CHAPTER 2

Cisco UCS Faults

This chapter provides information about the faults that may be raised in a Cisco UCS instance.

This chapter contains the following sections:

Adapter-Related Faults

This section contains faults raised as a result of issues with the adapters in a server.

fltAdaptorExtEthIfMisConnect

Fault Code:F0625

Message

Adapter [id] eth interface [id] in server [id] mis-connected

Explanation

The link for a network-facing adapter interface is misconnected. Cisco UCS Manager raises this fault when any of the following scenarios occur:

- Cisco UCS Manager detects a new connectivity between a previously configured switch port or FEX port and the adapter's external interface.
- Cisco UCS Manager detects a misconnected link between a fabric interconnect or FEX and its non-peer adapter's interface.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check whether the adapter link is connected to a port that belongs to its peer fabric interconnect or FEX.

Step 2 If that connectivity seems correct, reacknowledge the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: link-misconnected
CallHome: none
mibFaultCode: 625
mibFaultName: fltAdaptorExtEthIfMisConnect
moClass: adaptor:ExtEthIf
Type: network
```

fltAdaptorExtEthIfMissing

Fault Code:F0775

Message

Connection to Adapter [id] eth interface [id] in server [id] missing

Explanation

The link for a network-facing adapter interface is misconnected. Cisco UCS Manager raises this fault when it detects that the connectivity between a previously configured port on a fabric interconnect or FEX and its prior peer network-facing adapter interface is misconnected or missing.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check whether the adapter interface is connected to a port belonging to its peer fabric interconnect or FEX.

Step 2 If the connectivity seems correct, reacknowledge the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: link-missing
CallHome: none
mibFaultCode: 775
mibFaultName: fltAdaptorExtEthIfMissing
moClass: adaptor:ExtEthIf
Type: network
```

fltAdaptorExtIfLink-down

Fault Code:F0209

Message

Adapter uplink interface [id]/[id]/[id] link state: [linkState]Adapter uplink interface [chassisId]/[slotId]/[id]/[id] link state: [linkState]

Explanation

The link for a network facing adapter interface is down. Cisco UCS Manager raises this fault when any of the following scenarios occur:

- Cisco UCS Manager cannot establish and/or validate the adapter's connectivity to any of the fabric interconnects.
- The endpoint reports a link down or vNIC down event on the adapter link.
- The endpoint reports an errored link state or errored vNIC state event on the adapter link.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the adapter is connected, configured properly, and is running the recommended firmware version.

Step 2 If the server is stuck at discovery, decommission the server and reacknowledge the server slot.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: link-down
CallHome: none
mibFaultCode: 209
mibFaultName: fltAdaptorExtIfLinkDown
moClass: adaptor:ExtIf
Type: network
```

fltAdaptorHostEthIfMisConnect

Fault Code:F0626

Message

Adapter [id] eth interface [id] in server [id] mis-connected

Explanation

The link for a network-facing host interface is misconnected. Cisco UCS Manager raises this fault when any of the following scenarios occur:

- Cisco UCS Manager detects a new connectivity between a previously configured switch port and the host Ethernet interface.
- Cisco UCS Manager detects a misconnected link between the host interface and its non-peer fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check whether the host Ethernet interface is connected to a port belonging to its peer fabric interconnect.

Step 2 If connectivity seems correct, reacknowledge the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: link-misconnected
CallHome: none
mibFaultCode: 626
mibFaultName: fltAdaptorHostEthIfMisConnect
moClass: adaptor:HostEthIf
Type: network
```

fltAdaptorHostEthIfMissing

Fault Code:F0708

Message

Connection to Adapter [id] eth interface [id] in server [id] missing

Explanation

The link for a network-facing host interface is missing. Cisco UCS Manager raises this fault when it detects missing connectivity between a previously configured switch port and its previous peer host interface.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check whether the adapter link is connected to a port that belongs to its non-peer fabric interconnect.

