Monitoring Hardware

This chapter includes the following sections:

Monitoring a Fabric Interconnect

Procedure

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

Step 2 On the **Equipment** tab, 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 the **Equipment** tab.

Step 2 On the **Equipment** tab, 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
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.
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.
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 the **Equipment** tab.

Step 2 On the **Equipment** tab, 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 the **Equipment** tab.

Step 2 On the **Equipment** tab, 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 the **Equipment** tab.

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

Step 3 Click the I/O module that you want to monitor.

Step 4 Click one of the following tabs to view the status of the I/O 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 I/O module.
Faults tab	Provides details of faults generated by the I/O module.
Events tab	Provides details of events generated by the I/O module.
FSM tab	Provides details about and the status of FSM tasks related to the I/O module. You can use this information to diagnose errors with those tasks.
Statistics tab	Provides statistics about the I/O 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 disabled.

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 end-points.

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

Configuring the Management Interfaces Monitoring Policy

Procedure

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

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 the system 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 the system 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 the system to use. This can be one of the following: • **Mii Status**—The system 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**—The system 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**—The system 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 the system 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 the system 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 following fields in the **ARP Target Monitoring** area:

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

Name	Description
Max Deadline Timeout field	The number of seconds to wait 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 to remove the ARP 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 the system should ping the gateway. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds to wait for a response from the gateway until the system assumes the address is unavailable. Enter an integer between 5 and 15.

Step 9 Click **Save Changes**.

Server Disk Drive Monitoring

The 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.

Support for Disk Drive Monitoring

Disk drive monitoring only supports certain blade servers and a specific LSI storage controller firmware level.

Supported Cisco UCS Servers

Through Cisco UCS Manager, you can monitor disk drives for the following servers:

- B-200 blade server
- B-230 blade server
- B-250 blade server
- B-440 blade server

Cisco UCS Manager cannot monitor disk drives in any other blade server or rack-mount server.

Storage Controller Firmware Level

The storage controller on a supported server must have LSI 1064E firmware.

Cisco UCS Manager cannot monitor disk drives in servers with a different level of storage controller firmware.

Prerequisites for Disk Drive Monitoring

In addition to the supported servers and storage controller firmware version, you must ensure that the following prerequisites have been met for 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.

Viewing the Status of a Disk Drive

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.

Step 3 Click the server for which you want to view the status of the disk drive.

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

Step 5 Click the **Storage** subtab.

Step 6 Click the down arrows to expand the **Disks** bar and view the following fields in the **States** section for each disk drive:

Name	Description
Operability field	The operational state of the disk drive. This can be the following: • **Operable**—The disk drive is operable. • **Inoperable**—The disk drive is inoperable, possibly due to a hardware issue such as bad blocks. • **N/A**—The operability of the disk drive cannot be determined. This could be due to the server or firmware not being support for disk drive monitoring, or because the server is powered off. **Note** The **Operability** field may show the incorrect status for several reasons, such as if the disk is part of a broken RAID set or if the BIOS POST (Power On Self Test) has not completed.
Presence field	The presence of the disk drive, and whether it can be detected in the server drive bay, regardless of its operational state. This can be the following: • **Equipped**—A disk drive can be detected in the server drive bay. • **Missing**—No disk drive can be detected in the server drive bay.

Interpreting the Status of a Monitored Disk Drive

Cisco UCS Manager displays the following properties for each monitored disk drive:

- Operability—The operational state of the disk drive.
- Presence—The presence of the disk drive, and whether it can be detected in the server drive bay, regardless of its operational state.

You need to look at both properties to determine the status of the monitored disk drive. The following table shows the likely interpretations of the property values.

Operability Status	Presence Status	Interpretation
Operable	Equipped	No fault condition. The disk drive is in the server and can be used.

Operability Status	Presence Status	Interpretation
Inoperable	Equipped	Fault condition. The disk drive is in the server, but one of the following could be causing an operability problem: • The disk drive is unusable due to a hardware issue such as bad blocks. • There is a problem with the IPMI link to the storage controller.
N/A	Missing	Fault condition. The server drive bay does not contain a disk drive.
N/A	Equipped	Fault condition. The disk drive is in the server, but one of the following could be causing an operability problem: • The server is powered off. • The storage controller firmware is the wrong version and does not support disk drive monitoring. • The server does not support disk drive monitoring.

Note The **Operability** field may show the incorrect status for several reasons, such as if the disk is part of a broken RAID set or if the BIOS POST (Power On Self Test) has not completed.