Hardware Monitoring

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.
Physical Ports tab	Displays the status of all ports on the fabric interconnect. This tab includes the following subtabs: • **Ethernet Ports** tab

Option	Description
	• **FC 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.
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.
Faults tab	Provides details of faults generated by the fabric interconnect.
Events tab	Provides details of events generated by the fabric interconnect.
Neighbors tab	Provides details about the LAN, SAN, and LLDP neighbors of the fabric interconnect. **Note** Enable **Info Policy** to view **Neighbors** details.
Statistics tab	Provides statistics about the fabric interconnect and its components. 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.
Inventory tab	Provides details about the properties and status of the components of the server on the following subtabs:

Option	Description
	• **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.
CIMC Sessions tab	Provides data about the CIMC sessions on the server.
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.
Events tab	Displays an overview of the events generated by the server. You can click any event to view additional information.

Option	Description
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.
Health tab	Displays details about the health status of the server and its components.
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 **Navigation** pane, click on one or more of the following components of the adapter to open the navigator and view the status of the component:

-
- DCE interfaces
- HBAs
- NICs
- iSCSI vNICs

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**.

Note For Cisco UCS C125 M5 Servers, expand **Equipment** > **Rack Mounts** > **Enclosures** > **Rack Enclosure** ***rack_enclosure_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.
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. **Note** If the firmware of C-Series/S-Series servers is upgraded from Cisco UCSM release 2.2(6) to 3.1(2) or later release, the Platform Controller Hub (PCH) storage controller (along with the SSD boot drives) does not appear in UCSM GUI. **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.

Option	Description
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.
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 IO Module

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **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 IO module, including a summary of any faults, a summary of the module properties, and a physical display of the module and its components.
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.
Health tab	Provides details about the health status of the module.
Statistics tab	Provides statistics about the module and its components. You can view these statistics in tabular or chart format.

Monitoring Crypto Cards

Cisco Crypto Card Management for Blade Servers

Cisco UCS Manager provides inventory management for the Cisco Mezzanine Crypto Card (UCSB-MEZ-INT8955) for the Cisco UCSB-B200-M4 Blade Server. The main function of Cisco Crypto Card is to provide hardware based encryption capability to UCS blade server for certain applications.

The Cisco B200 M4 Blade Server includes two optional, hot-pluggable, SAS, SATA hard disk drives (HDDs) or solid-state drives (SSDs) and is suited for a broad spectrum of IT workloads. Place the Crypto Card in slot 2 of the blade server.

Cisco UCS Manager discovers the Crypto Card present in a blade server and displays the model, revision, vendor, serial number on the Equipment > Chassis > *Server_Number* > Inventory > Security subtab. Discovery of the Crypto Card fails if you add the Crypto Card to an unsupported blade server.

Cisco UCS Manager does not support firmware management for the Crypto Card.

Insertion and removal of a Crypto Card triggers deep discovery. Replacing the Crypto Card with another Crypto Card, Adaptor or Fusion I/O, or pass through card triggers deep discovery for commissioned servers. The following are the various Crypto Card replacement scenarios:

- Replacing a Crypto Card with another Crypto Card

- Replacing a Crypto Card with an adaptor
- Replacing a Crypto Card with a Fusion I/O
- Replacing a Crypto Card with a GPU card
- Replacing Crypto Card with a pass through card
- Replacing an adaptor with a Crypto Card
- Replacing a storage Mezzanine with a Crypto Card
- Replacing a GPU card with a Crypto Card

No cleanup is necessary for the downgrade of Cisco UCS Manager to an earlier version. If you upgrade UCS Manager after a downgrade, rediscovery of the card is necessary to inventory the card. For servers that do not support crypto cards, discovery proceeds uninterrupted.

Cisco UCS Manager discovers, associates, disassociates, and decommissions Crypto Cards.

Viewing Crypto Card Properties

Procedure

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

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

Step 3 On the **Work** pane, click the **Inventory** tab, then click the **Security** subtab.

Name	Description
ID field	
Slot ID field	Specifies the Slot ID where the Mezzanine card is placed.
Magma Expander Slot Id field	Specifies the ID number of the PCI slot.
Is Supported field	Specifies whether the card is supported.
Vendor field	Specifies the vendor of the card.
Model field	Specifies the model number of the card.
Serial field	Specifies the serial number of the card.
Firmware Version field	Specifies the Crypto card serial number.

