Servicing the Blade Server

This chapter contains the following sections:

Removing a Blade Server Cover

Procedure

Step 1   Press and hold the button down as shown in the figure below.

Step 2   While holding the back end of the cover, pull the cover back and then up.

Drive Replacement

You can remove and install hard drives without removing the blade server from the chassis.

The drives supported in this blade server come with the drive sled attached. Spare drive sleds are not available. A list of currently supported drives is in the Cisco UCS B420 M4 Blade Server Specification Sheet.

Before upgrading or adding a drive to a running blade server, check the service profile in Cisco UCS Manager and make sure the new hardware configuration will be within the parameters allowed by the service profile.

⚠️

Caution   To prevent ESD damage, wear grounding wrist straps during these procedures.

✎

Note   See also 4K Sector Format SAS/SATA Drives Considerations, on page 3.

Removing a Blade Server Hard Drive

To remove a hard drive from a blade server, follow these steps:

Procedure

Step 1   Push the button to release the ejector, and then pull the hard drive from its slot.

Step 2   Place the hard drive on an antistatic mat or antistatic foam if you are not immediately reinstalling it in another server.

Step 3   Install a hard disk drive blank faceplate to keep dust out of the blade server if the slot will remain empty.

Installing a Blade Server Drive

To install a drive in a blade server, follow these steps:

Procedure

Step 1   Place the drive ejector into the open position by pushing the release button.

Step 2   Gently slide the drive into the opening in the blade server until it seats into place.

Step 3   Push the drive ejector into the closed position.

You can use Cisco UCS Manager to format and configure RAID services. For details, see the *Configuration Guide* for the version of Cisco UCS Manager that you are using. The configuration guides are available at the following URL:
http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

If you need to move a RAID cluster, see the Cisco UCS Manager Troubleshooting Reference Guide.

4K Sector Format SAS/SATA Drives Considerations

- You must boot 4K sector format drives in UEFI mode, not legacy mode. See the procedure in this section for setting UEFI boot mode in the boot policy.

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

- Operating system support on 4K sector drives is as follows: Windows: Win2012 and Win2012R2; Linux: RHEL 6.5, 6.6, 6.7, 7.0, 7.2, 7.3; SLES 11 SP3, and SLES 12. ESXi/VMWare is not supported.

Setting Up UEFI Mode Booting in the UCS Manager Boot Policy

Procedure

Step 1 In the Navigation pane, click **Servers**.

Step 2 Expand **Servers > Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the root node.

Step 4 Right-click **Boot Policies** and select **Create Boot Policy**.

The Create Boot Policy wizard displays.

Step 5 Enter a unique name and description for the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period). You cannot change this name after the object is saved.

Step 6 (Optional) After you make changes to the boot order, check the **Reboot on Boot Order Change** check box to reboot all servers that use this boot policy.

For boot policies applied to a server with a non-Cisco VIC adapter, even if the Reboot on Boot Order Change check box is not checked, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.

Step 7 (Optional) If desired, check the **Enforce vNIC/vHBA/iSCSI Name** check box.

- If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the Boot Order table match the server configuration in the service profile.

- If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.

Step 8 In the **Boot Mode** field, choose the **UEFI** radio button.

Step 9 Check the Boot Security check box if you want to enable UEFI boot security.

Step 10 Configure one or more of the following boot options for the boot policy and set their boot order:

- Local Devices boot—To boot from local devices, such as local disks on the server, virtual media, or remote virtual disks, continue with *Configuring a Local Disk Boot for a Boot Policy* in the Cisco UCS Manager Server Management Guide for your release.

- SAN boot—To boot from an operating system image on the SAN, continue with *Configuring a SAN Boot for a Boot Policy* in the Cisco UCS Manager Server Management Guide for your release.

You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

- LAN boot—To boot from a centralized provisioning server, continue with *Configuring a LAN Boot For a Boot Policy* in the Cisco UCS Manager Server Management Guide for your release.

- iSCSI boot—To boot from an iSCSI LUN, continue with *Creating an iSCSI Boot Policy* in the Cisco UCS Manager Server Management Guide for your release.

Air Baffles

The air baffles shown below ship with this server; they direct and improve air flow for the server components. No tools are necessary to install them. Place them over the DIMMs and align them to the standoffs.
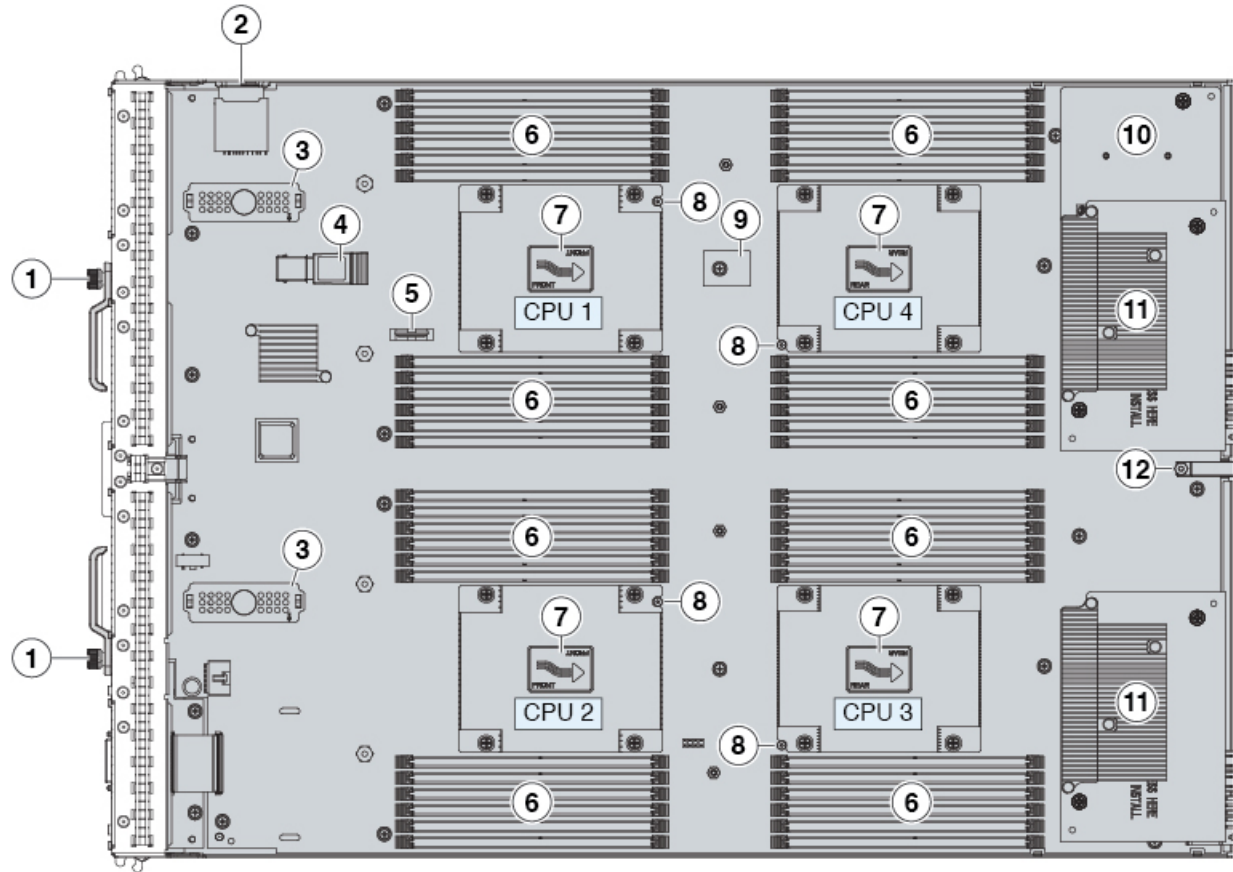
⚠

Caution   Be sure that the tabs on the baffles are set in the slots provided on the motherboard; otherwise, it may be difficult to replace the server cover or damage to the motherboard might occur.

