Monitoring Hardware

This chapter includes the following sections:

- Monitoring a Fabric Interconnect, page 1
- Monitoring a Chassis, page 2
- Monitoring a Blade Server, page 4
- Monitoring a Rack-Mount Server, page 6
- Monitoring an I/O Module, page 8
- Monitoring Management Interfaces, page 9
- Health Monitoring, page 13
- Local Storage Monitoring, page 16
- Graphics Card Server Support, page 19
- Managing Transportable Flash Module and Supercapacitor, page 20
- TPM Monitoring, page 22

Monitoring a Fabric Interconnect

Procedure

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

Step 2 Expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the node for the fabric interconnect that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the fabric interconnect:

Option	Description
General tab	Provides an overview of the status of the fabric interconnect, including a summary of any faults, a summary of the fabric interconnect properties, and a physical display of the fabric interconnect and its components.

Option	Description
Physical Ports tab	Displays the status of all ports on the fabric interconnect. This tab includes the following subtabs: • **Uplink Ports** tab • **Server Ports** tab • **Fibre Channel Ports** tab • **Unconfigured Ports** tab
Fans tab	Displays the status of all fan modules in the fabric interconnect.
PSUs tab	Displays the status of all power supply units in the fabric interconnect.
Physical Display tab	Provides a graphical view of the fabric interconnect and all ports and other components. If a component has a fault, the fault icon is displayed next to that component.
Faults tab	Provides details of faults generated by the fabric interconnect.
Events tab	Provides details of events generated by the fabric interconnect.
Statistics tab	Provides statistics about the fabric interconnect and its components. You can view these statistics in tabular or chart format.

Monitoring a Chassis

Tip To monitor an individual component in a chassis, expand the node for that component.

Procedure

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

Step 2 Expand **Equipment** > **Chassis**.

Step 3 Click the chassis that you want to monitor.

Step 4 Click one of the following tabs to view the status of the chassis:

Option	Description
General tab	Provides an overview of the status of the chassis, including a summary of any faults, a summary of the chassis properties, and a physical display of the chassis and its components.

Option	Description
Servers tab	Displays the status and selected properties of all servers in the chassis.
Service Profiles tab	Displays the status of the service profiles associated with servers in the chassis.
IO Modules tab	Displays the status and selected properties of all IO modules in the chassis.
Fans tab	Displays the status of all fan modules in the chassis.
PSUs	Displays the status of all power supply units in the chassis.
Hybrid Display tab	Displays detailed information about the connections between the chassis and the fabric interconnects. The display has an icon for the following: • Each fabric interconnect in the system • The I/O module (IOM) in the selected component, which is shown as an independent unit to make the connection paths easier to see • The selected chassis showing the servers and PSUs, or the selected rack server.
Slots tab	Displays the status of all slots in the chassis.
Installed Firmware tab	Displays the current firmware versions on the IO modules and servers in the chassis. You can also use this tab to update and activate the firmware on those components.
SEL Logs tab	Displays and provides access to the system event logs for the servers in the chassis.
Power Control Monitor tab	Provides details of the power group, chassis, and servers.
Connectivity Policy tab	Provides details of the chassis ID, fabric ID, and connectivity type for the fabric.
Faults tab	Provides details of faults generated by the chassis.
Events tab	Provides details of events generated by the chassis.
FSM tab	Provides details about and the status of FSM tasks related to the chassis. You can use this information to diagnose errors with those tasks.
Statistics tab	Provides statistics about the chassis and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Provides temperature statistics for the components of the chassis. You can view these statistics in tabular or chart format.

Option	Description
Power tab	Provides power statistics for the components of the chassis. You can view these statistics in tabular or chart format.

Monitoring a Blade Server

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the server:

Option	Description
General tab	Provides an overview of the status of the server, including a summary of any faults, a summary of the server properties, and a physical display of the server and its components.