Step 2 If that connectivity seems correct, reacknowledge the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: link-missing
CallHome: none
mibFaultCode: 708
mibFaultName: fltAdaptorHostEthIfMissing
moClass: adaptor:HostEthIf
Type: network
```

fltAdaptorHostIfLink-down

Fault Code:F0207

Message

Adapter [transport] host interface [id]/[id]/[id] link state: [linkState]Adapter [transport] host interface [chassisId]/[slotId]/[id]/[id] link state: [linkState]

Explanation

This fault typically occurs as a result of one of the following issues:

- The fabric interconnect is in End-Host mode, and all uplink ports failed.
- The server port to which the adapter is pinned failed.
- A transient error caused the link to fail.

Recommended Action

If you see this fault, take the following actions:

Step 1 If an associated port is disabled, enable the port.

Step 2 Reacknowledge the server with the adapter that has the failed link.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: link-down
CallHome: none
mibFaultCode: 207
mibFaultName: fltAdaptorHostIfLinkDown
moClass: adaptor:HostIf
Type: network
```

fltAdaptorUnitAdaptorReachability

Fault Code:F0206

Message

Adapter [id]/[id] is unreachableAdapter [chassisId]/[slotId]/[id] is unreachable

Explanation

Cisco UCS Manager cannot access the adapter. This fault typically occurs as a result of one of the following issues:

- The server does not have sufficient power.
- The I/O module is not functional.
- The adapter firmware has failed.
- The adapter is not functional

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the POST results for the server. In Cisco UCS Manager GUI, you can access the POST results from the General tab for the server. In Cisco UCS Manager CLI, you can access the POST results through the **show post** command under the scope for the server.

Step 2 In Cisco UCS Manager, check the power state of the server.

Step 3 Verify that the physical server has the same power state.

Step 4 If the server is off, turn the server on.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: connectivity-problem
CallHome: diagnostic
mibFaultCode: 206
mibFaultName: fltAdaptorUnitAdaptorReachability
moClass: adaptor:Unit
```

Type: connectivity

fltAdaptorUnitExtnMissing

Fault Code:F0901

Message

Adapter extension [id] in server [chassisId]/[slotId] presence: [presence]

Explanation

This fault typically occurs when an I/O adapter unit extension, such as a pass-through adapter, is missing. Cisco UCS Manager raises this fault when any of the following scenario occur:

- The endpoint reports there is no adapter unit extension, such as a pass-through adapter, plugged into the adapter slot.
- The endpoint cannot detect or communicate with the adapter unit extension plugged into the adapter slot.

Recommended Action

If you see this fault, take the following actions:

Step 1 Ensure the adapter unit extension is properly plugged into an adapter slot in the server.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: warning
Cause: equipment-missing
CallHome: none
mibFaultCode: 901
mibFaultName: fltAdaptorUnitExtnMissing
moClass: adaptor:UnitExtn
Type: equipment

fltAdaptorUnitExtnUnidentifiable-fru

Fault Code:F0900

Message

Adapter extension [id] in server [chassisId]/[slotId] has unidentified FRU

Explanation

This fault typically occurs because Cisco UCS Manager has detected an unsupported adapter unit extension, such as a pass-through adaptor. For example, the model, vendor, or revision is not recognized.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that a supported adapter unit extension is installed.

Step 2 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: unidentifiable-fru
CallHome: none
mibFaultCode: 900
mibFaultName: fltAdaptorUnitExtnUnidentifiableFru
moClass: adaptor:UnitExtn
Type: server
```

fltAdaptorUnitMissing

Fault Code:F0203

Message

Adapter [id] in server [id] presence: [presence]Adapter [id] in server [chassisId]/[slotId] presence: [presence]

Explanation

The adaptor is missing. Cisco UCS Manager raises this fault when any of the following scenarios occur:

- The endpoint reports there is no adapter in the adaptor slot.
- The endpoint cannot detect or communicate with the adapter in the adaptor slot.

Recommended Action

If you see this fault, take the following actions:

Step 1 Make sure an adapter is inserted in the adaptor slot in the server.

Step 2 Check whether the adaptor is connected and configured properly and is running the recommended firmware version.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-missing
CallHome: none
mibFaultCode: 203
mibFaultName: fltAdaptorUnitMissing
moClass: adaptor:Unit
Type: equipment
```

fltAdaptorUnitUnidentifiable-fru

Fault Code:F0200

Message

Adapter [id] in server [id] has unidentified FRUAdapter [id] in server [chassisId]/[slotId] has unidentified FRU

Explanation

This fault typically occurs because Cisco UCS Manager has detected an unsupported adapter. For example, the model, vendor, or revision is not recognized.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that a supported adapter is installed.

Step 2 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: unidentifiable-fru
CallHome: none
mibFaultCode: 200
mibFaultName: fltAdaptorUnitUnidentifiableFru
moClass: adaptor:Unit
Type: server
```