Internal Components

Figure 1: Inside View of the Blade Server

1	Ejector captive screw	7	Heat sink and CPU (underneath)
2	SD card slots	8	CPU heat sink install guide pins
3	Modular storage subsystem connector	9	Trusted Platform Module (TPM)
4	USB memory	10	Adapter 1 supports only the Cisco VIC 1340 adapter and the Cisco VIC 1240 adapter
5	CMOS battery	11	Adapter cards: • Adapter 2 is the slot on the left (facing the server) and partially covers Adapter 1 • Adapter 3 is the slot on the right (facing the server)
6	DIMM slots	12	Diagnostic button

Note The heat sinks and CPUs are numbered as follows:

- Left front heat sink and CPU 1
- Right front heat sink and CPU 2
- Right rear heat sink and CPU 3
- Left rear heat sink and CPU 4

Diagnostics Button and LEDs

At blade start-up, POST diagnostics test the CPUs, DIMMs, HDDs, and adapter cards, and any failure notifications are sent to UCS Manager. You can view these notifications in the Cisco UCS Manager System Error Log or in the output of the **show tech-support** command. If errors are found, an amber diagnostic LED also lights up next to the failed component. During run time, the blade BIOS and component drivers monitor for hardware faults and will light up the amber diagnostic LED as needed.

LED states are saved, and if you remove the blade from the chassis the LED values will persist for up to 10 minutes. Press and hold the diagnostics button on the motherboard for 30 seconds to display component faults. LED fault values are reset when the blade is reinserted into the chassis and booted, and the process begins from its start.

If DIMM insertion errors are detected, they may cause the blade discovery process to fail and errors will be reported in the server POST information, which is viewable using the UCS Manager GUI or CLI. DIMMs must be populated according to specific rules. The rules depend on the blade server model. Refer to the Cisco UCS B420 M4 Blade Server Specification Sheet for the DIMM population rules.

Faults on the DIMMs or adapter cards also cause the server health LED to light solid amber for minor error conditions or blinking amber for critical error conditions.

Installing a CMOS Battery

All Cisco UCS blade servers use a CR2032 battery to preserve BIOS settings while the server is not installed in a powered-on chassis. Cisco supports the industry standard CR2032 battery that is available at most electronics stores.

Warning There is danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

To install or replace the battery, follow these steps:

Procedure

Step 1 Remove the existing battery:

a) Power off the blade, remove it from the chassis, and remove the top cover.

   b)   Push the battery socket retaining clip away from the battery.

   c)   Lift the battery from the socket. Use needle-nose pliers to grasp the battery if there is not enough clearance for your fingers.

Step 2   Install the replacement battery:

   a)   Push the battery socket retaining clip away from where the battery fits in the housing.

   b)   Insert the new battery into the socket with the battery's positive (+) marking facing away from the retaining clip. Ensure that the retaining clip can click over the top of the battery to secure it in the housing.

   c)   Replace the top cover.

   d)   Replace the blade server in the chassis.

Installing a Modular Storage Subsystem

The UCS B420 M4 Blade Server uses an optional Cisco UCS FlexStorage modular storage subsystem that can provide support for two drive bays and RAID controller.

Figure 2: Modular Storage System Installation
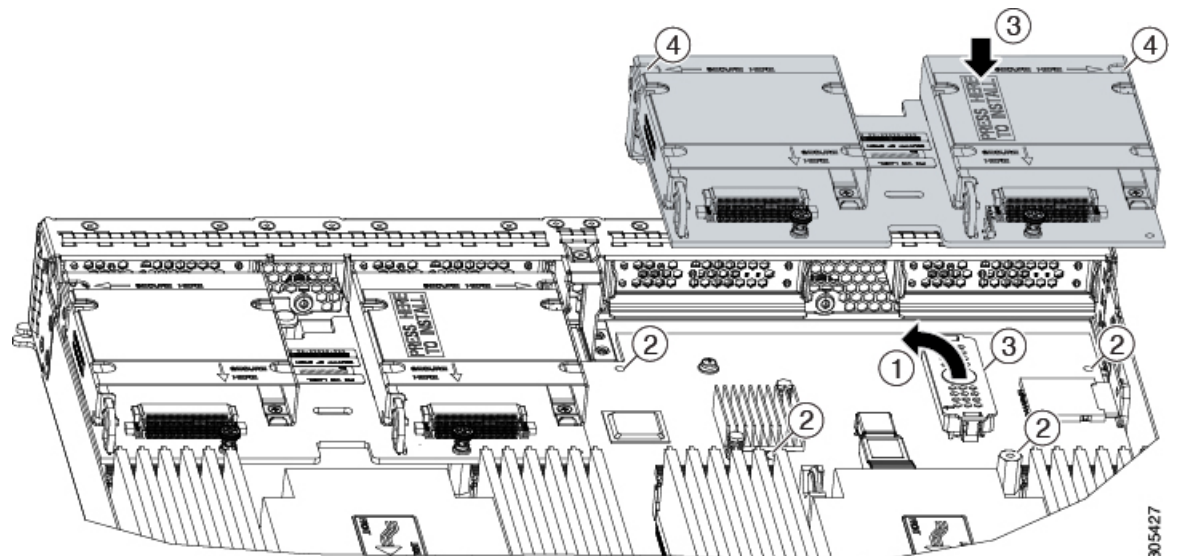
Procedure

Step 1   Remove the protective cover on the connector from both the modular storage subsystem and the motherboard.

Step 2   Position the modular storage subsystem connector above the motherboard connector and align the captive screws to the standoffs and the motherboard mounting holes.

Step 3   Press the modular storage subsystem where the label states "PRESS HERE TO INSTALL" onto the motherboard connector.

Step 4   Tighten the screws.

Replacing the SuperCap Module

The SuperCap module is a battery bank which connects to the front mezzanine storage module board and provides power to the RAID controller if facility power is interrupted.

To replace the SuperCap module, use the following topics:

Removing the SuperCap Module

The SuperCap module sits in a plastic tray. The module connects to the board through a ribbon cable with one connector to the module and one connector to the board. The SuperCap replacement PID (UCSB-MRAID-SC=) contains the module only, so you must leave the ribbon cable in place on the board.

⚠️

Caution　When disconnecting the SuperCap module, disconnect the ribbon cable from the module only. Do not disconnect the cable from the board. The board connection and the tape that secures the cable must remain connected and undamaged.