Monitoring NVMe PCIe SSD Devices

NVMe PCIe SSD Storage Device Inventory

Cisco UCS Manager GUI discovers, identifies, and displays the inventory of Non-Volatile Memory Express (NVMe) Peripheral Component Interconnect Express (PCIe) SSD storage devices. You can view the health of the storage devices in the server. NVMe with PCIe SSD storage devices reduce latency, increase Input/Output Operations Per Second (IOPS), and lower power consumption compared to SAS or SATA SSDs.

The optional Intel VMD-enabled NVMe driver and Intel VMD-enabled LED Command line interface tool provide additional functionality by aggregating the NVMe PCIe SSD devices attached to its root port. This enables Suprise hot-plug and allows optional configuration of LED blinking patterns on PCIe SSD storage attached to Intel VMD enabled domains.

Viewing NVMe PCIe SSD Storage Inventory

Procedure

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

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

Step 3 Click the **Inventory** tab.

Step 4 Do one of the following:

a) Click the **Storage** tab.

The list of NVMe PCIe SSD storage devices named **Storage Controller NVME *ID number*** is displayed. You can view the name, size, serial number, operating status, state and other details.

b) Click the NVMe PCIe SSD storage device.

The following inventory details are displayed:

Name	Description
Actions Area	
ID field	The NVMe PCIe SSD storage device configured on the server.
Description field	Brief description of the NVMe PCIe SSD storage device configured on the server.
Model field	The NVMe PCIe SSD storage device model.
Revision field	The NVMe PCIe SSD storage device revision.

Name	Description
Subtype field	The vendor name of the NVMe PCIe SSD storage device.
RAID Support field	Indicated whether the NVMe PCIe SSD storage device is RAID enabled.
OOB Interface Support field	Indicates if the NVMe PCIe SSD storage device supports out-of-band management .
PCIe Address field	The NVMe PCIe SSD storage device on the virtual interface card (VIC).
Number of Local Disks field	The number of disks contained in the NVMe PCIe SSD storage device.
Rebuild Rate field	The time it takes the storage device to rebuild RAID when a disk fails.
SubOemID	The OME ID for the NVMe PCIe SSD storage device on the virtual interface card (VIC).
Supported Strip Sizes field	The strip size supported by the NVMe PCIe SSD storage device.
Sub Device ID field	The sub device ID of the controller
Sub Ventor ID field	The sub vendor ID of the controller
Name field	The name of the controller.
PID field	The NVMe PCIe SSD storage device product ID, also known as product name, model name, product number
Serial field	The storage device serial number.
Vendor field	The vendor that manufactured the NVMe PCIe SSD storage device.
PCI Slot field	The PCI slot of the storage device.

Name	Description
Controller Status field	The current status of the controller as reported by CIMC. This can be one of the following: • Optimal—The controller is functioning properly. • Failed—The controller is not functioning. • Unresponsive—The CIMC is unable to communicate with the controller.
Pinned Cache Status field	The pin cache status of the storage device.
Default Strip Size field	The default strip size the storage device can support.
Device ID field	The ID of the storage device.
Vendor ID field	The ID of the manufacturer.
Security field	The device security applied to the storage device.
Embedded Storage Area	
Presence field	Whether the storage is embedded or not.
Operability field	The operable status of the device.
Block Size field	The memory of the device.
Size (MB) field	The fractional memory of the device in MB.
Connection Protocol field	The connection protocol followed.
Oper Qualified Reason	The operability reason of the device
Number of Blocks field	The number of memory blocks.
Firmware Area	
Boot-loader Version field	Displays the firmware version that is associated with the boot-loader software on the component.

Name	Description
Running Version field	The firmware version used by the component.
Package Version field	The firmware package version in which the firmware was included.
Startup Version field	The version of the firmware that takes effect the next time that the component reboots.
Activate Status field	This can be one of the following: • Ready—Activation succeeded and the component is running the new version. • Activating—The system is activating the new firmware version. • Failed—The firmware activation failed. For more information, double-click the failed component to view its status properties.

Viewing NVMe PCIe SSD Storage Statistics

Procedure

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

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

Step 3 Click the **Inventory** tab.

Step 4 Click the **Storage** tab.

Step 5 Click the **Controller** tab.

Step 6 Click the NVMe PCIe SSD storage device for which you wish to view the statistics.

Step 7 Click the **Statistics** tab.

