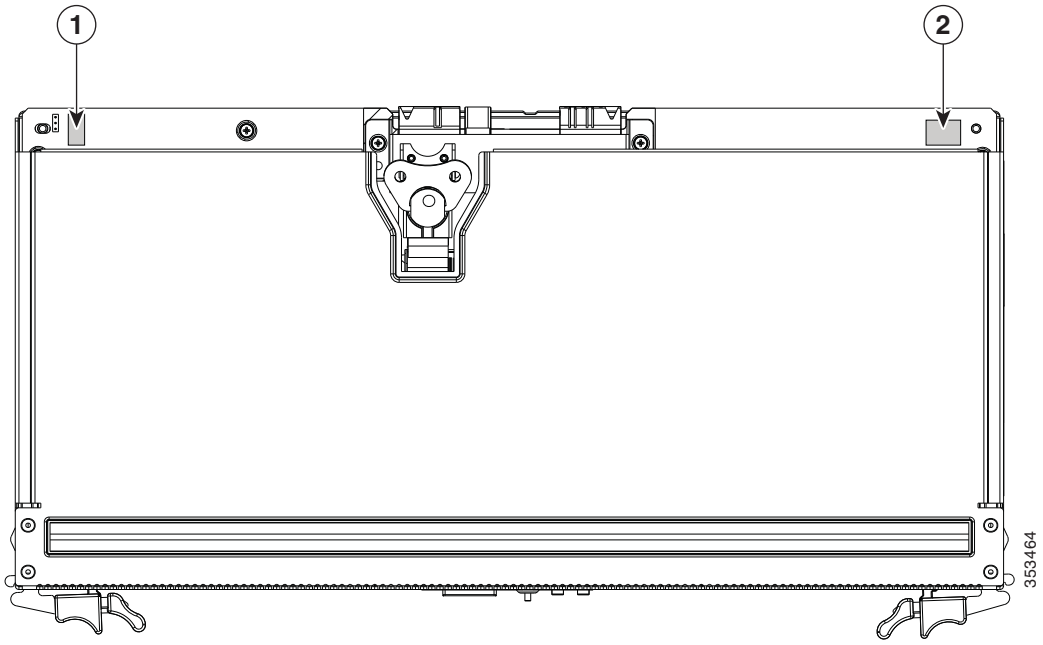
NOTE: You do not have to remove the server node cover to access the RTC battery.

3. Remove the server node RTC battery:
   a. Locate the RTC battery. See Figure 10.
   b. Bend the battery retaining clip away from the battery and pull the battery from the socket.
4. Install the new RTC battery:
   a. Bend the retaining clip away from the battery socket and insert the battery in the socket.

NOTE: The flat, positive side of the battery marked “+” should face the retaining clip.

   b. Push the battery into the socket until it is fully seated and the retaining clip clicks over the top of the battery.
5. Install a server node:
   a. With the two ejector levers open, align the new server node with the empty bay.
   — Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1
   — Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.
   b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.
   c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.
6. Power on the server node.
7. Reconfigure the BMC settings for this node.

Figure 10 RTC Battery and USB Port Inside the C3X60 M3 Server Node



1	Server node RTC battery on board, below edge of cover	2	Internal USB port on board, below edge of cover

Replacing an Internal USB Drive Inside the C3X60 M3 Server Node

This section contains the following topics:

Replacing an Internal USB Drive

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers on the node and pinch their latches to release the levers.
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.

NOTE: You do not have to remove the server node cover to access the USB socket.

3. Remove an existing USB flash drive from the port on the server node board (see Figure 10). Pull the drive horizontally from the port.
4. Install a USB flash drive. Insert the new USB flash drive into the horizontal socket on the server node board.
5. Install a server node:
   a. With the two ejector levers open, align the new server node with the empty bay:
   — Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1

— Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.

b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.

c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.

6. Power on the server node.

Enabling or Disabling the Internal USB Port

The factory default is for all USB ports on the system to be enabled. However, the internal USB port can be enabled or disabled in the system BIOS. To enable or disable the internal USB port, follow these steps:

1. Enter the BIOS Setup utility by pressing the **F2** key when prompted during bootup.
2. Navigate to the **Advanced** tab.
3. On the Advanced tab, select **USB Configuration**.
4. On the USB Configuration page, select **USB Ports Configuration**.
5. Scroll to **USB Port: Internal**, press **Enter**, and then select either Enabled or Disabled from the menu.
6. Press F10 to save and exit the utility.

Installing a Trusted Platform Module (TPM) Inside the C3X60 M3 Server Node

The trusted platform module (TPM) is a small circuit board that attaches to a socket on the server node board. This section contains the following procedures, which must be followed in this order when installing and enabling a TPM:

1. Installing the TPM Hardware, page 21
2. Enabling TPM Support in the BIOS, page 22
3. Enabling the Intel TXT Feature in the BIOS, page 23

Installing the TPM Hardware

NOTE: For security purposes, the TPM is installed with a one-way screw. It cannot be removed with a standard screwdriver.

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:

   a. Grasp the two ejector levers on the node and pinch their latches to release the levers.

   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.

   c. Pull the server node straight out from the system.

NOTE: You do not have to remove the server node cover to access the TPM socket.

3. Install a TPM:

   a. Locate the TPM socket on the server node board, as shown in Figure 11.

b. Align the connector that is on the bottom of the TPM circuit board with the TPM socket. Align the screw hole on the TPM board with the screw hole adjacent to the TPM socket.

c. Push down evenly on the TPM to seat it in the motherboard socket.

d. Install the single one-way screw that secures the TPM to the motherboard.