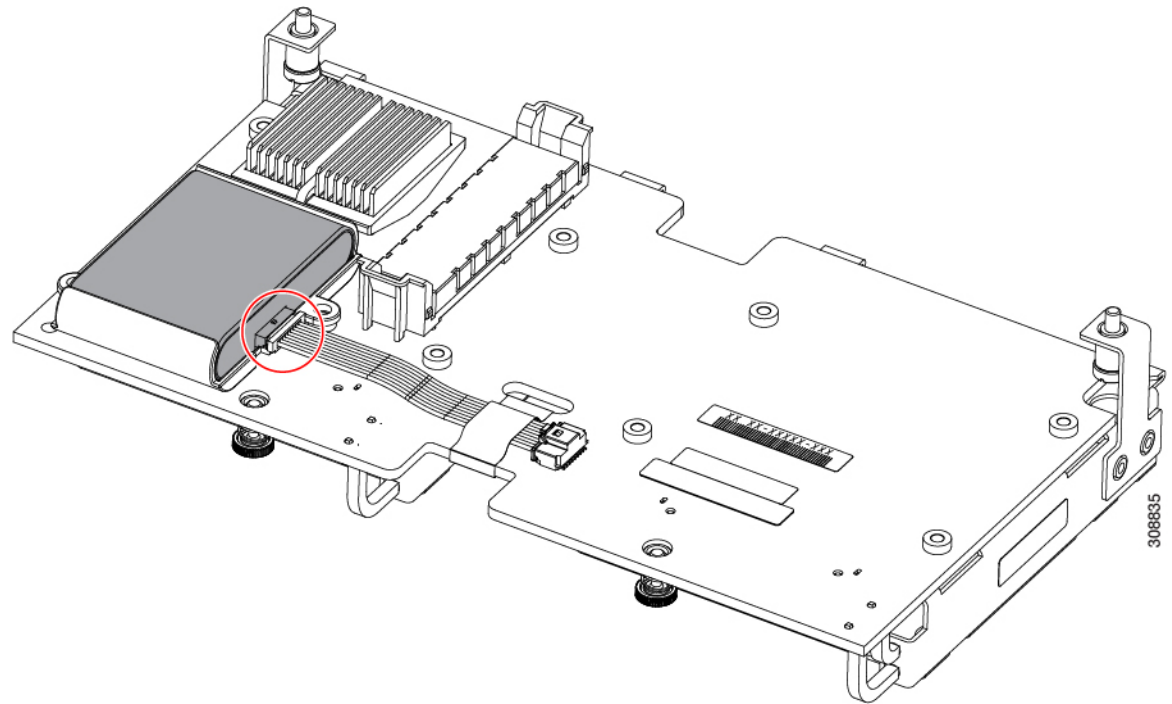To replace the SuperCap module, follow these steps:

Procedure

Step 1　Grasp the cable connector at the SuperCap module and gently pull to disconnect the cable from the SuperCap module.

Do not grasp the cable itself, the tape, or the board connector.

Figure 3: Disconnecting the SuperCap Cable from the Module, Not the Board

Step 2   Before removing the SuperCap module, note its orientation in the tray.

When correctly oriented, the connector is on the bottom half of the module and faces the cable. You will need to install the new SuperCap module with the same orientation.

Step 3   Grasp the sides of the SuperCap module, but not the connector, and lift the SuperCap module out of the tray.

Figure 4: Removing the SuperCap Module
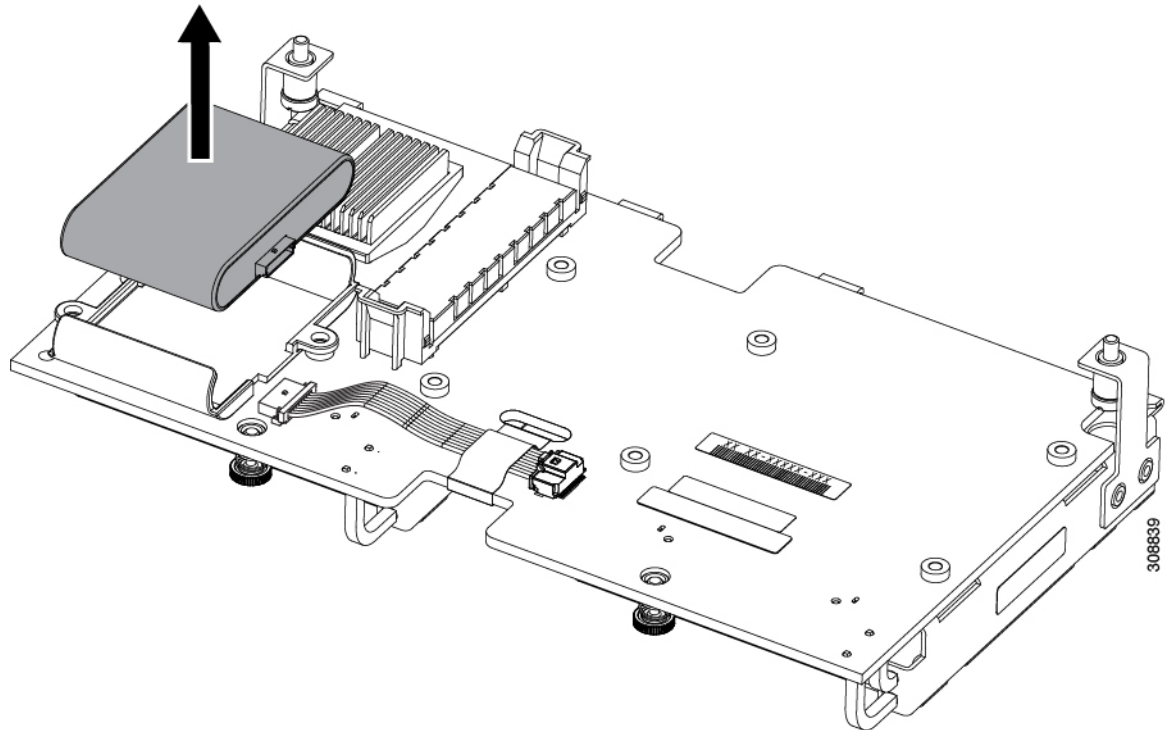
You might feel some resistance because the tray is curved to secure the module.

Installing the SuperCap Module

To install a SuperCap module (UCSB-MRAID-SC=), use the following steps:

Procedure

Step 1   Orient the SuperCap module correctly, as shown (1).

When correctly oriented:

- The connector is on the bottom half of the module facing the cable.

- The connector will fit into the rectangular notch in the tray. This notch is specifically designed to accept the SuperCap module connector.

Caution   Make sure the SuperCap module is properly oriented before proceeding. If the module is installed incorrectly, the ribbon cable can get snagged or damaged.

Step 2   When the module is correctly oriented, lower the module and press down until it clips into the tray.

You might feel some resistance while the module passes the curved clips at the top of the tray.