Option	Description
Inventory tab	Provides details about the properties and status of the components of the server on the following subtabs: • **Motherboard—**Information about the motherboard and information about the server BIOS settings. You can also recover corrupt BIOS firmware from this subtab. • **CIMC—**Information about the CIMC and its firmware, and provides access to the SEL for the server. You can also assign a static or pooled management IP address, and update and activate the CIMC firmware from this subtab. • **CPUs—**Information about each CPU in the server. • **Memory—**Information about each memory slot in the server and the DIMM in that slot. • **Adapters—**Information about each adapter installed in the server. • **HBAs—**Properties of each HBA and the configuration of that HBA in the service profile associated with the server. • **NICs—**Properties of each NIC and the configuration of that NIC in the service profile associated with the server. You can expand each row to view information about the associated VIFs and vNICs. • **iSCSI vNICs—**Properties of each iSCSI vNIC and the configuration of that vNIC in the service profile associated with the server. • **Storage—**Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server. **Tip** If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the **Vendor** field. However, Cisco UCS Manager CLI displays ATA in the **Vendor** field and includes the vendor information, such as the vendor name, in a **Vendor Description** field. This second field does not exist in Cisco UCS Manager GUI.
Virtual Machines tab	Displays details about any virtual machines hosted on the server.
Installed Firmware tab	Displays the firmware versions on the CIMC, adapters, and other server components. You can also use this tab to update and activate the firmware on those components.
SEL Logs tab	Displays the system event log for the server.
VIF Paths tab	Displays the VIF paths for the adapters on the server.
Faults tab	Displays an overview of the faults generated by the server. You can click any fault to view additional information.

Option	Description
Events tab	Displays an overview of the events generated by the server. You can click any event to view additional information.
FSM tab	Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.
Statistics tab	Displays statistics about the server and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.
Power tab	Displays power statistics for the components of the server. You can view these statistics in tabular or chart format.

Step 5 In the **Navigation** pane, expand ***Server_ID*** > **Adapters** > ***Adapter_ID*** .

Step 6 In the **Work** pane, right-click one or more of the following components of the adapter to open the navigator and view the status of the component:

- Adapters
- DCE interfaces
- HBAs
- NICs

Tip Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

Monitoring a Rack-Mount Server

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **Servers**.

Step 3 Click the server that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the server:

Option	Description
General tab	Provides an overview of the status of the server, including a summary of any faults, a summary of the server properties, and a physical display of the server and its components.

Option	Description
Inventory tab	Provides details about the properties and status of the components of the server on the following subtabs: • **Motherboard—**Information about the motherboard and information about the server BIOS settings. You can also recover corrupt BIOS firmware from this subtab. • **CIMC—**Information about the CIMC and its firmware, and provides access to the SEL for the server. You can also assign a static or pooled management IP address, and update and activate the CIMC firmware from this subtab. • **CPU—**Information about each CPU in the server. • **Memory—**Information about each memory slot in the server and the DIMM in that slot. • **Adapters—**Information about each adapter installed in the server. • **HBAs—**Properties of each HBA and the configuration of that HBA in the service profile associated with the server. • **NICs—**Properties of each NIC and the configuration of that NIC in the service profile associated with the server. You can expand each row to view information about the associated VIFs and vNICs. • **iSCSI vNICs—**Properties of each iSCSI vNIC and the configuration of that vNIC in the service profile associated with the server. • **Storage—**Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server. **Tip** If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the **Vendor** field. However, Cisco UCS Manager CLI displays ATA in the **Vendor** field and includes the vendor information, such as the vendor name, in a **Vendor Description** field. This second field does not exist in Cisco UCS Manager GUI.
Virtual Machines tab	Displays details about any virtual machines hosted on the server.
Installed Firmware tab	Displays the firmware versions on the CIMC, adapters, and other server components. You can also use this tab to update and activate the firmware on those components.
SEL Logs tab	Displays the system event log for the server.
VIF Paths tab	Displays the VIF paths for the adapters on the server.
Faults tab	Displays an overview of the faults generated by the server. You can click any fault to view additional information.

Option	Description
Events tab	Displays an overview of the events generated by the server. You can click any event to view additional information.
FSM tab	Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.
Statistics tab	Displays statistics about the server and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.
Power tab	Displays power statistics for the components of the server. You can view these statistics in tabular or chart format.

Step 5 In the **Navigation** pane, expand ***Server_ID*** > **Adapters** > ***Adapter_ID*** .

Step 6 In the **Work** pane, right-click one or more of the following components of the adapter to open the navigator and view the status of the component:

- Adapters
- DCE interfaces
- HBAs
- NICs

Tip Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

Monitoring an I/O Module

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis Number** > **FI-IO Modules**.

Step 3 Click the module that you want to monitor.

Step 4 Click one of the following tabs to view the status of the module:

Option	Description
General tab	Provides an overview of the status of the I/O module, including a summary of any faults, a summary of the module properties, and a physical display of the module and its components.