Chassis-Related Faults

This section contains faults raised as a result of issues related to a chassis in the Cisco UCS instance.

fltEquipmentChassisIdentity

Fault Code:F0404

Message

Chassis [id] has a mismatch between FRU identity reported by Fabric/IOM vs. FRU identity reported by CMC

Explanation

This fault typically occurs when the FRU information for an I/O module is corrupted or malformed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: fru-problem
CallHome: diagnostic
mibFaultCode: 404
mibFaultName: fltEquipmentChassisIdentity
moClass: equipment:Chassis
Type: equipment
```

fltEquipmentChassisIdentity-unestablishable

Fault Code:F0543

Message

Chassis [id] has an invalid FRU

Explanation

This fault typically occurs because Cisco UCS Manager has detected an unsupported chassis. For example, the model, vendor, or revision is not recognized.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, execute the **show tech-support** command and contact Cisco technical support.

Fault Details

```
Severity: major
Cause: identity-unestablishable
CallHome: none
mibFaultCode: 543
mibFaultName: fltEquipmentChassisIdentityUnestablishable
moClass: equipment:Chassis
Type: equipment
```

fltEquipmentChassisInoperable

Fault Code:F0456

Message

Chassis [id] operability: [operability]

Explanation

This fault typically occurs for one of the following reasons:

- The fabric interconnect cannot communicate with a chassis. For a cluster configuration, this fault means that neither fabric interconnect can communicate with the chassis.
- The chassis has an invalid FRU.

Recommended Action

If you see this fault, take the following actions:

Step 1 In Cisco UCS Manager, reacknowledge the chassis that raised the fault.

Step 2 Physically unplug and replug the power cord into the chassis.

Step 3 Verify that the I/O modules are functional.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 456
mibFaultName: fltEquipmentChassisInoperable
moClass: equipment:Chassis
Type: equipment
```

fltEquipmentChassisPowerProblem

Fault Code:F0408

Message

Power state on chassis [id] is [power]

Explanation

This fault typically occurs when the chassis fails to meet the minimal power requirements defined in the power policy or when one or more power supplies have failed.

Recommended Action

If you see this fault, take the following actions:

Step 1 In Cisco UCS Manager, verify that all PSUs for the chassis are functional.

Step 2 Verify that all PSUs are seated properly within the chassis and are powered on.

Step 3 Physically unplug and replug the power cord into the chassis.

Step 4 If all PSUs are operating at maximum capacity, either add more PSUs to the chassis or redefine the power policy in Cisco UCS Manager.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-problem
CallHome: environmental
mibFaultCode: 408
mibFaultName: fltEquipmentChassisPowerProblem
moClass: equipment:Chassis
Type: environmental
```

fltEquipmentChassisSeeprom-inoperable

Fault Code:F0733

Message

Device [id] SEEPROM operability: [seepromOperState]

Explanation

This fault occurs in the unlikely event that the Chassis shared storage (SEEPROM) is not operational.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 733
mibFaultName: fltEquipmentChassisSeepromInoperable
moClass: equipment:Chassis
Type: equipment
```

fltEquipmentChassisThermalThresholdCritical

Fault Code:F0409

Message

Thermal condition on chassis [id] cause: [thermalStateQualifier]

Explanation

This fault occurs under the following conditions:

- If a component within a chassis is operating outside the safe thermal operating range.

- If the chassis controller in the IOM is unable to determine the thermal condition of a blade server, the **show tech-support** file for the chassis provides a more detailed report of the most severe thermal conditions currently applicable for that chassis.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the temperature readings for the blade servers and IOM and ensure they are within the recommended thermal safe operating range.

Step 2 If the fault reports a "Thermal Sensor threshold crossing in blade" error for one or more blade servers, check if DIMM or processor temperature related faults have been raised against that blade.

Step 3 If the fault reports a "Thermal Sensor threshold crossing in IOM" error for one or both the IOMs, check if thermal faults have been raised against that IOM. Those faults include details of the thermal condition.

Step 4 If the fault reports a "Missing or Faulty Fan" error, check on the status of that fan. If it needs replacement, create a **show tech-support** file for the chassis and contact Cisco TAC.