Figure 5: Orienting and Installing the SuperCap Module
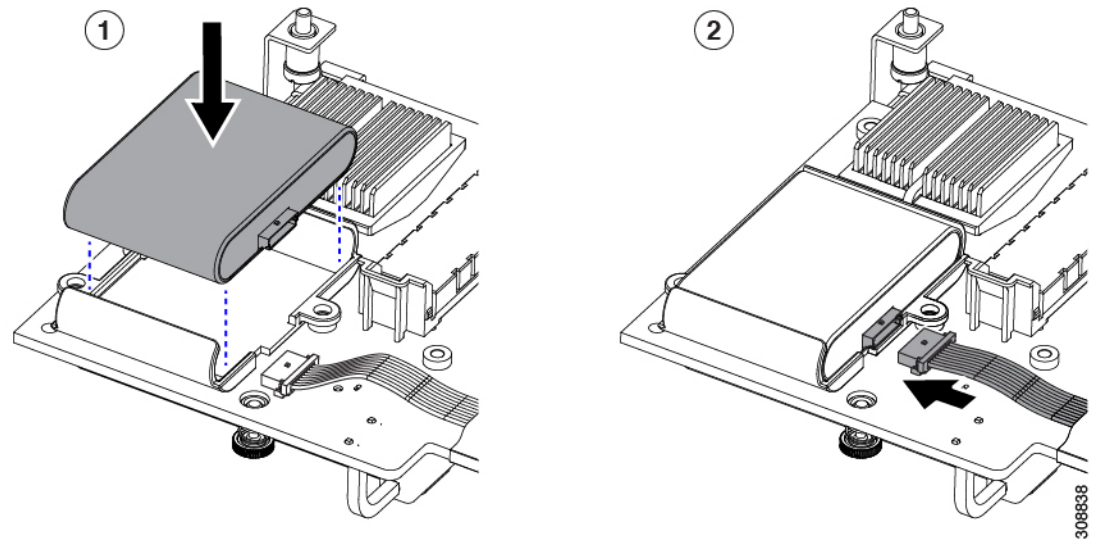
Step 3 When the module is seated in the tray, reconnect the cable (2):

a) Grasp the cable connector and verify that the pins and sockets on the cable connector and module connector are correctly aligned.

b) When the cable connector and module connector are properly aligned, plug the cable into the SuperCap module.

What to do next

Reinstall the blade server. Go to Installing a Blade Server.

Upgrading to Intel Xeon E5-4600 v4 Series CPUs

Before upgrading to Intel Xeon E5-4600 v4 Series CPUs, ensure that the server is running the required minimum software and firmware versions that support Intel E5-4600 v4 Series CPUs, as listed in the following table.

Software or Firmware	Minimum Version
Cisco UCS Manager	Release 3.1(2) or Release 2.2(8) (See the following Note for additional supported versions.)
Cisco IMC	Release 3.1(2) or Release 2.2(8)
BIOS	Release 3.1(2) or Release 2.2(8)

Note   Cisco UCS Manager Release 2.2(4) introduced a server pack feature that allows Intel E5-4600 v4 CPUs to run with Cisco UCS Manager Release 2.2(4) or later, provided that the Cisco IMC, BIOS and Capability Catalog are all running Release 2.2(8) or later.

Caution   Ensure that the server is running the required software and firmware before installing the Intel E5-4600 v4 Series CPUs. Failure to do so can result in a non-bootable CPU.

Do one of the following actions:

- If the server software and firmware are already at the required minimum version as shown in the preceding table, replace the CPUs by using the procedure in the following section.
- If the server software or firmware is not at the required minimum version, follow the instructions in the Cisco UCS B420 M4 Server Upgrade Guide for E5-4600 v4 Series CPUs to upgrade it. Then replace the CPUs by using the procedure in the following section.

- For PID information when re-using or using new CPUs and heat sinks, see

Rules for Replacing CPUs and Heat Sinks

If you re-use both CPUs and heat sinks when replacing the motherboard, the following PIDs are used:

- UCSX-HSCK=
- UCS-CPU-GREASE=

When you replace CPUs and use new heat sinks that you ordered, the following PIDs are used:

- UCSB-HS-EP-M4-F= CPU Heat Sink for UCS B200/B420M4 Socket 1 (Front)

- UCSB-HS-EP-M4-R= CPU Heat Sink for UCS B200/B420M4 Socket 2 (Rear)
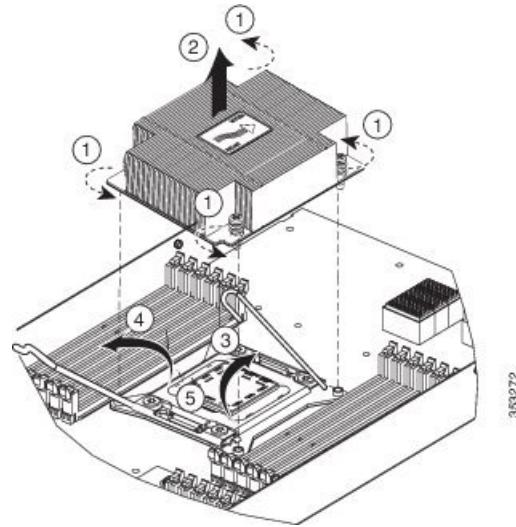- UCS-CPU-GREASE3=

Removing a Heat Sink and CPU

Before beginning this procedure, you may find it helpful to review the conditions in Rules for Replacing CPUs and Heat Sinks, on page 12.

**Procedure**

Step 1   Unscrew the four captive screws.

Step 2   Remove the heat sink.

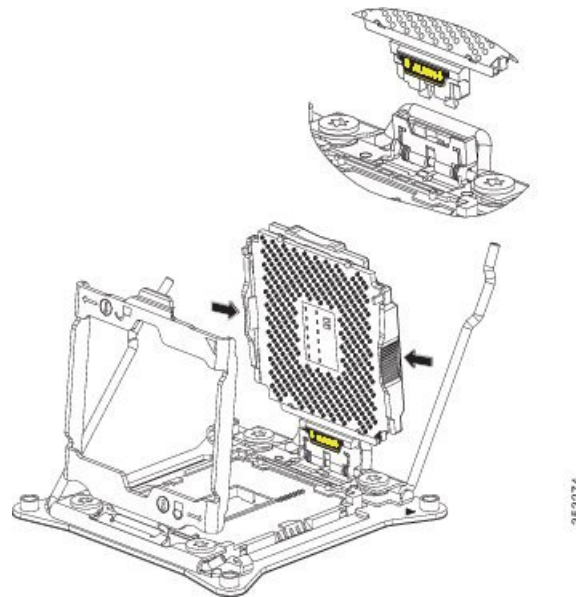*Figure 6: Removing the Heat Sink and CPU*

Step 3   Unhook the self-loading socket (SLS) lever that has the unlock icon ⊐⌒.

Step 4   Unhook the SLS lever that has the lock icon ⊖.

Step 5   Grasp the sides of the CPU carrier (indicated by the arrows in the illustration) and swing it into a standing position in the SLS plug seat.

Figure 7: CPU Carrier and SLS Plug Seat

Step 6   Pull the CPU carrier up and out of the SLS plug seat.

Installing a New CPU and Heat Sink

Before installing a new CPU in a server, verify the following:

- A BIOS update is available and installed that supports the CPU and the given server configuration.

- The service profile for this server in Cisco UCS Manager will recognize and allow the new CPU.

Procedure

Step 1   Hold the CPU carrier by its sides (indicated by the arrows). Insert and align the two CPU carrier pegs into the self-loading socket (SLS) plug seat. To ensure proper seating, verify that the horizontal yellow line below the word ALIGN is straight.