Option	Description
Fabric Ports tab	Displays the status and selected properties of all fabric ports in the I/O module.
Backplane Ports tab	Displays the status and selected properties of all backplane ports in the module.
Faults tab	Provides details of faults generated by the module.
Events tab	Provides details of events generated by the module.
FSM tab	Provides details about and the status of FSM tasks related to the module. You can use this information to diagnose errors with those tasks.
Statistics tab	Provides statistics about the module and its components. You can view these statistics in tabular or chart format.

Monitoring Management Interfaces

Management Interfaces Monitoring Policy

This policy defines how the mgmt0 Ethernet interface on the fabric interconnect should be monitored. If Cisco UCS detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault. By default, the management interfaces monitoring policy is enabled.

If the affected management interface belongs to a fabric interconnect which is the managing instance, Cisco UCS confirms that the subordinate fabric interconnect's status is up, that there are no current failure reports logged against it, and then modifies the managing instance for the endpoints.

If the affected fabric interconnect is currently the primary inside of a high availability setup, a failover of the management plane is triggered. The data plane is not affected by this failover.

You can set the following properties related to monitoring the management interface:

- Type of mechanism used to monitor the management interface.
- Interval at which the management interface's status is monitored.
- Maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.

Important In the event of a management interface failure on a fabric interconnect, the managing instance may not change if one of the following occurs:

- A path to the endpoint through the subordinate fabric interconnect does not exist.
- The management interface for the subordinate fabric interconnect has failed.
- The path to the endpoint through the subordinate fabric interconnect has failed.

Configuring the Management Interfaces Monitoring Policy

Procedure

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

Step 2 In the **Admin** tab, expand **All** > **Communication Management**.

Step 3 Click **Management Interfaces**.

Step 4 In the **Work** pane, click the **Management Interfaces Monitoring Policy** tab.

Step 5 Complete the following fields:

Name	Description
Admin Status field	Whether the monitoring policy is enabled or disabled for the management interfaces.
Poll Interval field	The number of seconds Cisco UCS should wait between data recordings. Enter an integer between 90 and 300.
Max Fail Report Count field	The maximum number of monitoring attempts that can fail before Cisco UCS assumes that the management interface is unavailable and generates a fault message. Enter an integer between 2 and 5.

Name	Description
Monitoring Mechanism field	The type of monitoring you want Cisco UCS to use. This can be one of the following: • **Mii Status—**Cisco UCS monitors the availability of the Media Independent Interface (MII). If you select this option, Cisco UCS Manager GUI displays the **Media Independent Interface Monitoring** area. • **Ping Arp Targets—**Cisco UCS pings designated targets using the Address Resolution Protocol (ARP). If you select this option, Cisco UCS Manager GUI displays the **ARP Target Monitoring** area. • **Ping Gateway—**Cisco UCS pings the default gateway address specified for this Cisco UCS domain on the **Management Interfaces** tab. If you select this option, Cisco UCS Manager GUI displays the **Gateway Ping Monitoring** area.

Step 6 If you chose **Mii Status** for the monitoring mechanism, complete the following fields in the **Media Independent Interface Monitoring** area:

Name	Description
Retry Interval field	The number of seconds Cisco UCS should wait before requesting another response from the MII if a previous attempt fails. Enter an integer between 3 and 10.
Max Retry Count field	The number of times Cisco UCS polls the MII until the system assumes the interface is unavailable. Enter an integer between 1 and 3.

Step 7 If you chose **Ping Arp Targets** for the monitoring mechanism, complete the fields on the appropriate tab in the **ARP Target Monitoring** area.
If you are using IPv4 addresses, complete the following fields in the **IPv4** subtab:

Name	Description
Target IP 1 field	The first IPv4 address Cisco UCS pings.
Target IP 2 field	The second IPv4 address Cisco UCS pings.
Target IP 3 field	The third IPv4 address Cisco UCS pings.
Number of ARP Requests field	The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.

Name	Description
Max Deadline Timeout field	The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.

If you are using IPv6 addresses, complete the following fields in the **IPv6** subtab:

Name	Description
Target IP 1 field	The first IPv6 address Cisco UCS pings.
Target IP 2 field	The second IPv6 address Cisco UCS pings.
Target IP 3 field	The third IPv6 address Cisco UCS pings.
Number of ARP Requests field	The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.

Type 0.0.0.0 for an IPv4 address to remove the ARP target or :: for an IPv6 address to remove the N-disc target.

Step 8 If you chose **Ping Gateway** for the monitoring mechanism, complete the following fields in the **Gateway Ping Monitoring** area:

Name	Description
Number of Ping Requests field	The number of times Cisco UCS should ping the gateway. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for a response from the gateway until Cisco UCS assumes the address is unavailable. Enter an integer between 5 and 15.