The following statistics are displayed:

Name	Description
Toggle History Table button	Splits the right-hand pane vertically and displays the **History** table in the bottom portion of the pane. When you select a counter in the top portion of the pane, the **History** table displays the information recorded each time the data from that counter was collected.
Modify Collection Policy button	Open the **General** tab for the selected counter, which enables you to specify the collection and reporting intervals for the counter. **Note** This option is only available if a counter is selected.
Name column	A tree view showing the system components for which statistical counters are available. To view the counters associated with a component, expand that part of the navigation tree. To view all counters, click the + (plus sign) button at the top of the chart. System statistics for fabric interconnects and FEX are available. These include: • CPU usage • Memory usage, including low kernel memory **Note** A major fault is raised on the fabric interconnect if the available kernel memory is less than 100 MB • ECC errors Disk statistics are displayed for PCH, SAS, and SATA storage controllers. NVMe statistics are displayed for NVMe drives. These include: • **DriveLifeUsedPercentage**: The NVMe drive read and write life used presented in percentage. • **LifeLeftInDays**: The NVMe drive read and write life left based on the workload. Once full, the drive can be used only to read. • **Temperature**: The drive temperature.

Name	Description
Value column	For the top-level component, this column shows the date and time the counter was last updated. For the actual counters, this column shows the current value of the counter. The unit the value is in can be determined by the code appended to the name of the counter: • **(A)**— Amperes • **(babbles)** • **(bytes)**— Number of bytes • **©)**—Celsius • **(collisions)**— Number of times a network collision was encountered • **(drops)**— Number of times packets were dropped during the transfer • **(errors)**— Number of errors encountered • **(lostCarrier)**— Number of times the carrier was lost during transmission • **(MB)**— Megabytes • **(noCarrier)**— Number of times no carrier could be found • **(packets)**— Number of packets transferred • **(pause)**— Number of pauses encountered during data transmission • **(resets)**— Number or resets encountered during data transmission • **(V)**—Volts • **(W)**— Watts • **(**blank**)**
Avg column	The average value for the counter. **Note** For aggregated counters, this is the average delta within the reporting interval.
Max column	The maximum recorded value for the counter. **Note** For aggregated counters, this is the maximum delta within the reporting interval.
Min column	The minimum recorded value for the counter. **Note** For aggregated counters, this is the minimum delta within the reporting interval.

Name	Description
Delta column	The largest change recorded for the counter.

Health Monitoring

Monitoring Fabric Interconnect Low Memory Statistics and Correctable Parity Errors

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 Manager raises a major fault on a fabric interconnect when kernel memory falls below 100 MB. See Monitoring Fabric Interconnect Low Memory Faults, on page 16. Two statistics KernelMemFree and KernelMemTotal alarm, when low memory thresholds are met. KernelMemFree and KernelMemTotal statistics are added to the threshold policy for system statistics where you can define your own thresholds.

  Low memory faults are supported on the following Cisco UCS fabric interconnects:

  - UCS 6248-UP
  - UCS 6296-UP
  - UCS Mini
  - UCS-FI-6332
  - UCS-FI-6332-16UP

- **Correctable Parity Errors**—(For UCS 6300 fabric interconnects only) The system collects and reports these errors for the fabric interconnect under **Statistics > sysstats > CorrectableParityError**.
- **Uncorrectable Parity Errors**—(For UCS 6300 fabric interconnects only) These errors raise a major fault on fabric interconnects under the **Faults** tab and triggers CallHome. These major faults may cause you to reboot the fabric interconnect. See Monitoring Fabric Interconnect Uncorrectable Parity Error Major Faults, on page 16.

To view fabric interconnect low memory statistics and correctable memory statistics:

Procedure

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

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

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

Step 4 On the **Statistics** tab, expand the **sysstats** node to monitor fabric interconnect low memory statistics and correctable parity errors.

A major fault is raised when kernel memory free (KernelMemFree) goes below 100 MB. The system also raises a major fault when an Uncorrectable Parity Error occurs.

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 Cisco UCS fabric interconnects:

- UCS 6248-UP
- UCS 6296-UP
- UCS Mini
- UCS-FI-6332
- UCS-FI-6332-16UP

To view fabric interconnect low memory faults:

Procedure

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

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

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

Step 4 On the **Faults** tab, look for a major severity fault with the description: `Fabric Interconnect_Name kernel low memory free reached critical level: ## (MB)`

Monitoring Fabric Interconnect Uncorrectable Parity Error Major Faults

Uncorrectable Parity Errors raise a major fault on fabric interconnects under the **Faults** tab and triggers CallHome. Major faults may cause you to reboot the fabric interconnect.

Note This applies for UCS 6300 fabric interconnects only.