Step 5 If the fault reports a "No connectivity between IOM and blade" or "Thermal Sensor readings unavailable from blade" error, check if that blade server is operational and whether any faults have been raised against that blade server. In this situation, the chassis controller may go into a fail-safe operating mode and the fan speeds may increase as a precautionary measure.

Step 6 If the above actions did not resolve the issue and the condition persists, create a **show tech-support** file for Cisco UCS Manager and the chassis and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 409
mibFaultName: fltEquipmentChassisThermalThresholdCritical
moClass: equipment:Chassis
Type: environmental
```

fltEquipmentChassisThermalThresholdNonCritical

Fault Code:F0410

Message

Thermal condition on chassis [id] cause: [thermalStateQualifier]

Explanation

UCSM raises this fault under the following conditions:

- If a component within a chassis is operating outside the safe thermal operating range.
- If the chassis controller in the IOM is unable to determine the thermal condition of a blade server, the **show tech-support** file for the chassis provides a more detailed report of the most severe thermal conditions currently applicable for that chassis.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the temperature readings for the blade servers and IOM and ensure they are within the recommended thermal safe operating range.

Step 2 If the fault reports a "Thermal Sensor threshold crossing in blade" error for one or more blade servers, check if DIMM or processor temperature related faults have been raised against that blade.

Step 3 If the fault reports a "Thermal Sensor threshold crossing in IOM" error for one or both the IOMs, check if thermal faults have been raised against that IOM. Those faults include details of the thermal condition.

Step 4 If the fault reports a "Missing or Faulty Fan" error, check on the status of that fan. If it needs replacement, create a **show tech-support** file for the chassis and contact Cisco TAC.

Step 5 If the fault reports a "No connectivity between IOM and blade" or "Thermal Sensor readings unavailable from blade" error, check if that blade server is operational and whether any faults have been raised against that blade server. In this situation, the chassis controller may go into a fail-safe operating mode and the fan speeds may increase as a precautionary measure.

Step 6 If the above actions did not resolve the issue and the condition persists, create a **show tech-support** file for Cisco UCS Manager and the chassis and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 410
mibFaultName: fltEquipmentChassisThermalThresholdNonCritical
moClass: equipment:Chassis
Type: environmental
```

fltEquipmentChassisThermalThresholdNonRecoverable

Fault Code:F0411

Message

Thermal condition on chassis [id] cause:[thermalStateQualifier]

Explanation

UCSM raises this fault under the following conditions:

Step 1 If a component within a chassis is operating outside the safe thermal operating range.

Step 2 If the chassis controller in the IOM is unable to determine the thermal condition of a blade server, the **show tech-support** file for the chassis provides a more detailed report of the most severe thermal conditions currently applicable for that chassis.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the temperature readings for the blade servers and IOM and ensure they are within the recommended thermal safe operating range.

Step 2 If the fault reports a "Thermal Sensor threshold crossing in blade" error for one or more blade servers, check if DIMM or processor temperature related faults have been raised against that blade.

Step 3 If the fault reports a "Thermal Sensor threshold crossing in IOM" error for one or both the IOMs, check if thermal faults have been raised against that IOM. Those faults include details of the thermal condition.

Step 4 If the fault reports a "Missing or Faulty Fan" error, check on the status of that fan. If it needs replacement, create a **show tech-support** file for the chassis and contact Cisco TAC.

Step 5 If the fault reports a "No connectivity between IOM and blade" or "Thermal Sensor readings unavailable from blade" error, check if that blade server is operational and whether any faults have been raised against that blade server. In this situation, the chassis controller may go into a fail-safe operating mode and the fan speeds may increase as a precautionary measure.

Step 6 If the above actions did not resolve the issue and the condition persists, create a **show tech-support** file for Cisco UCS Manager and the chassis and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 411
mibFaultName: fltEquipmentChassisThermalThresholdNonRecoverable
moClass: equipment:Chassis
Type: environmental
```

fltEquipmentChassisUnacknowledged

Fault Code:F0400

Message

Chassis [id] connectivity configuration: [configState]

Explanation

This fault typically occurs when or more of the I/O module links from the chassis are unacknowledged.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the state of the I/O module links.

Step 2 Reacknowledge the chassis.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-unacknowledged
CallHome: none
mibFaultCode: 400
mibFaultName: fltEquipmentChassisUnacknowledged
moClass: equipment:Chassis
Type: connectivity
```

fltEquipmentChassisUnsupportedConnectivity

Fault Code:F0399

Message

Current connectivity for chassis [id] does not match discovery policy: [configState]

Explanation

This fault typically occurs when the current connectivity for a chassis does not match the configuration in the chassis discovery policy.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the correct number of links are configured in the chassis discovery policy.