Figure 8: Inserting the CPU Carrier
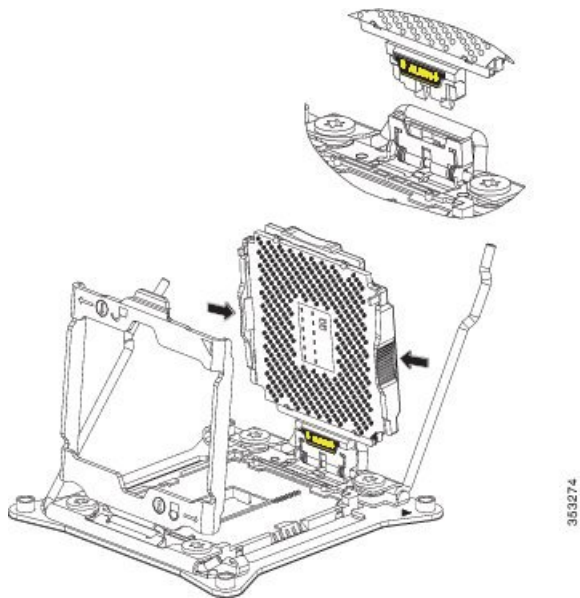
Step 2   Press gently on the top of the CPU carrier from the exterior side until it snaps into place.

Step 3   Close the socket latch.

**Step 4**   Hook the self-loading socket (SLS) lever that has the lock icon 🔒.

**Step 5**   Hook the SLS lever that has the unlock icon 🔓.

Step 6   Thermally bond the CPU and heat sink. Using the syringe of thermal grease provided with the replacement CPU, apply 2 cubic centimeters of thermal grease to the top of the CPU where it will contact the heat sink. Apply the grease in the pattern shown in the following figure, which should use approximately half the contents of the syringe.

Figure 9: Thermal Grease Application Pattern
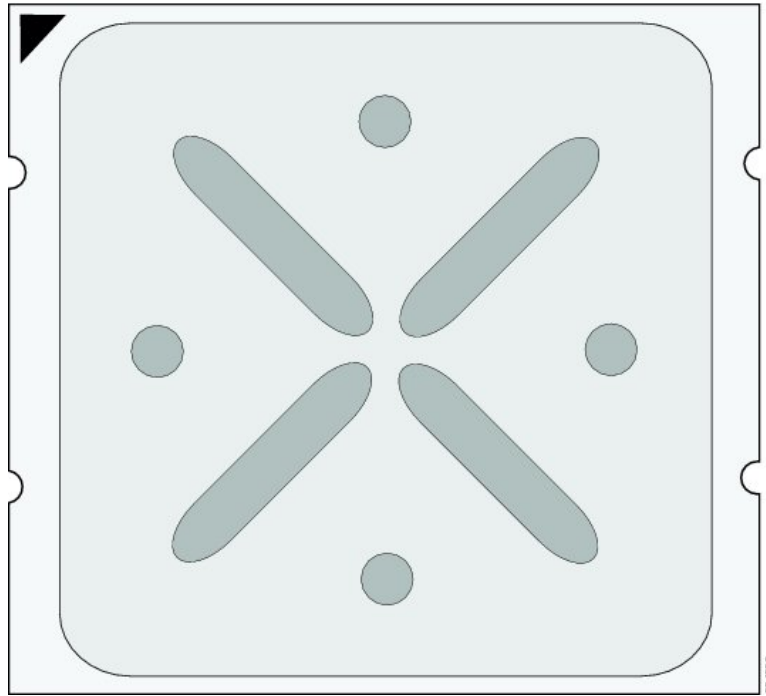
Step 7   Replace the heat sink. The yellow CPU heat sink install guide pins that are attached to the motherboard must align with the cutout on the heat sink to ensure proper installation of the heat sink.

Figure 10: Replacing the Heat Sink
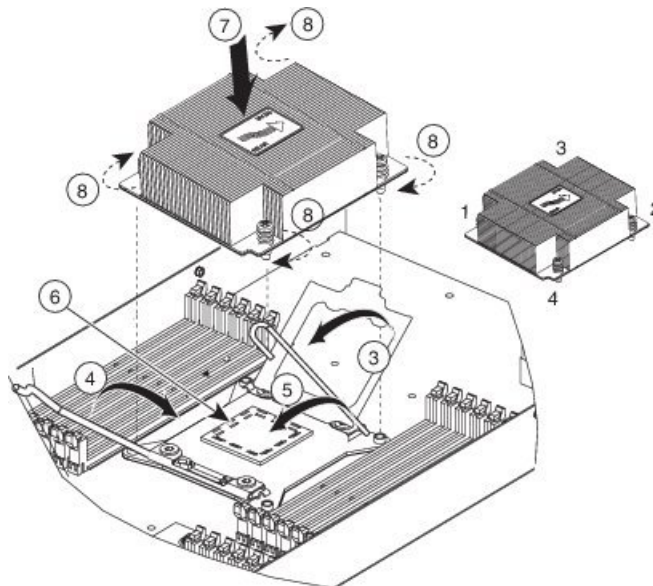
Step 8   Tighten the four captive screws in the order shown.

Installing Memory

To install a DIMM into the blade server, follow these steps:

Procedure

Step 1 Press the DIMM into its slot evenly on both ends until it clicks into place.

DIMMs are keyed. If a gentle force is not sufficient, make sure the notch on the DIMM is correctly aligned.

Note Be sure that the notch in the DIMM aligns with the slot. If the notch is misaligned you may damage the DIMM, the slot, or both.

Step 2 Press the DIMM connector latches inward slightly to seat them fully.

Supported DIMMs

The DIMMs supported in this blade server are constantly being updated. A list of currently supported and available DIMMs is in the Cisco UCS B420 M4 Blade Server Specification Sheet.

Do not use any memory DIMMs other than those listed in the specification sheet. Doing so may irreparably damage the server and require down time.

Memory Arrangement

The Cisco UCS B420 high-performance blade server contains 48 slots for installing DIMMs—12 for each CPU. Each CPU has 12 DIMM slots spread over 4 channels. This blade server needs at least one DIMM attached to all populated CPUs. DIMMs installed in slots for an absent CPU will not be recognized. For optimal performance, distribute DIMMs evenly across all CPUs. DIMM connector latches are color coded blue, black, and white, and the DIMMs must be installed in that order.