To monitor Uncorrectable Parity Error faults:

Procedure

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

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

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

Step 4 On the **Faults** tab, look for a major severity fault with the description: `SER, Uncorrectable Error: Unrecoverable error found, maybe some corrupted file system. Reboot FI for recovery.`

Step 5 Reboot the fabric interconnect.

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.

To view CIMC memory usage events:

Procedure

Do one of the following:

- **For Blade Servers**:
  a. On the **Equipment** tab, expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.
  b. Click ***Server_Number***.
  c. In the **Work** pane, click the **Health** tab.
- **For Rack-Mount Servers**:
  a. On the **Equipment** tab, expand **Equipment** > **Rack-Mounts** > **Servers**.
  b. Click ***Server_Number***.
  c. 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. Every 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 Input/Output Modules

The Cisco Chassis Management Controller (CMC) reports memory usage events for IOMs and chassis.

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

To view CMC memory usage events:

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Click ***IO Module_Number***.

The **Health** tab **Management Services** subtab appears.

Every event does not translate to a fault. The highest severity events translate to fault. Faults appear under ***IO Module_Number*** > **Faults** tab.

Monitoring FEX Statistics

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 users can define their own thresholds.

Procedure

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

The **Statistics** tab appears. You can view the statistics in tabular or chart format.

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

Management Interfaces Monitoring Policy

The management interfaces monitoring policy defines how the mgmt0 Ethernet interface on the fabric interconnect is monitored. If Cisco UCS Manager 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.

When the management interface of a fabric interconnect which is currently the managing instance fails, Cisco UCS Manager first confirms if the status of the subordinate fabric interconnect is up. In addition, if there are no current failure reports logged against the fabric interconnect, Cisco UCS Manager modifies the managing instance for the endpoints.

If the affected fabric interconnect is currently the primary in a high availability setup, a failover of the management plane is triggered. This failover does not affect the data plane. You can set the following properties related to monitoring the management interface:

- The type of mechanism used to monitor the management interface.
- The interval at which the status of the management interface is monitored.
- The maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.

Important When the management interface fails 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 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	Indicates whether the monitoring policy is enabled or disabled for the management interfaces.

Name	Description
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.
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.

Name	Description
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.

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**.

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 (Battery Backup Unit), Transportable Flash Modules (TFM), supercapacitors, FlexFlash controllers, and SD cards.

Cisco UCS Manager communicates directly with the LSI MegaRAID controllers and FlexFlash controllers using an out-of-band 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 supercapacitor 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 may 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 M6 Server
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS B200 M4 blade server
- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server
- Cisco UCS B200 M3 blade server

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

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

- Cisco UCS C420 M3 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
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C480 M5 Server
- Cisco UCS C220 M6 Server
- Cisco UCS C240 M6 Server
- Cisco UCS C225 M6 Server
- Cisco UCS C245 M6 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.

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.

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 B200 M4 blade server
- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS B200 M6 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.

RAID 0 Check Consistency Limitation

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 the *UCS Manager Server Management Guide,* Server Related Policies chapter, Changing a Local Disk Policy topic.

Graphics Card Monitoring

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 C460 M4 Rack Server
- Cisco UCS B200M4 Blade Server
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C480 M5 Server
- Cisco UCS C225 M6 Server
- Cisco UCS C245 M6 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.

GPU Mezzanine Graphics Module Management for Blade Servers

Cisco UCS Manager provides inventory and firmware management support for the NVIDIA Graphics Processing Unit (GPU) Mezzanine Graphic Module (N16E-Q5) for Cisco B200 M4 Blade Servers. GPU computing accelerates scientific, analytics, engineering, consumer, and enterprise applications. The Cisco B200 M4 Blade Server includes two optional, hot-pluggable, SAS, SATA hard disk drives (HDDs) or solid-state drives (SSDs) and is suited for a broad spectrum of IT workloads.

Cisco UCS Managerdiscovers the presence of the GPU Graphics Card in a blade server as a field replaceable unit and collects device inventory information, such as model, vendor, serial number, PCI slot and address, and firmware. Cisco UCS Manager displays GPU Card inventory on the Equipment > Chassis > *Server_Number* > Inventory > GPUs subtab.

GPU Card firmware management includes firmware upgrade and downgrade. Upgrade the GPU firmware through existing Cisco UCS Manager service profiles. Do not downgrade GPU firmware with older firmware versions, because cleanup is required.

Place the GPU Card in slot 2 of the blade server. GPU Card discovery fails if you is insert a card in an unsupported blade.