Step 2 Check the state of the I/O module links.

Step 3 Reacknowledge the chassis.

Step 4 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: unsupported-connectivity-configuration
CallHome: none
mibFaultCode: 399
mibFaultName: fltEquipmentChassisUnsupportedConnectivity
moClass: equipment:Chassis
Type: connectivity
```

Chassis Slot-Related Faults

This section contains faults raised as a result of issues with a server slot in a chassis.

fltFabricComputeSlotEpMisplacedInChassisSlot

Fault Code:F0156

Message

Server, vendor([vendor]), model([model]), serial([serial]) in slot [chassisId]/[slotId] presence: [presence]

Explanation

This fault typically occurs when Cisco UCS Manager detects a server in a chassis slot that does not match what was previously equipped in the slot.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the previous server was intentionally removed and a new one was inserted, reacknowledge the server.

Step 2 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: server-moved
CallHome: none
mibFaultCode: 156
mibFaultName: fltFabricComputeSlotEpMisplacedInChassisSlot
moClass: fabric:ComputeSlotEp
Type: equipment
```

fltFabricComputeSlotEpServerIdentificationProblem

Fault Code:F0157

Message

Problem identifying server in slot [chassisId]/[slotId]

Explanation

This fault typically occurs when Cisco UCS Manager encountered a problem identifying the server in a chassis slot.

Recommended Action

If you see this fault, take the following actions:

Step 1 Remove and reinsert the server.

Step 2 Reacknowledge the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: server-identification-problem
CallHome: none
mibFaultCode: 157
mibFaultName: fltFabricComputeSlotEpServerIdentificationProblem
moClass: fabric:ComputeSlotEp
Type: equipment
```

Cisco UCS Manager-Related Faults

This section contains faults raised as a result of issues with Cisco UCS Manager.

fltMgmtPmonEntryUCSM process failure

Fault Code:F0867

Message

UCSM process [name] failed on FI [switchId]

Explanation

This fault occurs in an unlikely event of a Cisco UCS Manager process crash. Typically, the failed process restarts and recovers from the problem. Any pending operations are restarted after the process successfully restarts.

Recommended Action

If you see this fault and the process does not restart successfully, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: ucsm-process-failure
CallHome: none
mibFaultCode: 867
mibFaultName: fltMgmtPmonEntryUCSMProcessFailure
moClass: mgmt:PmonEntry
Type: management
```

Ethernet-Related Faults

This section contains faults raised as a result of issues with the Ethernet configuration for a vNIC.

fltEtherServerIntFIoHardware-failure

Fault Code:F0458

Message

IOM [transport] interface [portId] on chassis [id] oper state: [operState], reason: [stateQual]Fabric Interconnect [transport] interface [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual]IOM [transport] interface [portId] on fex [id] oper state: [operState], reason: [stateQual]

Explanation

This fault is raised on the IOM/FEX backplane ports when Cisco UCS Manager detects a hardware failure.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: interface-failed
CallHome: none
mibFaultCode: 458
mibFaultName: fltEtherServerIntFIoHardwareFailure
moClass: ether:ServerIntFIo
Type: network
```

fltFabricEthEstcPcEpDown

Fault Code:F0777

Message

[type] Member [slotId]/[portId] of Port-Channel [portId] on fabric interconnect [id] is down, membership: [membership]

Explanation

This fault typically occurs when a member port in an Ethernet port channel is down.

Recommended Action

If you see this fault, take the following action:

Step 1 Check the link connectivity on the upstream Ethernet switch.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: membership-down
CallHome: none
mibFaultCode: 777
mibFaultName: fltFabricEthEstcPcEpDown
moClass: fabric:EthEstcPcEp
Type: network
```

fltFabricEthLanPcEpDown

Fault Code:F0727

Message

[type] Member [slotId]/[portId] of Port-Channel [portId] on fabric interconnect [id] is down, membership: [membership]

Explanation

This fault typically occurs when a member port in an Ethernet port channel is down.