Figure 11: Memory Slots Within the Blade Server
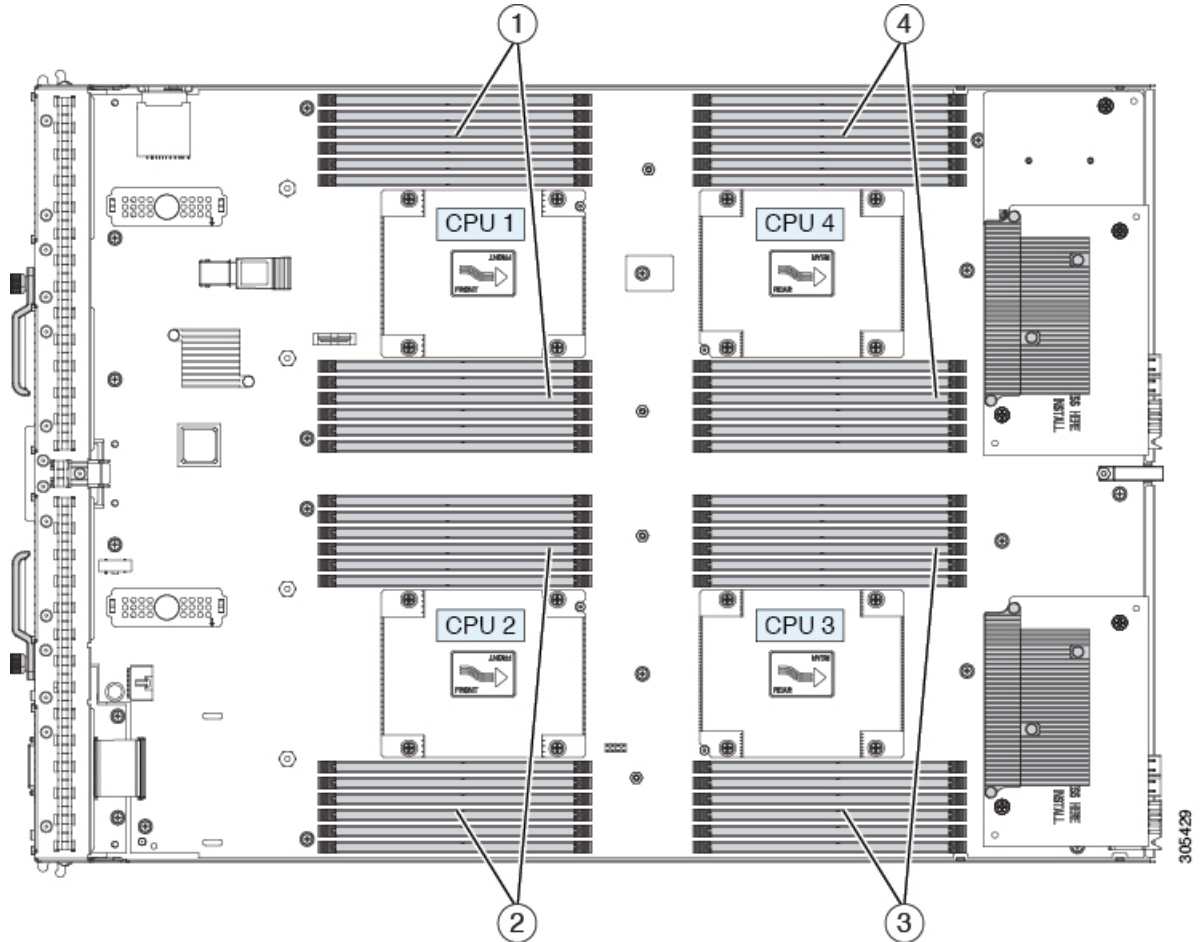
1	DIMMs for CPU 1	3	DIMMs for CPU 3
2	DIMMs for CPU 2	4	DIMMs for CPU 4

Channels

Each CPU has 4 channels, consisting of 3 DIMMs. Each channel is identified by a letter. Each channel member is identified by numbers, 1, 2 or 3.

The DIMM slots are contiguous to their associated CPU. When installing DIMMs, you must add them in the configurations shown in the following table.

Table 1: UCS B420 M4 DIMM Slot Population

DIMMs per CPU	Populate CPU 1 Slots	Populate CPU 2 Slots	Populate CPU 3 Slots	Populate CPU 4 Slots	Color Coding
1	A1	E1	I1	M1	Blue

DIMMs per CPU	Populate CPU 1 Slots	Populate CPU 2 Slots	Populate CPU 3 Slots	Populate CPU 4 Slots	Color Coding
2	A1, B1	E1, F1	I1, J1	M1, N1	Blue
3	A1, B1, C1	E1, F1, G1	I1, J1, K1	M1, N1, O1	Blue
4	A1, B1, C1, D1	E1, F1, G1, H1	I1, J1, K1, L1	M1, N1, O1, P1	Blue
5	Not recommended for performance reasons.				
6	A1, B1, C1, A2, B2, C2	E1, F1, G1, E2, F2, G2	I1, J1, K1, I2, J2, K2	M1, N1, O1, M2, N2, O2	Blue, Black
7	Not recommended for performance reasons.				
8	A1, B1, C1, D1, A2, B2, C2, D2	E1, F1, G1, H1, E2, F2, G2, H2	I1, J1, K1, L1, I2, J2, K2, L2	M1, N1, O1, P1, M2, N2, O2, P2	Blue, Black
9	A1, B1, C1, A2, B2, C2, A3, B3, C3	E1, F1, G1, E2, F2, G2, E3, F3, G3	I1, J1, K1, I2, J2, K2, I3, J3, K3	M1, N1, O1, M2, N2, O2, M3, N3, O3	Blue, Black, White
10	Not recommended for performance reasons.				
11	Not recommended for performance reasons.				
12	A1, B1, C1, D1, A2, B2, C2, D2, A3, B3, C3, D3	E1, F1, G1, H1, E2, F2, G2, H2, E3, F3, G3, H3	I1, J1, K1, L1, I2, J2, K2, L2, I3, J3, K3, L3	M1, N1, O1, P1, M2, N2, O2, P2, M3, N3, O3, P3	Blue, Black, White