Step 9 Click **Save Changes**.

Health Monitoring

Monitoring Fabric Interconnect Low Memory Statistics

You can monitor Cisco UCS Fabric Interconnect system statistics and faults that allow you to manage overall system health, such as:

- **Low kernel memory—**This is the segment that the Linux kernel addresses directly. Cisco UCS Managerraises a major fault on a Fabric Interconnect when kernel memory falls below 100 MB. Two statistics, KernelMemFree and KernelMemTotal, alarm when low memory thresholds are met. KernelMemFree and KernelMemTotal statistics are added to threshold policy for system statistics where you can define your own thresholds.

  Low memory faults are supported on the following UCS Fabric Interconnects, including:

  - ◦ UCS 6248-UP
    - ◦ UCS 6296-UP

To view Fabric Interconnect low memory statistics and correctable memory statistics:

Procedure

Step 1 Click the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 2 In the **Work** pane, click the **Statistics** tab.

Step 3 On the **Statistics** tab, expand the **sysstats** node to monitor Fabric Interconnect low memory statistics. A major fault is raised when kernel memory free goes below 100 MB.

Monitoring Fabric Interconnect Low Memory Faults

Cisco UCS Manager system raises a major severity fault on a Fabric Interconnect when kernel memory free falls below 100 MB.

Low memory faults are supported on the following UCS Fabric Interconnects, including:

- ◦ UCS 6248-UP
  - ◦ UCS 6296-UP

To view Fabric Interconnect

Procedure

Step 1 Click the **Equipment** tab, expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 2 In the **Work** pane, click the **Faults** tab.

Step 3 On the **Fault** tab, look for a major severity fault with the description: `Fabric Interconnect_Name kernel low memory free reached critical level: ## (MB)`

Monitoring CIMC Memory Usage for Blade and Rack-Mount Servers

The Cisco Integrated Management Controller (CIMC) reports the following memory usage events for blade and rack-mount servers:

- When memory falls below 1MB, CIMC has fatal memory usage. Reset is imminent.
- When memory falls below 5 MB, CIMC has extremely high memory usage.
- When memory falls below 10 MB, CIMC has high memory usage.

If CIMC reports two health events, one with major severity, the other with minor severity, the system raises a major severity fault and displays details under the **Health** tab **Management Services** subtab.

To view CIMC memory usage events:

Procedure

Do one of the following:

- **For Blade Servers**:
  1. On the **Equipment** tab, expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**
  2. Click ***Server_Number***.
  3. In the **Work** pane, click the **Health** tab.
- **For Rack-Mount Servers**:
  1. On the **Equipment** tab, expand **Equipment** > **Rack-Mounts** > **Servers**
  2. Click ***Server_Number***.
  3. In the **Work** pane, click the **Health** tab.

If CIMC reports two health events, one with major severity, the other with minor severity, the system raises a major severity fault and displays details under the **Health** tab **Management Services** subtab. Each health event does not translate to a fault. The highest severity health event translates to a fault. Faults appear under ***Server_Number*** > **Faults** tab.

Monitoring CMC Memory Usage for I/O Modules

The Cisco Chassis Management Controller (CMC) reports memory usage events for I/O modules and chassis.

The system raises a fault on the aggregation of reported health status.

To view CMC memory usage events:

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 2 Click ***I/O Module_Number***.
The **Health** tab **Management Services** subtab appears.

Each event does not translate to fault. The highest severity events translate to fault. Faults appear under ***I/O Module_Number*** > **Faults** tab.

Monitoring FEX Statistics

The Cisco UCS Manager reports the following statistics for Cisco Fabric Extenders (FEXs) under the System Stats:

- Load
- Available Memory
- Cached Memory
- Kernel
- Total Memory
- Kernel Memory Free

Cisco 2200 Series and 2300 Series FEX support statistics monitoring.

Note FEX stats are not supported on the Cisco UCS Mini platform.

All FEX stats are added to threshold policy as FexSystemStats where user can define there own thresholds.

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Rack Mounts** > **FEX** > ***FEX Number***.
The **Statistics** tab appears.

Step 2 Expand the **sys-stats** node to monitor FEX statistics.

Local Storage Monitoring

Local storage monitoring in Cisco UCS provides status information on local storage that is physically attached to a blade or rack server. This includes RAID controllers, physical drives and drive groups, virtual drives, RAID controller batteries (BBU), Transportable Flash Modules (TFM) and super-capacitors, FlexFlash controllers, and SD cards.