Recommended Action

If you see this fault, take the following action:

Step 1 Check the link connectivity on the upstream Ethernet switch.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: membership-down
CallHome: none
mibFaultCode: 727
mibFaultName: fltFabricEthLanPcEpDown
moClass: fabric:EthLanPcEp
Type: network
```

fltVnicEtherConfig-failed

Fault Code:F0169

Message

Eth vNIC [name], service profile [name] failed to apply configuration

Explanation

This fault typically occurs when Cisco UCS Manager could not place the vNIC on the vCon.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the server was successfully discovered.

Step 2 Verify that the correct type of adapters are installed on the server.

Step 3 Confirm that the vCon assignment is correct.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: configuration-failed
CallHome: none
mibFaultCode: 169
mibFaultName: fltVnicEtherConfigFailed
moClass: vnic:Ether
Type: configuration
```

Fabric Extender (FEX)-Related Faults

This section contains faults raised as a result of issues related to a fabric extender module in the Cisco UCS instance.

fltEquipmentFexFex-unsupported

Fault Code:F0905

Message

Fex [id] with model [model] is unsupported

Explanation

This fault typically occurs because Cisco UCS Manager has detected an unsupported FEX. For example, the model, vendor, or revision is not recognized.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that a supported FEX is installed.

Step 2 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: fex-unsupported
CallHome: none
```

mibFaultCode: 905
mibFaultName: fltEquipmentFexFexUnsupported
moClass: equipment:Fex
Type: equipment

fltEquipmentFexIdentity

Fault Code:F0703

Message

Fex [id] has a malformed FRU

Explanation

This fault typically occurs when the FRU information for a FEX is corrupted or malformed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: critical
Cause: fru-problem
CallHome: diagnostic
mibFaultCode: 703
mibFaultName: fltEquipmentFexIdentity
moClass: equipment:Fex
Type: equipment

fltEquipmentFexIdentity-unestablishable

Fault Code:F0778

Message

Fex [id] has an invalid FRU

Explanation

This fault typically occurs because Cisco UCS Manager detected an unsupported chassis. For example, the model, vendor, or revision is not recognized.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: identity-unestablishable
CallHome: none
mibFaultCode: 778
mibFaultName: fltEquipmentFexIdentityUnestablishable
moClass: equipment:Fex
Type: equipment
```

fltEquipmentFexPost-failure

Fault Code:F0702

Message

fex [id] POST failure

Explanation

This fault typically occurs when a FEX encounters errors during the Power On Self Test (POST). The impact of this fault varies depending on which errors were encountered during POST.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the POST results for the FEX. In the Cisco UCS Manager GUI, you can access the POST results from the General tab for the FEX. In the Cisco UCS Manager CLI, you can access the POST results by entering the **show post** command under the scope for the FEX.

Step 2 Reboot the FEX.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-problem
CallHome: diagnostic
mibFaultCode: 702
mibFaultName: fltEquipmentFexPostFailure
moClass: equipment:Fex
Type: equipment
```

Fabric Interconnect-Related Faults

This section contains faults raised as a result of issues with a fabric interconnect.

fltEtherSwitchIntFIoSatellite-wiring-problem

Fault Code:F0368

Message

Invalid connection between IOM port [chassisId]/[slotId]/[portId] and fabric interconnect [switchId]:[peerSlotId]/[peerPortId]

Explanation

This fault typically occurs as a result of a satellite wiring problem on the network-facing interface of an I/O module and Cisco UCS Manager detects that at least one IOM uplink is misconnected to one of the fabric interconnect ports.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify the fabric interconnect-chassis topology. Make sure each I/O module is connected to only one fabric interconnect.

Step 2 Ensure that the links are plugged in properly and re-acknowledge the chassis.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: satellite-mis-connected
CallHome: none
mibFaultCode: 368
mibFaultName: fltEtherSwitchIntFIoSatelliteWiringProblem
moClass: ether:SwitchIntFIo
Type: connectivity
```

fltEtherSwitchIntFIoSatellite-wiring-numbers-unexpected

Fault Code:F0440

Message

Chassis discovery policy conflict: Link IOM [chassisId]/[slotId]/[portId] to fabric interconnect [switchId]:[peerSlotId]/[peerPortId] not configured

Explanation

The configuration of the chassis discovery policy conflicts with the physical IOM uplinks. Cisco UCS Manager raises this fault when the chassis discovery policy is configured for more links than are physically cabled between the IOM uplinks on the chassis and the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 Ensure that you cable at least the same number of IOM uplinks as are configured in the chassis discovery policy, and that you configure the corresponding server ports on the fabric interconnect.