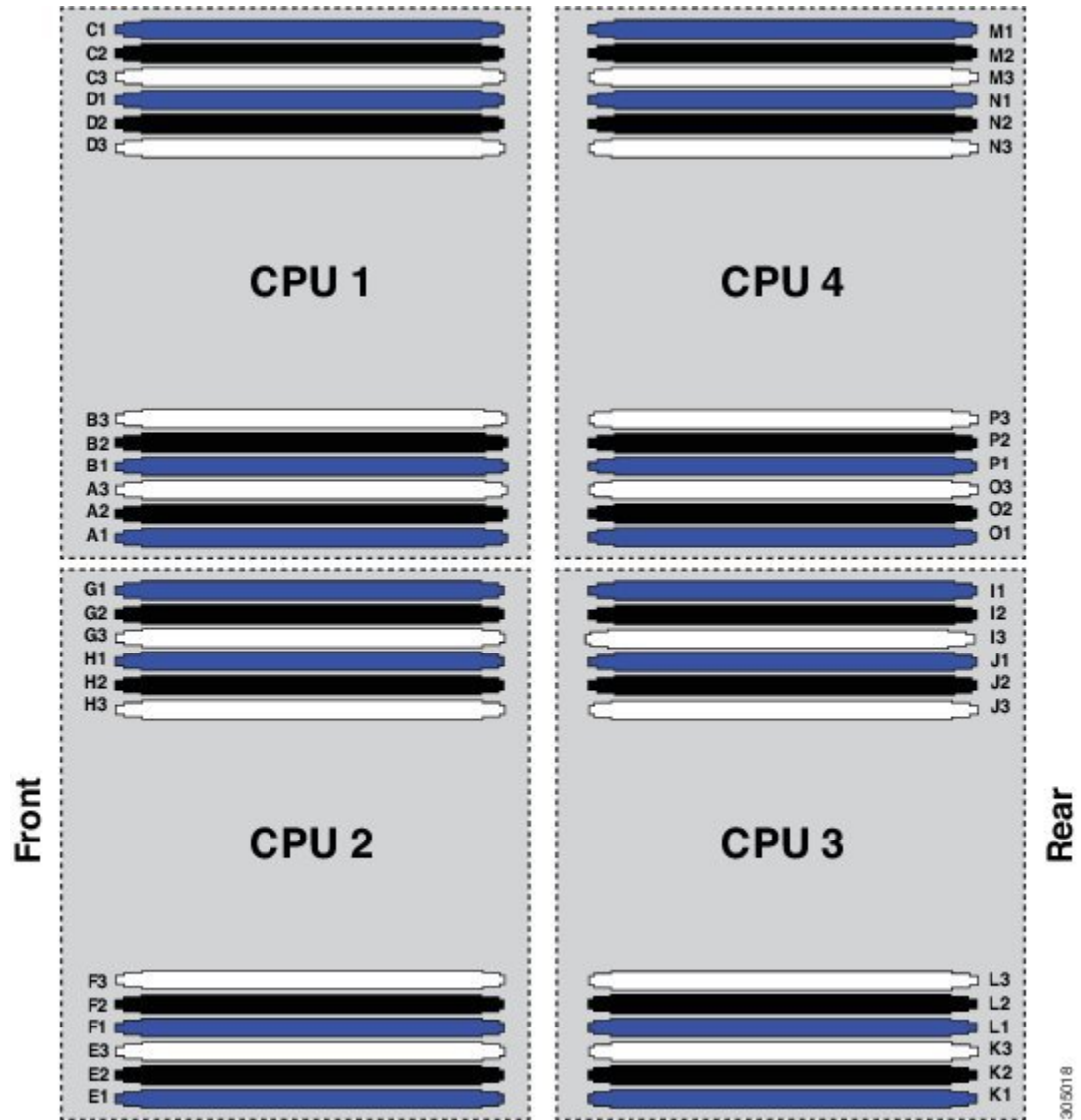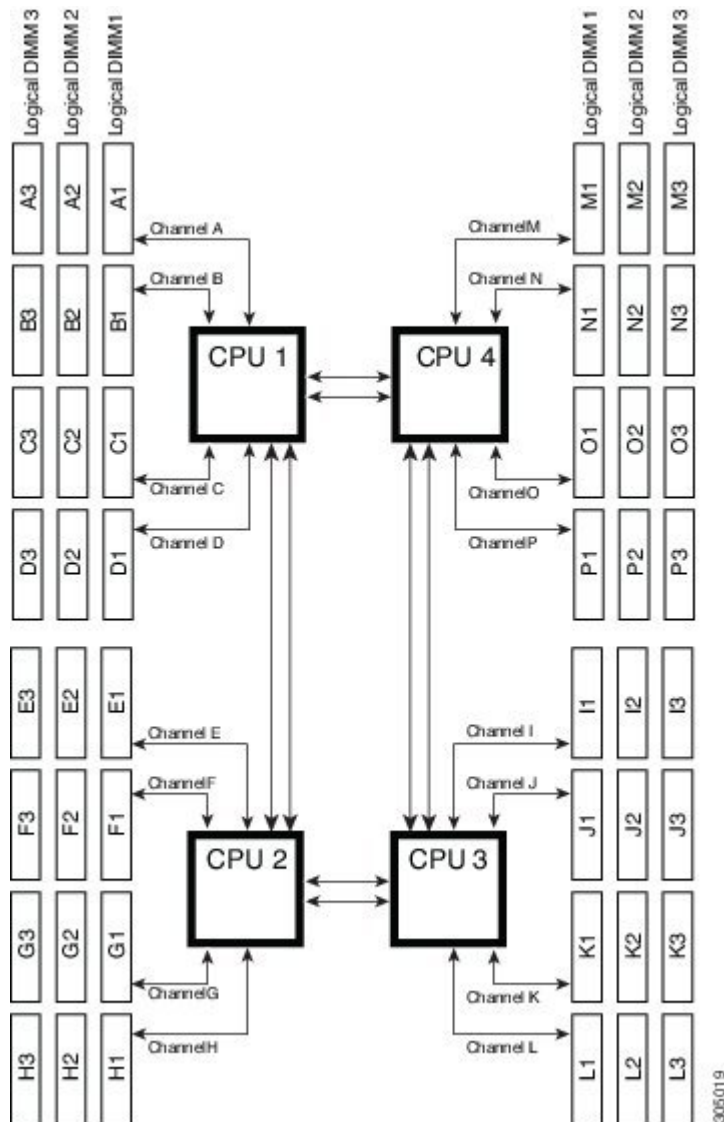*Figure 12: Physical Representation of DIMMs and CPUs*

Figure 13: Logical Representation of Channels

Memory Performance

When configuring your server, consider the following:

- DIMMs within the blade can be of different speeds, but all DIMMs will run at the speed of the DIMM with the lowest speed.

- No mixing of DIMM type (LRDIMM, RDIMM, TSV-RDIMM) is allowed.

- Your selected CPU(s) can have some affect on performance. CPUs used must be of the same type.

- Mixing DIMM ranks and densities can lower performance.

- Unevenly populating DIMMs between CPUs can lower performance.

Installing a Virtual Interface Card Adapter

**Note**   You must remove the adapter card to service it.

To install a Cisco VIC 1340 or VIC 1240 in the blade server, follow these steps:

Procedure

Step 1   Position the VIC board connector above the motherboard connector and align the captive screw to the standoff post on the motherboard.

Step 2   Firmly press the VIC board connector into the motherboard connector.

Step 3   Tighten the captive screw.

Tip   To remove a VIC, reverse the above procedure. You might find it helpful when removing the connector from the motherboard to gently rock the board along the length of the connector until it loosens.

Figure 14: Installing a VIC mLOM Adapter
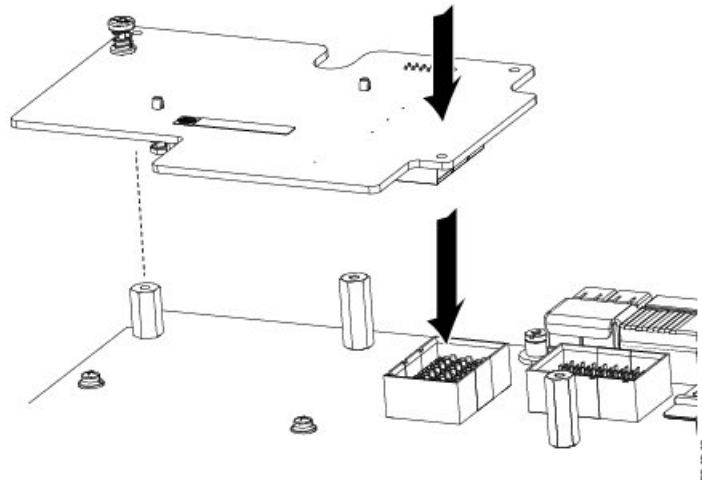
Installing an Adapter Card in Slots 2 or 3

The network adapters and interface cards share a common installation process. These cards are updated frequently. Currently supported models that are available for this server are listed in the specification sheets at this URL:

http://www.cisco.com/en/US/products/ps10280/products_data_sheets_list.html

- Adapter slot 1 (4 x 10 Gb) is for the VIC 1340 or VIC 1240 adapter. No other adapter card can be installed in slot 1.

- Adapter slot 2 (4 x 10 Gb) is for the VIC port expander card or the storage accelerator cards. The port expander can only be used if the VIC 1340 or VIC 1240 is installed.