Cisco UCS Manager communicates directly with the LSI MegaRAID controllers and FlexFlash controllers using an out-of-band (OOB) interface, which enables real-time updates. Some of the information that is displayed includes:

- RAID controller status and rebuild rate.
- The drive state, power state, link speed, operability and firmware version of physical drives.
- The drive state, operability, strip size, access policies, drive cache, and health of virtual drives.
- The operability of a BBU, whether it is a supercap or battery, and information about the TFM.

  LSI storage controllers use a Transportable Flash Module (TFM) powered by a super-capacitor to provide RAID cache protection.
- Information on SD cards and FlexFlash controllers, including RAID health and RAID state, card health, and operability.
- Information on operations that are running on the storage component, such as rebuild, initialization, and relearning.

  Note After a CIMC reboot or build upgrades, the status, start time, and end times of operations running on the storage component might not be displayed correctly.
- Detailed fault information for all local storage components.

  Note All faults are displayed on the **Faults** tab.

Support for Local Storage Monitoring

The type of monitoring supported depends upon the Cisco UCS server.

Supported Cisco UCS Servers for Local Storage Monitoring

Through Cisco UCS Manager, you can monitor local storage components for the following servers:

- Cisco UCS B200 M3 blade server
- Cisco UCS B420 M3 blade server
- Cisco UCS B22 M3 blade server
- Cisco UCS B200 M4 blade server

- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server
- Cisco UCS C460 M2 rack server
- Cisco UCS C420 M3 rack server
- Cisco UCS C260 M2 rack server
- Cisco UCS C240 M3 rack server
- Cisco UCS C220 M3 rack server
- Cisco UCS C24 M3 rack server
- Cisco UCS C22 M3 rack server
- Cisco UCS C220 M4 rack server
- Cisco UCS C240 M4 rack server
- Cisco UCS C460 M4 rack server

Note Not all servers support all local storage components. For Cisco UCS rack servers, the onboard SATA RAID 0/1 controller integrated on motherboard is not supported.

Supported Cisco UCS Servers for Legacy Disk Drive Monitoring

Only legacy disk drive monitoring is supported through Cisco UCS Manager for the following servers:

- Cisco UCS B200 M1/M2 blade server
- Cisco UCS B250 M1/M2 blade server

Note In order for Cisco UCS Manager to monitor the disk drives, the 1064E storage controller must have a firmware level contained in a UCS bundle with a package version of 2.0(1) or higher.

Prerequisites for Local Storage Monitoring

These prerequisites must be met for local storage monitoring or legacy disk drive monitoring to provide useful status information:

- The drive must be inserted in the server drive bay.
- The server must be powered on.
- The server must have completed discovery.
- The results of the BIOS POST complete must be TRUE.

Legacy Disk Drive Monitoring

Note The following information is applicable only for B200 M1/M2 and B250 M1/M2 blade servers.

The legacy disk drive monitoring for Cisco UCS provides Cisco UCS Manager with blade-resident disk drive status for supported blade servers in a Cisco UCS domain. Disk drive monitoring provides a unidirectional fault signal from the LSI firmware to Cisco UCS Manager to provide status information.

The following server and firmware components gather, send, and aggregate information about the disk drive status in a server:

- Physical presence sensor—Determines whether the disk drive is inserted in the server drive bay.
- Physical fault sensor—Determines the operability status reported by the LSI storage controller firmware for the disk drive.
- IPMI disk drive fault and presence sensors—Sends the sensor results to Cisco UCS Manager.
- Disk drive fault LED control and associated IPMI sensors—Controls disk drive fault LED states (on/off) and relays the states to Cisco UCS Manager.

Flash Life Wear Level Monitoring

Flash life wear level monitoring enables you to monitor the life span of solid state drives. You can view both the percentage of the flash life remaining, and the flash life status. Wear level monitoring is supported on the Fusion IO mezzanine card with the following Cisco UCS blade servers:

- Cisco UCS B22 M3 blade server
- Cisco UCS B200 M3 blade server
- Cisco UCS B420 M3 blade server
- Cisco UCS B200 M4 blade server
- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server

Note Wear level monitoring requires the following:

- Cisco UCS Manager must be at release 2.2(2a) or greater.
- The Fusion IO mezzanine card firmware must be at version 7.1.15 or greater.

Viewing the Status of Local Storage Components

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to view the status of your local storage components.

Step 4 In the **Work** pane, click the **Inventory** tab.