4. Install a server node:

a. With the two ejector levers open, align the new server node with the empty bay.

— Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1

— Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.

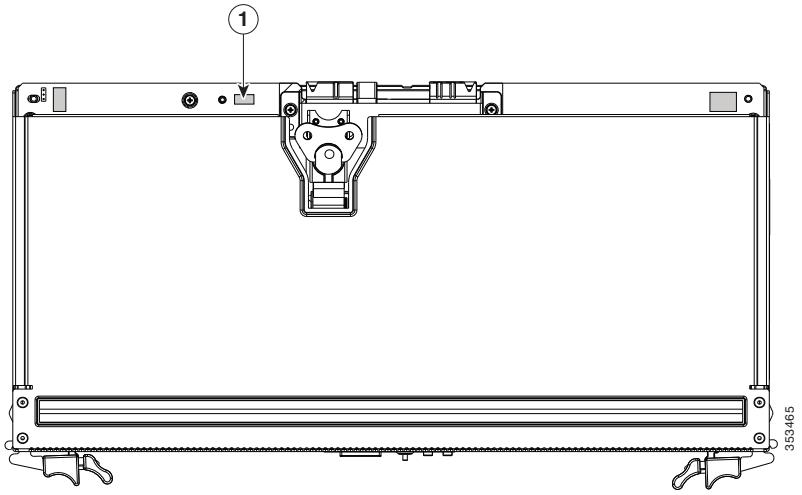
b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.

c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.

5. Power on the server node.

6. Continue with Enabling TPM Support in the BIOS, page 22.

Figure 11 TPM Location Inside the C3X60 M3 Server Node



1	TPM socket location on board		

Enabling TPM Support in the BIOS

NOTE: After hardware installation, you must enable TPM support in the BIOS.

NOTE: You must set a BIOS Administrator password before performing this procedure. To set this password, press the **F2** key when prompted during system boot to enter the BIOS Setup utility. Then navigate to **Security > Set Administrator Password** and enter the new password twice as prompted.

1. Enable TPM support:

d. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.

e. Log in to the BIOS Setup Utility with your BIOS Administrator password.

f. On the BIOS Setup Utility window, choose the **Advanced** tab.

g. Choose **Trusted Computing** to open the TPM Security Device Configuration window.

h. Change TPM SUPPORT to **Enabled**.

i. Press **F10** to save your settings and reboot the server node.

2. Verify that TPM support is now enabled:

a. Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.

b. Log into the BIOS Setup utility with your BIOS Administrator password.

c. Choose the **Advanced** tab.

d. Choose **Trusted Computing** to open the TPM Security Device Configuration window.

e. Verify that TPM SUPPORT and TPM State are Enabled.

3. Continue with Enabling the Intel TXT Feature in the BIOS, page 23.

Enabling the Intel TXT Feature in the BIOS

Intel Trusted Execution Technology (TXT) provides greater protection for information that is used and stored on the business server. A key aspect of that protection is the provision of an isolated execution environment and associated sections of memory where operations can be conducted on sensitive data, invisibly to the rest of the system. Intel TXT provides for a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code.

1. Reboot the server node and watch for the prompt to press F2.

2. When prompted, press **F2** to enter the BIOS Setup utility.

3. Verify that the prerequisite BIOS values are enabled:

a. Choose the **Advanced** tab.

b. Choose **Intel TXT(LT-SX) Configuration** to open the Intel TXT(LT-SX) Hardware Support window.

c. Verify that the following items are listed as Enabled:

— VT-d Support (default is Enabled)

— VT Support (default is Enabled)

— TPM Support

— TPM State

- If VT-d Support and VT Support are already enabled, skip to 4..
- If VT-d Support and VT Support are not enabled, continue with the next steps to enable them.

a. Press **Escape** to return to the BIOS Setup utility **Advanced** tab.

b. On the Advanced tab, choose **Processor Configuration** to open the Processor Configuration window.

c. Set Intel (R) VT and Intel (R) VT-d to **Enabled**.

4. Enable the Intel Trusted Execution Technology (TXT) feature:

a. Return to the Intel TXT(LT-SX) Hardware Support window if you are not already there.

b. Set TXT Support to **Enabled**.

5. Press **F10** to save your changes and exit the BIOS Setup utility.

Replacing a Storage Controller Card in the C3X60 M3 Server Node

The Cisco storage controller card connects to a mezzanine-style socket inside the server node.