- Adapter slot 3 (8 x 10 Gb) is for the VIC 1380 or VIC 1280 adapter or the storage accelerator cards.

The VIC 1340 and VIC 1380 adapters require a Cisco UCS 6200 Series Fabric Interconnect or Cisco UCS 6300 Series Fabric Interconnect, and they support the Cisco Nexus 2208XP, 2204XP, and 2348UPQ Fabric Extender (FEX) modules.

The VIC 1240 and VIC 1280 adapters support Cisco UCS 6100, 6200, and 6300 Series Fabric Interconnects, and they support the Cisco Nexus 2104XP, 2204XP, 2208XP, and 2304XP FEX modules.

If you switch from one type of adapter card to another, download the latest device drivers and load them into the server's operating system before you physically switch the adapters. For more information, see the firmware management chapter of one of the Cisco UCS Manager software configuration guides.

Procedure

Step 1   Position the adapter board connector above the motherboard connector and align the two adapter captive screws to the standoff posts on the motherboard (callout 1).

Step 2   Firmly press the adapter connector into the motherboard connector (callout 2).

Step 3   Tighten the captive screws (callout 3).

Figure 15: Installing an Adapter Card
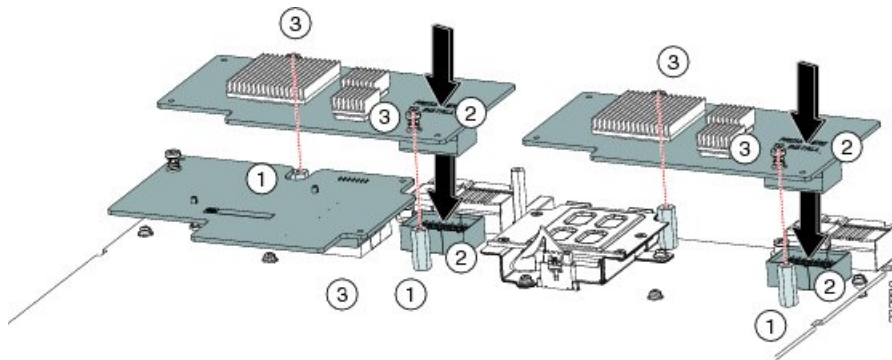

Enabling the Trusted Platform Module

The Trusted Platform Module (TPM) is a component that can securely store artifacts used to authenticate the server. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.

It is a requirement for the Intel Trusted Execution Technology (TXT) security feature, which must be enabled in the BIOS settings for a server equipped with a TPM.

Procedure

Step 1   Install the TPM hardware.

a)   Decommission and remove the blade server from the chassis.

b)   Remove the blade server cover.

c)   Install the TPM to the TPM socket on the server motherboard and secure it using the one-way screw that is provided. See the figure below for the location of the TPM socket.

d)   Return the blade server to the chassis and allow it to be automatically reacknowledged, reassociated, and recommissioned.

e)   Continue with enabling TPM support in the server BIOS in the next step.

Figure 16: TPM Socket
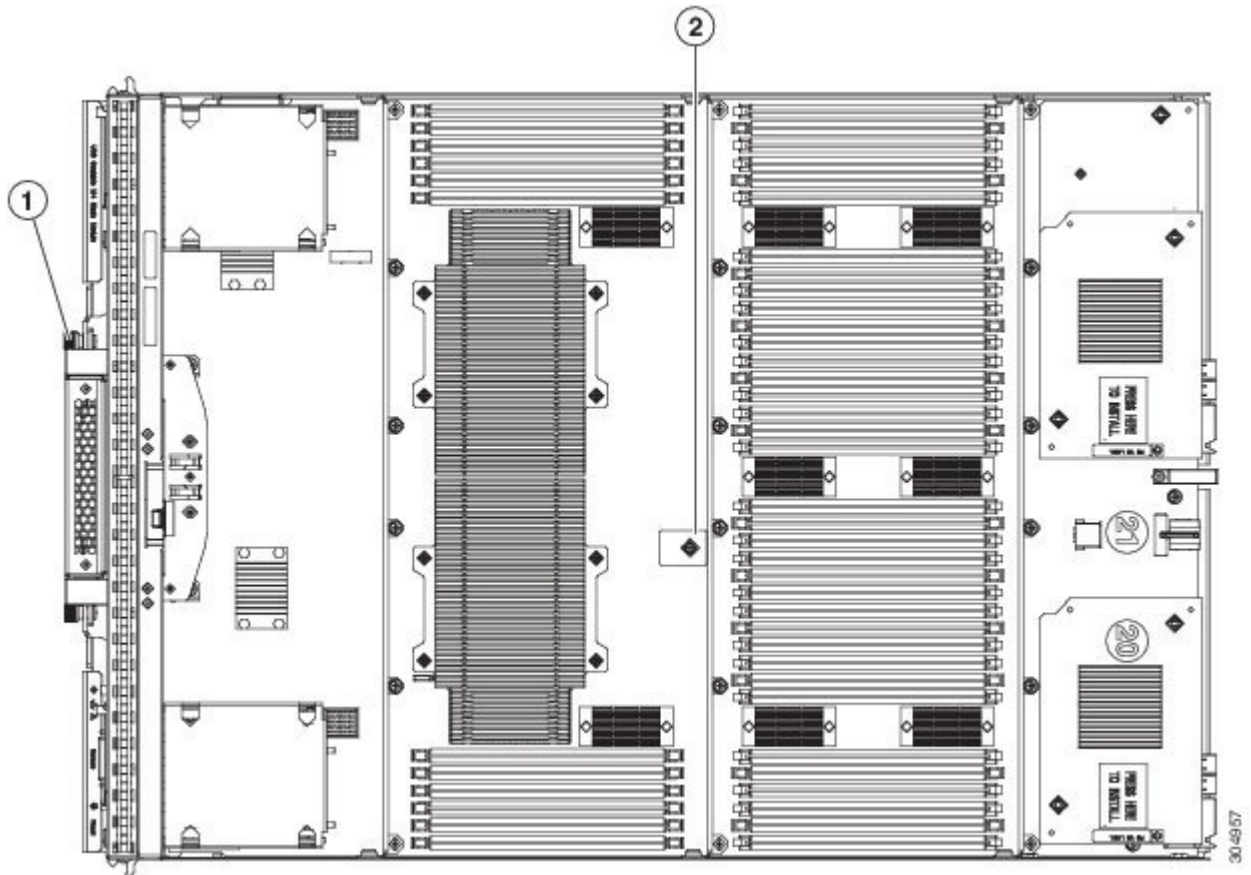
Step 2   Enable TPM Support in the BIOS.

If TPM support was disabled for any reason, use the following procedure to enable it.

a)   In the Cisco UCS Manager Navigation pane, click the **Servers** tab.

b)   On the Servers tab, expand **Servers > Policies**.

c)   Expand the node for the organization where you want to configure the TPM.

d) Expand BIOS Policies and select the BIOS policy for which you want to configure the TPM.

e) In the Work pane, click the **Advanced** tab.

f) Click the **Trusted Platform** sub-tab.

g) To enable TPM support, click **Enable** or **Platform Default.**

h) Click **Save Changes**.

i) Continue with the next step.

Step 3 Enable TXT Support in the BIOS Policy.

Follow the procedures in the Cisco UCS Manager Configuration Guide for the release that is running on the server.