Step 5 Click the **Storage** subtab to view the status of your RAID controllers and any FlexFlash controllers.

Step 6 Click the down arrows to expand the **Local Disk Configuration Policy**, **Actual Disk Configurations**, **Disks**, and **Firmware** bars and view additional status information.

Note The **Local Disk Configuration Policy** and **Actual Disk Configurations** areas only display data for the Cisco UCS B460 blade server master node. No fields are displayed for the slave node.

Limitations

The Check Consistency operation is not supported for RAID 0 volumes. You must change the local disk configuration policy to run Check Consistency. For more information, see Changing a Local Disk Configuration Policy.

Graphics Card Server Support

With Cisco UCS Manager, you can view the properties for certain graphics cards and controllers. Graphics cards are supported on the following servers:

- Cisco UCS C240 M3 Rack Server
- Cisco UCS C460 M4 Rack Server
- Cisco UCS B200M4 Blade Server

Note Certain NVIDIA Graphics Processing Units (GPU) do not support Error Correcting Code (ECC) and vGPU together. Cisco recommends that you refer to the release notes published by NVIDIA for the respective GPU to know whether it supports ECC and vGPU together.

Viewing Graphics Card Properties

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **Servers**.

Step 3 Choose the server for which you want to view the Graphics Card settings.

Step 4 On the **Work** pane, click the **Inventory** tab.

Step 5 Click the **GPU** subtab.

Managing Transportable Flash Module and Supercapacitor

LSI storage controllers use a Transportable Flash Module (TFM) powered by a supercapacitor to provide RAID cache protection. With Cisco UCS Manager, you can monitor these components to determine the status of the battery backup unit (BBU). The BBU operability status can be one of the following:

- **Operable—**The BBU is functioning successfully.
- **Inoperable—**The TFM or BBU is missing, or the BBU has failed and needs to be replaced.
- **Degraded—**The BBU is predicted to fail.

TFM and supercap functionality is supported beginning with Cisco UCS Manager Release 2.1(2).

TFM and Supercap Guidelines and Limitations

TFM and Supercap Limitations

- The CIMC sensors for TFM and supercap on the Cisco UCS B420 M3 blade server are not polled by Cisco UCS Manager.
- If the TFM and supercap are not installed on the Cisco UCS B420 M3 blade server, or are installed and then removed from the blade server, no faults are generated.
- If the TFM is not installed on the Cisco UCS B420 M3 blade server, but the supercap is installed, Cisco UCS Manager reports the entire BBU system as absent. You should physically check to see if both the TFM and supercap is present on the blade server.

Supported Cisco UCS Servers for TFM and Supercap

The following Cisco UCS servers support TFM and supercap:

- Cisco UCS B420 M3 blade server
- Cisco UCS C22 M3 rack server

- Cisco UCS C24 M3 rack server
- Cisco UCS C220 M3 rack server
- Cisco UCS C240 M3 rack server
- Cisco UCS C420 M3 rack server
- Cisco UCS C460 M4 rack server

- Cisco UCS C220 M3 rack server
- Cisco UCS C240 M3 rack server

Monitoring RAID Battery Status

This procedure applies only to Cisco UCS servers that support RAID configuration and TFM. If the BBU has failed or is predicted to fail, you should replace the unit as soon as possible.

Procedure

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

Step 2 In the **Equipment** pane, expand **Chassis** > ***Chassis Number*** > **Servers** > ***Server Number***.

Step 3 In the **Work** pane, click the **Inventory** tab.

Step 4 Click the **Storage** subtab to view the **RAID Battery (BBU)** area.

Viewing a RAID Battery Fault

Note This applies only to Cisco UCS servers that support RAID configuration and TFM.

Procedure

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

Step 2 In the **Equipment** pane, expand **Chassis** > ***Chassis Number*** > **Servers** > ***Server Number***.

Step 3 In the **Work** pane, click the **Faults** tab.

Step 4 Select the battery to see more information on its condition.

TPM Monitoring

Trusted Platform Module (TPM) is included on all Cisco UCS M3 blade and rack-mount servers. Operating systems can use TPM to enable encryption. For example, Microsoft's BitLocker Drive Encryption uses the TPM on Cisco UCS servers to store encryption keys.

Cisco UCS Manager enables monitoring of TPM, including whether TPM is present, enabled, or activated.

Viewing TPM Properties

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Choose the server for which you want to view the TPM settings.

Step 4 On the **Work** pane, click the **Inventory** tab.

Step 5 Click the **Motherboard** subtab.