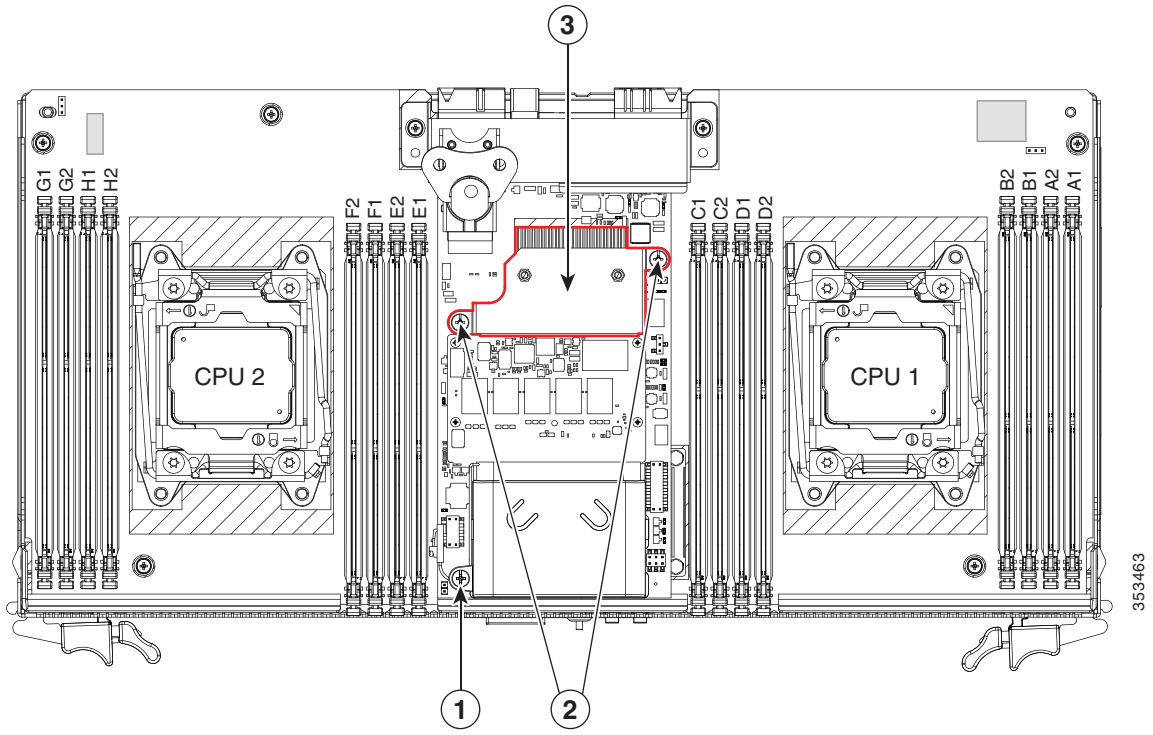
To replace a supercap power module (RAID backup), see Replacing a SuperCap Power Module (RAID Backup), page 26.

NOTE: Do not mix different storage controllers in the same system. If the system has two server nodes, they must both contain the same controller.

NOTE: See Storage Controller Considerations, page 28 for information about the controllers supported in the C3X60 M3 server node.

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers on the node and pinch their latches to release the levers.
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.
3. Remove the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.
4. Remove a storage controller card:
   a. Loosen the two captive thumbscrews that secure the card to the board (see Figure 12).
   b. Remove the screw that is next to the supercap power module.
   c. Grasp the card at both ends and lift it evenly to disengage the connector on the underside of the card from the mezzanine socket.
5. Install a storage controller card:
   a. Align the card and bracket over the mezzanine socket and the three standoffs.
   b. Press down on both ends of the card to engage the connector on the underside of the card with the mezzanine socket.
   c. Install the screw that is next to the supercap power module (backup battery) cover (see Figure 12).
6. Install the heat sink assembly to the controller card:
   a. Remove the protective tape from the thermal interface that is on the underside of the heatsink.
   b. Align the heat sink assembly and its two captive screws with the holes in the controller card.
   c. Tighten the two captive screws to the two standoffs that are under the controller card.
7. Replace the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.
8. Install a server node:
   a. With the two ejector levers open, align the new server node with the empty bay.
   — Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1.
   — Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.
   b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.
   c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.
9. Power on the server node.

Figure 12 Storage Controller Card Inside the C3X60 M3 Server Node



1	Screw next to supercap power module	3	Heatsink assembly
2	Two captive screws that pass through heatsink assembly to standoffs		

Replacing a SuperCap Power Module (RAID Backup)

The server node supports one supercap power module (SCPM) that mounts directly to the RAID controller.

The SCPM provides approximately 3 years of backup for the disk write-back cache DRAM in the case of sudden power loss by offloading the cache to the NAND flash.

The PID for the spare SCPM is UCSC-SCAP-M5=.

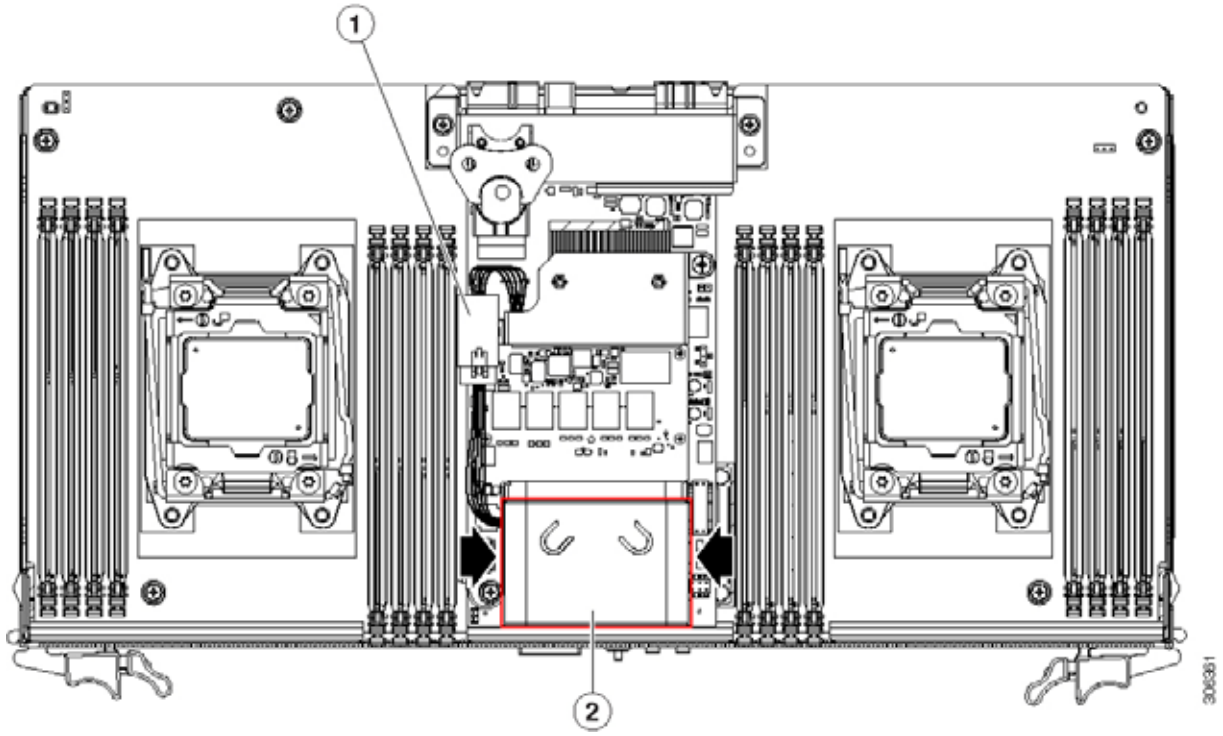
1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers on the node and pinch their latches to release the levers.
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.
3. Remove the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.
4. Remove the SCPM from the RAID controller:
   a. Remove the plastic cover that sits over the SCPM.