Step 2 Reacknowledge the chassis.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: unexpected-number-of-links
CallHome: none
mibFaultCode: 440
mibFaultName: fltEtherSwitchIntFIoSatelliteWiringNumbersUnexpected
moClass: ether:SwitchIntFIo
Type: connectivity
```

fltEquipmentSwitchCardPowerOff

Fault Code:F0884

Message

Switch card is powered down.

Explanation

This fault occurs when the switch card is powered down.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: power-down
CallHome: none
mibFaultCode: 884
mibFaultName: fltEquipmentSwitchCardPowerOff
moClass: equipment:SwitchCard
Type: equipment
```

fltExtmgmtIfMgmtifdown

Fault Code:F0736

Message

Management interface on Fabric Interconnect [id] is [operState]

Explanation

This fault occurs when a fabric interconnect reports that the operational state of an external management interface is down.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the state transitions of the external management interface on the fabric interconnect.

Step 2 Check the link connectivity for the external management interface.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: mgmtif-down
CallHome: diagnostic
mibFaultCode: 736
mibFaultName: fltExtmgmtIfMgmtifdown
moClass: extmgmt:If
Type: management
```

fltMgmtEntityDegraded

Fault Code:F0293

Message

Fabric Interconnect [id], HA Cluster interconnect link failure

Explanation

This fault occurs when one of the cluster links (either L1 or L2) of a fabric interconnect is not operationally up. This issue impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that both L1 and L2 links are properly connected between the fabric interconnects.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: link-down
CallHome: diagnostic
mibFaultCode: 293
mibFaultName: fltMgmtEntityDegraded
moClass: mgmt:Entity
Type: network
```

fltMgmtEntityDevice-1-shared-storage-error

Fault Code:F0863

Message

device [chassis1], error accessing shared-storage

Explanation

This fault occurs in an unlikely event that the shared storage selected for writing the cluster state is not accessible. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.lt;br/

Fault Details

```
Severity: warning
Cause: device-shared-storage-error
CallHome: none
mibFaultCode: 863
mibFaultName: fltMgmtEntityDevice1SharedStorageError
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityDevice-2-shared-storage error

Fault Code:F0864

Message

device [chassis2], error accessing shared-storage

Explanation

This fault occurs in an unlikely event that the shared storage selected for writing the cluster state is not accessible. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.lt;br/

Fault Details

```
Severity: warning
Cause: device-shared-storage-error
CallHome: none
mibFaultCode: 864
mibFaultName: fltMgmtEntityDevice2SharedStorageError
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityDevice-3-shared-storage error

Fault Code:F0865

Message

device [chassis3], error accessing shared-storage

Explanation

This fault occurs in an unlikely event that the shared storage selected for writing the cluster state is not accessible. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.lt;br/

Fault Details

```
Severity: warning
Cause: device-shared-storage-error
CallHome: none
mibFaultCode: 865
mibFaultName: fltMgmtEntityDevice3SharedStorageError
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityDown

Fault Code:F0294

Message

Fabric Interconnect [id], HA Cluster interconnect total link failure

Explanation

This fault occurs when both cluster links (L1 and L2) of the fabric interconnects are in a link-down state. This issue impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that both L1 and L2 links are properly connected between the fabric interconnects.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: link-down
CallHome: diagnostic
mibFaultCode: 294
mibFaultName: fltMgmtEntityDown
moClass: mgmt:Entity
Type: network
```

fltMgmtEntityElection-failure

Fault Code:F0428

Message

Fabric Interconnect [id], election of primary managemt instance has failed

Explanation

This fault occurs in an unlikely event that the fabric interconnects in a cluster configuration could not reach an agreement for selecting the primary fabric interconnect. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the initial setup configuration is correct on both fabric interconnects.

Step 2 Verify that the L1 and L2 links are properly connected between the fabric interconnects.