Replacing a GPU card triggers deep discovery for commissioned servers. The following are the various GPU card replacement scenarios that cause deep discovery:

- Replacing a GPU card with another GPU card
- Replacing a GPU card with an adaptor
- Replacing a GPU card with a storage Mezzanine
- Replacing an adaptor with a GPU card
- Replacing a storage Mezzanine with GPU card
- Replacing a GPU card with Crypto card
- Replacing a Crypto card with a GPU card

Cisco UCS Manager discovers, associates, disassociates, and decommissions GPU Graphics Cards. To view GPU Graphics Cards, see Viewing Graphics Card Properties, on page 26.

Note There is a maximum limit on the GPU Graphics Card memory (DIMMS) of 1 TB.

Viewing Graphics Card Properties

Procedure

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

Step 2 Do one of the following:

- Expand **Equipment** > **Chassis** > ***Chassis_Number*** > **Servers** > ***Server_Number***.
- Expand **Equipment** > **Rack-Mounts** > **Servers** > ***Server_Number***.

Step 3 On the **Work** pane, click the **Inventory** tab, then click the **GPU** subtab.

Name	Description
ID field	The unique ID for the graphics card.
PCI Slot field	The PCI slot number where the graphics card is installed.
Expander Slot ID field	The expander slot ID.
PID field	Product Identifier of the graphics card.
Is Supported field	Whether the graphics card is supported. This can be one of the following: • **Yes** • **No**
Vendor field	The name of the manufacturer.
Model field	The model number of the graphics card.
Serial field	The serial number of the component.

Name	Description
Running Version field	The firmware version of the graphics card. **Note** Starting with Cisco UCS Manager Release 4.2(3e), UCS Manager supports the firmware management for the following NVIDIA A Series GPUs with and without Crypto-Embedded Controller (CEC): • NVIDIA A10 • NVIDIA A16 • NVIDIA A30 • NVIDIA A40 • NVIDIA A100-80GB **Example:** • GPU version with CEC: 94.02.5C.00.03|G133.0200.00.05|5.01 • GPU version without CEC: 94.02.5C.00.0F|G133.0200.00.05
Activate Status	Status of graphics card firmware activation: • **Ready**—Activation succeeded and the component is running the new version. • **Activating**—The system is activating the new firmware version. • **Failed**—The firmware activation failed. For more information, double-click the failed component to view its status properties.
Mode field	The mode of the configured graphics card. This can be one of the following: • **Compute** • **Graphic** • **Any Configuration**
Part Details	
Vendor ID field	The vendor ID of the graphics card.
Sub Vendor ID field	The sub vendor ID of the graphics card.
Device ID field	The device ID of the graphics card.
Sub Device ID field	The sub device ID of the graphics card.

PCI Switch Monitoring

PCI Switch Server Support

With Cisco UCS Manager, you can view the properties for PCI switches. PCI switches are supported on the following servers:

- Cisco UCS C480 M5 ML Server

Viewing PCI Switch Properties

PCI Switch properties are visible only for servers which support PCI switch.

Procedure

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

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

Step 3 On the **Work** pane, click the **Inventory** tab, then click the **PCI Switch** subtab.

Name	Description
Device ID field	The device ID of the PCI switch.
ID field	The unique ID for the PCI switch.
PCI Slot field	The PCI slot number where the PCI switch is installed.
PCI Address	The PCI address for the specific PCI switch.
PID field	The Cisco Product Identifier (PID) of the PCI switch.
Switch Name field	The name of the PCI switch. This typically includes the ID of the switch. For example, PCI Switch 2.
Switch Status	Indicates whether the PCI switch is working correctly. The switch status could be one of the following: • Good—When the PCI switch works correctly. • Degraded—When the PCI switch has uncorrectable critical errors.
Vendor field	The name of the manufacturer.
Vendor ID field	The vendor ID of the PCI switch.
Model field	The model number of the PCI switch.
Sub Device ID field	The sub device ID of the PCI switch.

Name	Description
Sub Vendor ID field	The sub vendor ID of the PCI switch.
Temperature field	The current temperature of the PCI switch
PCI Link Details	
Link Speed field	Speed of the PCI link.
Link Status field	Status of the PCI link
Link Width field	Width of the PCI link
Slot Status field	Indicates whether the PCI slot is working correctly.
PCI Slot field	PCI slot number

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:

Viewing the RAID Controller Stats

The following procedure shows how to see RAID controller stats for a server with PCIe\NVMe Flash Storage

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** > **Controller** > **General** subtab to view the controller stats.

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 and higher 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.