   The plastic SCPM cover has two tabs that fit into slots on the RAID controller board. Pinch inward on both ends of the plastic cover to free the tabs and then lift straight up.

   b. Disconnect the SCPM cable from the RAID controller cable that it is attached to.
   c. Lift the SCPM from the RAID controller.
5. Install a new SCPM to the RAID controller:
   a. Set the new SCPM in the rectangle printed on the RAID controller board.
   b. Connect the SCPM cable to the RAID controller cable to which the old SCPM was attached.
   c. Set the plastic SCPM cover over the SCPM.

   Carefully insert the tabs on the cover into the slots on the RAID controller board.
6. Replace the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.
7. Install a server node:
   a. With the two ejector levers open, align the new server node with the empty bay.
   — Cisco IMC releases earlier than 2.0(13): If your S3260 system has only one server node, it must be installed in bay 1.
   — Cisco IMC releases 2.0(13) and later: If your S3260 system has only one server node, it can be installed in either server bay.
   b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.
   c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.
8. Power on the server node.

Figure 13 Supercap Power Module on RAID Controller Card



1	SCPM cable connector	2	Plastic SCPM cover Pinch on the points indicated by the arrows to disengage the cover tabs from the slots on the controller board.

Storage Controller Considerations

Supported Storage Controllers and Required Cables

Table 3 lists the supported storage controller cards for the C3X60 M3 server node.

Table 3 Cisco UCS C3X60 M3 Supported Storage Controller Options

Controller	Style	Maximum Drives	SCPM?	RAID Levels	Required Cables
Embedded RAID (PCH SATA)	Chip on-board in each server node	2 rear-panel SSDs (each server node)	N/A	0, 1	None. Chip on-board in each server node.
Cisco UCS C3X60 12G SAS RAID UCSC-C3X60-R1GB UCSC-C3X60-R4GB (with 1-GB or 4-GB write cache)	Mezzanine	60 internal	Yes	0, 1, 5, 6, 10, 50, 60 JBOD mode (non-RAID) is also supported.	None. Card installs to mezzanine socket inside the server node.
Cisco UCS 12G SAS HBA pass-through controller UCSC-C3X60-HBA	Mezzanine	60 internal	No	Non-RAID	None. Card installs to mezzanine socket inside the server node.

Cisco UCS 12G SAS RAID Controller Specifications

The Cisco UCS C3X60 12G SAS RAID controller can be ordered with a 1-GB or a 4-GB write cache (UCSC-C3X60-R1GB or UCSC-C3X60-R4GB).

The controller can be used in JBOD mode (non-RAID) or in RAID mode with a choice of RAID levels 0,1,5,6,10, 50, or 60.

- Maximum drives controllable—64 (the server has maximum 60 internal drives)
- Maximum drives per span—32
- Maximum spans—8

Best Practices For Configuring RAID Controllers

4K Sector Format Drives

Do not configure 4K sector format and 512-byte sector format drives as part of the same RAID volume.

RAID Card Firmware Compatibility

Firmware on the RAID controller must be verified for compatibility with the current Cisco IMC and BIOS versions that are installed on the server. If not compatible, upgrade or downgrade the RAID controller firmware accordingly using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: HUU Guides

Choosing Between RAID 0 and JBOD

The Cisco UCS C3X60 12G SAS RAID controller supports JBOD mode (non-RAID) on physical drives that are in pass-through mode and directly exposed to the OS. We recommended that you use JBOD mode instead of individual RAID 0 volumes when possible.

RAID 5/RAID 6 Volume Creation

The Cisco UCS C3X60 12G SAS RAID controller allows you to create of large RAID 5 or 6 volume by including all the drives in the system with a spanned array configuration (RAID 50/RAID 60). Where possible, we recommended you create multiple, smaller RAID 5/6 volumes with fewer drives per RAID array. This provides redundancy and reduces the operations time for initialization, RAID rebuilds, and other operations.

Choosing I/O Policy

The I/O policy applies to reads on a specific virtual drive. It does not affect the read-ahead cache. RAID volumes can be configured in two types of I/O policies. These are:

- Cached I/O—In this mode, all reads are buffered in cache memory. Cached I/O provides faster processing.
- Direct I/O—In this mode, reads are not buffered in cache memory. Data is transferred to the cache and the host concurrently. If the same data block is read again, it comes from cache memory. Direct I/O makes sure that the cache and the host contain the same data.

Although Cached I/O provides faster processing, it is useful only when the RAID volume has a small number of slower drives. With the C3X60 4-TB SAS drives, Cached I/O has not shown any significant advantage over Direct I/O. Instead, Direct I/O has shown better results over Cached I/O in a majority of I/O patterns. We recommended you use Direct I/O (the default) in all cases and to use Cached I/O cautiously.

Background Operations (BGOPs)

The Cisco UCS 12G SAS RAID controller conducts different background operations like Consistency Check (CC), Background Initialization (BGI), Rebuild (RBLD), Volume Expansion & Reconstruction (RLM), and Patrol Real (PR).

While these BGOPS are expected to limit their impact to I/O operations, there have been cases of higher impact during some of the operations like Format or similar I/O operations. In these cases, both the I/O operation and the BGOPS may take more time to complete. In such cases, we recommend you limit concurrent BGOPS and other intensive I/O operations where possible.

BGOPS on large volumes can take an extended period of time to complete, presenting a situation where operations complete and begin with limited time between operations. Since BGOPS are intended to have a very low impact in most I/O operations, the system should function without any issues. If there are any issues that arise while running concurrent BGOPS and I/O operations, we recommend you to stop either activity to let the other complete before reusing and/or schedule the BGOPS at a later time when the I/O operations are low.

Restoring RAID Configuration After Replacing a RAID Controller

When you replace a RAID controller, the RAID configuration that is stored in the controller is lost.

To restore your RAID configuration to your new RAID controller, follow these steps.

1. Replace your RAID controller. See Replacing a Storage Controller Card in the C3X60 M3 Server Node, page 24.
2. If this was a full chassis swap, replace all drives into the drive bays, in the same order that they were installed in the old chassis.
3. Reboot the server node.
4. Press any key (other than C) to continue when you see the following onscreen prompt:

```
All of the disks from your previous configuration are gone. If this is
an unexpected message, then please power of your system and check your cables
to ensure all disks are present.
Press any key to continue, or 'C' to load the configuration utility.
```

5. Watch the subsequent screens for confirmation that your RAID configuration was imported correctly:

- If you see the following message, your configuration was successfully imported. The LSI virtual drive is also listed among the storage devices.

  ```
  N Virtual Drive(s) found on host adapter.
  ```

- If you see the following message, your configuration was not imported. In this case, reboot the server node and try the import operation again.

  ```
  0 Virtual Drive(s) found on host adapter.
  ```

Embedded Software RAID

Each server node includes an embedded MegaRAID controller that can control two rear-panel solid state drives (SSDs) in a RAID 0 or 1 configuration.

NOTE: VMware ESX/ESXi or any other virtualized environments are not supported for use with the embedded MegaRAID controller. Hypervisors such as Hyper-V, Xen, or KVM are also not supported for use with the embedded MegaRAID controller.

NOTE: The embedded RAID controller in server node 1 can control the upper two rear-panel SSDs; the embedded RAID controller in server node 2 can control the lower two rear-panel SSDs.

Launching the LSI Embedded MegaRAID Configuration Utility

1. When the server reboots, watch for the prompt to press Ctrl+M.
2. When you see the prompt, press **Ctrl+M** to launch the utility.

Installing LSI MegaSR Drivers For Windows and Linux

NOTE: The required drivers for this controller are already installed and ready to use with the LSI software RAID Configuration Utility. However, if you will use this controller with Windows or Linux, you must download and install additional drivers for those operating systems.

This section explains how to install the LSI MegaSR drivers for the following supported operating systems:

- Microsoft Windows Server
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your server release.

This section contains the following topics:

Downloading the LSI MegaSR Drivers

The MegaSR drivers are included in the C-Series driver ISO for your server and OS. Download the drivers from Cisco.com.

1. Find the drivers ISO file download for your server online and download it to a temporary location on your workstation:
   a. See the following URL: **http://www.cisco.com/cisco/software/navigator.html**
   b. Click **Unified Computing and Servers** in the middle column.
   c. Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right-hand column.

d. Click your model of server in the right-hand column.

e. Click **Unified Computing System (UCS) Drivers**.

f. Click the release number that you are downloading.

g. Click **Download** to download the drivers' ISO file.

h. Verify the information on the next page, and click **Proceed With Download**.

i. Continue through the subsequent screens to accept the license agreement and then browse to a location where you want to save the drivers' ISO file.

Microsoft Windows Driver Installation

This section describes how to install the LSI MegaSR driver in a Windows installation.

This section contains the following topics:

Windows Server 2008R2 Driver Installation

The Windows operating system automatically adds the driver to the registry and copies the driver to the appropriate directory.

1. Create a RAID drive group using the LSI Software RAID Configuration Utility before you install this driver for Windows. Launch this utility by pressing **Ctrl+M** when `LSI SWRAID` is shown during the BIOS POST.
2. Download the Cisco UCS C-Series drivers' ISO, as described in Downloading the LSI MegaSR Drivers, page 31.
3. Prepare the drivers on a USB thumb drive:
   a. Burn the ISO image to a disk.
   b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

   /<OS>/Storage/Intel/C600/

   c. Expand the Zip file, which contains the folder with the MegaSR driver files.
   d. Copy the expanded folder to a USB thumb drive.
4. Start the Windows driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the server and then insert the first Windows installation disk into the drive. Skip to 6..
- To install from remote ISO, log in to the server's Cisco IMC interface and continue with the next step.

5. Launch a Virtual KVM console window and click the **Virtual Media** tab.
   a. Click **Add Image** and browse to select your remote Windows installation ISO file.
   b. Check the check box in the Mapped column for the media that you just added, and then wait for mapping to complete.
6. Power cycle the server.
7. Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

8. On the Boot Manager window, choose the physical disk or virtual DVD and press **Enter**. The Windows installation begins when the image is booted.
9. Press **Enter** when you see the prompt, “Press any key to boot from CD.”
10. Observe the Windows installation process and respond to prompts in the wizard as required for your preferences and company standards.
11. When Windows prompts you with “Where do you want to install Windows,” install the drivers for embedded MegaRAID:
    a. Click **Load Driver**. You are prompted by a Load Driver dialog box to select the driver to be installed.
    b. Connect the USB thumb drive that you prepared in 3. to the target server.
    c. On the Windows Load Driver dialog that you opened in Step a, click **Browse**.
    d. Use the dialog box to browse to the location of the drivers folder on the USB thumb drive, and then click **OK**.

    Windows loads the drivers from the folder and when finished, the driver is listed under the prompt, “Select the driver to be installed.”

    e. Click **Next** to install the drivers.

Updating the Windows Driver

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **System**, click the **Hardware** tab, and then click **Device Manager**. Device Manager starts.
3. In Device Manager, double-click **SCSI and RAID Controllers**, right-click the device for which you are installing the driver, and then click **Properties**.
4. On the Driver tab, click **Update Driver** to open the Update Device Driver wizard, and then follow the wizard instructions to update the driver.

Linux Driver Installation

This section explains the steps to install the embedded MegaRAID device driver in a Red Hat Enterprise Linux installation or a SUSE Linux Enterprise Server installation.

This section contains the following topics:

Obtaining the Driver Image File

See Downloading the LSI MegaSR Drivers, page 31 for instructions on obtaining the drivers. The Linux driver is offered in the form of dud-[*driver version*].img, which is the boot image for the embedded MegaRAID stack.

NOTE: The LSI MegaSR drivers that Cisco provides for Red Hat Linux and SUSE Linux are for the original GA versions of those distributions. The drivers do not support updates to those OS kernels.

Preparing Physical Installation Disks For Linux

This section describes how to prepare physical Linux installation disks from the driver image files, using either the Windows operating system or the Linux operating system.

NOTE: The driver image is too large for a floppy disk, so use a USB thumb drive instead.

NOTE: Alternatively, you can mount the dud.img file as a virtual floppy disk, as described in the installation procedures.

Preparing Physical Installation Disks For Linux With the Windows Operating System

Under Windows, you can use the RaWrite floppy image-writer utility to create disk images from image files.

1. Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page 31 and save it to your Windows system that has a diskette drive.
2. Extract the dud.img file:
   a. Burn the ISO image to a disc.
   b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

   /<OS>/Storage/Intel/C600/

   c. Expand the Zip file, which contains the folder with the driver files.
3. Copy the driver update disk image dud-[driver version].img and your file raw write.exe to a directory.

NOTE: RaWrite is not included in the driver package.

4. If necessary, use this command to change the filename of the driver update disk to a name with fewer than eight characters: **copy dud-[***driver version***].img dud.img**
5. Open the DOS Command Prompt and navigate to the directory where raw write.exe is located.
6. Enter the following command to create the installation diskette: **raw write**
7. Press **Enter**.

   You are prompted to enter the name of the boot image file.
8. Enter: **dud.img**
9. Press **Enter**.

   You are prompted for the target disk.
10. Insert a floppy disk into the server and enter: **A:**
11. Press **Enter**.
12. Press **Enter** again to start copying the file to the diskette.
13. After the command prompt returns and the floppy disk drive LED goes out, remove the disk.
14. Label the diskette with the image name.

Preparing Installation Disks with a Linux Operating System

Under Red Hat Linux and SUSE Linux, you can use a driver disk utility to create disk images from image files.

NOTE: The driver image is too large for a floppy disk, so use a USB thumb drive instead.

1. Download the Cisco UCS C-Series drivers ISO, as described in Downloading the LSI MegaSR Drivers, page 31 and save it to your Linux system that has a disk drive.
2. Extract the dud.img file:
   a. Burn the ISO image to a disc.
   b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

   /<OS>/Storage/Intel/C600/

   c. Expand the Zip file, which contains the folder with the driver files.
3. Copy the driver update disk image dud-[driver version].img to your Linux system.
4. Insert a blank USB thumb drive into a port on your Linux system.
5. Create a directory and mount the DUD image to that directory:

   mkdir <*destination_folder*>

   mount -oloop <*driver_image*> <*destination_folder*>
6. Copy the contents in the directory to your USB thumb drive.

Installing the Red Hat Linux Driver

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your server release.

This section describes the fresh installation of the Red Hat Enterprise Linux device driver on systems with the embedded MegaRAID stack.

1. Create a RAID drive group using the LSI Software RAID Configuration utility before you install this driver for the OS. Launch this utility by pressing **Ctrl-M** when `LSI SWRAID` is shown during the BIOS POST.
2. Prepare the dud.img file using one of the following methods:

- To install from a physical disk: Use one of the procedures in Preparing Physical Installation Disks For Linux, page 34. Then return to 4. of this procedure.
- To install from a virtual floppy disk: Download and save the Cisco UCS C-Series drivers' ISO, as described in Downloading the LSI MegaSR Drivers, page 31. Then continue with the next step.

3. Extract the dud.img file:
   a. Burn the ISO image to a disc.
   b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

   /<OS>/Storage/Intel/C600/

   c. Copy the dud-<*`driver version`*>.img file to a temporary location on your workstation.
4. Start the Linux driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the server and then insert the first RHEL installation disk into the drive. Then continue with step 6.
- To install from remote ISO, log in to the server's Cisco IMC interface. Then continue with the next step.

5. Launch a Virtual KVM console window and click the **Virtual Media** tab.
   a. Click **Add Image** and browse to select your remote RHEL installation ISO file.
   b. Click **Add Image** again and browse to select your dud.img file.
   c. Check the check boxes in the Mapped column for the media that you just added, then wait for mapping to complete.
6. Power cycle the server.
7. Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.
8. On the Boot Manager window, select the physical disk or virtual DVD and press **Enter**.

   The RHEL installation begins when the image is booted.
9. Enter one of the following commands at the boot prompt:

- For RHEL 6.*x* (32- and 64-bit), enter:
  linux dd blacklist=isci blacklist=ahci nodmraid noprobe=<ata*drive number*>
- For RHEL 7.x (32- and 64-bit), enter:
  linux dd modprobe.blacklist=ahci nodmraid

NOTE: The **noprobe** values depend on the number of drives. For example, to install RHEL 6.5 on a RAID 5 configuration with three drives, enter **Linux dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1 noprobe=ata2**

10. Press **Enter**.

    The prompt asks whether you have a driver disk.
11. Use the arrow key to choose **Yes**, and then press **Enter**.
12. Choose **fd0** to indicate that you have a floppy disk with the driver on it.
13. Do one of the following actions:

- If you prepared the IMG file on a physical diskette in 2., connect an external disk drive to the target server and then insert the disk in the A:/ drive and press **Enter**.
- If you mapped the IMG file as a virtual floppy in 5., choose the location of the virtual floppy.

  The installer locates and loads the driver for your device. The following message appears:

  Loading megasr driver...

14. Follow the Red Hat Linux installation procedure to complete the installation.
15. Reboot the system.

Installing the SUSE Linux Enterprise Server Driver

For the specific supported OS versions, see the Hardware and Software Interoperability Matrix for your server release.

This section describes the installation of the SUSE Linux Enterprise Server driver on a system with the embedded MegaRAID stack.

1. Create a RAID drive group using the LSI SWRAID Configuration utility before you install this driver for the OS. Launch this utility by pressing **Ctrl+M** when `LSI SWRAID` is shown during the BIOS POST.
2. Prepare the dud.img file using one of the following methods:

- To install from a physical disk, use one of the procedures in Preparing Physical Installation Disks For Linux, page 34.
  Then return to step 4 of this procedure.

- To install from a virtual floppy disk, download and save the Cisco UCS C-Series drivers' ISO, as described in Downloading the LSI MegaSR Drivers, page 31. Then continue with the next step.

3. Extract the dud.img file:
   a. Burn the ISO image to a disc.
   b. Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers:

   /<OS>/Storage/Intel/C600/

   c. Copy the dud-<*driver version*>.img file to a temporary location on your workstation.
4. Start the Linux driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the server and then insert the first RHEL install disc into the drive. Skip to step 6.
- To install from remote ISO, log in to the server's Cisco IMC interface and continue with the next step.

5. Launch a Virtual KVM console window and click the **Virtual Media** tab.
   a. Click **Add Image** and browse to select your remote RHEL installation ISO file.
   b. Click **Add Image** again and browse to select your dud.img file.
   c. Check the check box in the Mapped column for the media that you just added, and then wait for mapping to complete.
6. Power cycle the server.
7. Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.
8. On the Boot Manager window, select the physical disk or virtual DVD and press **Enter**. The SLES installation begins when the image is booted.
9. When the first SLES screen appears, choose **Installation**.
10. Enter one of the following in the Boot Options field:

- For SLES 11 and SLES 11 SP1 (32- and 64-bit), enter: **brokenmodules=ahci**
- For SLES 11 SP2 (32-and 64-bit), enter: **brokenmodules=ahci brokenmodules=isci**
- For SLES 12, enter: **brokenmodules=ahci**

11. Press **F6** for the driver and choose **Yes**.
12. Do one of the following actions:

- If you prepared the IMG file on a physical disk in 2., insert the USB thumb drive to the target server and then insert the disk in the A:/ drive and press **Enter**.
- If you mapped the IMG file as a virtual floppy in 5., choose the location of the virtual floppy.

  "Yes" appears under the F6 Driver heading.

13. Press **Enter** to choose Installation.
14. Press **OK**.

    The following message is displayed: `LSI Soft RAID Driver Updates added.`

15. At the menu, choose the driver update medium and press the **Back** button.
16. Continue and complete the installation process by following the prompts in the installation wizard.

For More Information on Using Storage Controllers

The LSI utilities have help documentation for more information about using the utilities.

For basic information about RAID and for using the utilities for the RAID controller cards, see the Cisco UCS Servers RAID Guide.

Full Avago Technologies/LSI documentation is also available:

- For hardware SAS MegaRAID—Avago Technologies/LSI 12 Gb/s MegaRAID SAS Software User's Guide, Rev. F
- For embedded software MegaRAID—LSI Embedded MegaRAID Software User Guide

Service Headers on the Server Node Board

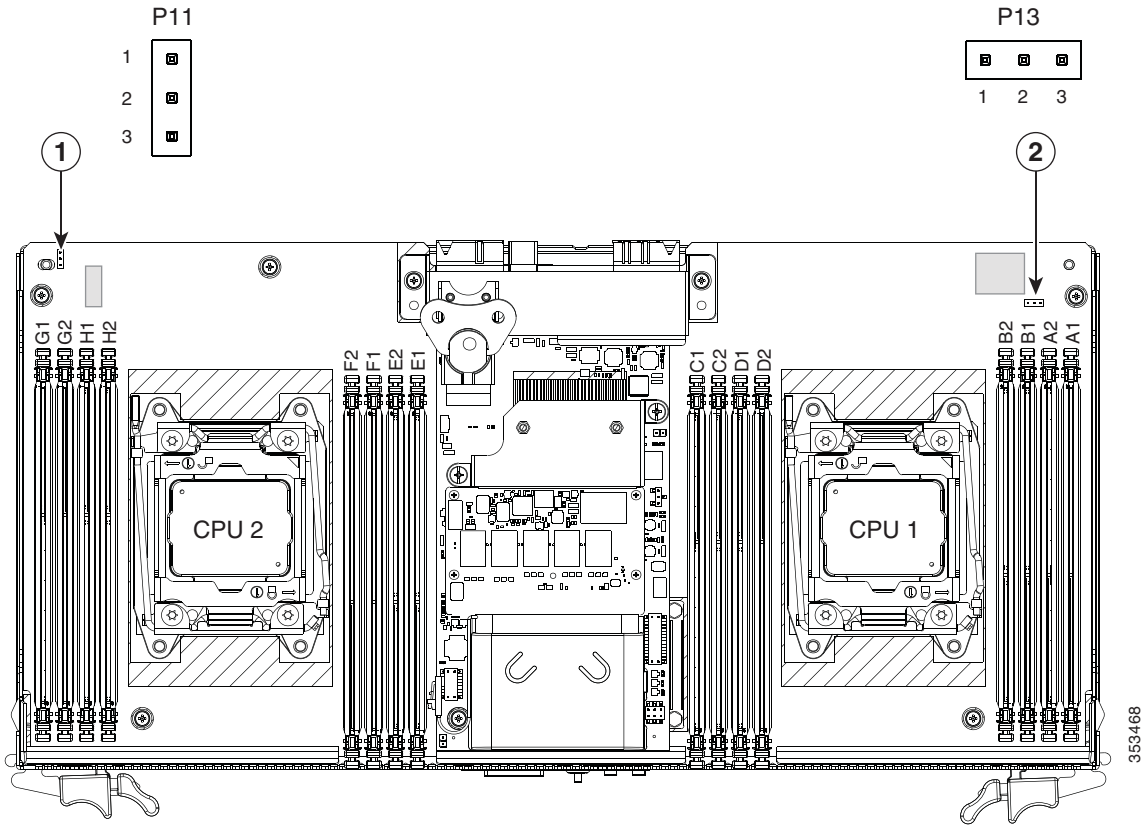
The server node board includes headers that you can jumper for certain service functions. This section includes the following topics:

Service Header Locations on the C3X60 M3 Server Node Board

There are two 3-pin service headers on the server node board that are supported for use. See Figure 14 for the locations.

- Header P11 = Password clear
- Header P13 = CMOS clear

Figure 14 Service Headers on the Server Node Board



1	Header P11 = Password clear	**2**	Header P13 = CMOS clear

Using the Clear Password Header P11

You can use a jumper on header P11 to clear the administrator password.

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Remove a server node from the system:
   a. Grasp the two ejector levers and pinch their latches to release the levers.
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node straight out from the system.

NOTE: You do not have to remove the server node cover to access the header.

3. Remove the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.
4. Locate header P11 (see Figure 14).
5. Install a jumper to pins 2 and 3 of the header.
6. Install the server node:
   a. With the two ejector levers open, align the new server node with the empty bay.
   b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.
   c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.
7. After the server node has fully booted, shut it down again, as described in Shutting Down a C3X60 M3 Server Node, page 4.
8. Remove the server node from the system, and then remove the server node cover.
9. Remove the jumper from pins 2 and 3.

NOTE: If you do not remove the jumper, the Cisco IMC clears the password each time that you boot the server node.

10. Install the server node cover, and then install server node back to the system.
11. Power on the server node.

Using the Clear CMOS Header P13

You can install a jumper to header P13 to clear the CMOS settings.

1. Shut down the server node by using the software interface or by pressing the node power button, as described in Shutting Down a C3X60 M3 Server Node, page 4.
2. Physically remove a server node chassis from the system:
   a. Grasp the two ejector levers and pinch their latches to release the levers.
   b. Rotate both levers to the outside at the same time to evenly disengage the server node from its midplane connectors.
   c. Pull the server node chassis straight out from the system.
3. Remove the server node cover as described in Removing a C3X60 M3 Server Node Top Cover, page 8.
4. Locate header P13 (see Figure 14).

5. Install a jumper to pins 2 and 3 of the header.
6. Install the server node chassis to the system:
   a. With the two ejector levers open, align the new server node with the empty bay.
   b. Push the server node into the bay until it engages with the midplane connectors and is flush with the chassis.
   c. Rotate both ejector levers toward the center until they lay flat and their latches lock into the rear of the server node.
7. After the server node has fully booted, shut it down again, as described in Shutting Down a C3X60 M3 Server Node, page 4.
8. Remove the server node from the system, and then remove the server node cover.
9. Remove the jumper from pins 2 and 3.

NOTE: If you do not remove the jumper, the Cisco IMC clears the CMOS settings each time that you boot the server node.

10. Install the server node cover, and then install server node back to the system.
11. Power on the server node.

Related Documentation

- Cisco UCS S3260 Storage Server Installation and Service Guide
- Regulatory Compliance and Safety Information For Cisco UCS S-Series Hardware

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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.