Step 3 In the Cisco UCS Manager CLI, run the **cluster force primary** local-mgmt command on one fabric interconnect.

Step 4 Reboot the fabric interconnects.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: election-failure
CallHome: diagnostic
mibFaultCode: 428
mibFaultName: fltMgmtEntityElectionFailure
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityHa-not-ready

Fault Code:F0429

Message

Fabric Interconnect [id], HA functionality not ready

Explanation

This fault occurs if Cisco UCS Manager cannot discover or communicate with one or more chassis or rack servers to write the HA Cluster state. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the initial setup configuration is correct on both fabric interconnects.

Step 2 Verify that the L1 and L2 links are properly connected between the fabric interconnects.

Step 3 Verify that the IOMs and/or FEXes are reachable and the server ports are enabled and operationally up.

Step 4 Verify that the chassis and/or rack servers are powered up and reachable

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: ha-not-ready
CallHome: none
mibFaultCode: 429
mibFaultName: fltMgmtEntityHaNotReady
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityHa-ssh-keys-mismatched

Fault Code:F0866

Message

Fabric Interconnect [id], management services, mismatched SSH keys

Explanation

This fault indicates that one of the following scenarios has occurred:

- The internal SSH keys used for HA in the cluster configuration are mismatched. This causes certain operations to fail.
- Another fabric interconnect is connected to the primary fabric interconnect in the cluster without first erasing the existing configuration in the primary.

Recommended Action

If you see this fault, take the following actions:

Step 1 Log into the Cisco UCS Manager CLI on the subordinate fabric interconnect.

Step 2 Enter **connect local-mgmt**

Step 3 Enter **erase configuration** to erase the configuration on the subordinate fabric interconnect and reboot it.

Step 4 When the secondary fabric interconnect has rebooted, reconfigure it for the cluster.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: ha-ssh-keys-mismatched
CallHome: none
mibFaultCode: 866
mibFaultName: fltMgmtEntityHaSshKeysMismatched
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityManagement-services-failure

Fault Code:F0451

Message

Fabric Interconnect [id], management services have failed

Explanation

This fault occurs in an unlikely event that management services fail on a fabric interconnect. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the initial setup configuration is correct on both fabric interconnects.

Step 2 Verify that the L1 and L2 links are properly connected between the fabric interconnects.

Step 3 Reboot the fabric interconnects.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: management-services-failure
CallHome: diagnostic
mibFaultCode: 451
mibFaultName: fltMgmtEntityManagementServicesFailure
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityManagement-services-unresponsive

Fault Code:F0452

Message

Fabric Interconnect [id], management services are unresponsive

Explanation

This fault occurs when management services on a fabric interconnect are unresponsive. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the initial setup configuration is correct on both fabric interconnects.

Step 2 Verify that the L1 and L2 links are properly connected between the fabric interconnects.

Step 3 Reboot the fabric interconnects.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: management-services-unresponsive
CallHome: diagnostic
mibFaultCode: 452
mibFaultName: fltMgmtEntityManagementServicesUnresponsive
moClass: mgmt:Entity
Type: management
```

fltMgmtEntityVersion-incompatible

Fault Code:F0430

Message

Fabric Interconnect [id], management services, incompatible versions

Explanation

This fault occurs if the Cisco UCS Manager software on the subordinate fabric interconnect is not the same release as that of the primary fabric interconnect. This impacts the full HA functionality of the fabric interconnect cluster.

Recommended Action

If you see this fault, take the following actions:

Step 1 Upgrade the Cisco UCS Manager software on the subordinate fabric interconnect to the same release as the primary fabric interconnect and verify that both fabric interconnects are running the same release of Cisco UCS Manager.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: version-incompatible
CallHome: diagnostic
mibFaultCode: 430
mibFaultName: fltMgmtEntityVersionIncompatible
moClass: mgmt:Entity
Type: management
```

fltNetworkElementInoperable

Fault Code:F0291

Message

Fabric Interconnect [id] operability: [operability]

Explanation

This fault typically occurs when the fabric interconnect cluster controller reports that the membership state of the fabric interconnect is down, indicating that the fabric interconnect is inoperable.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that both fabric interconnects in the cluster are running the same Kernel and System software versions.

Step 2 Verify that the fabric interconnects software version and the Cisco UCS Manager software versions are the same.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 291
mibFaultName: fltNetworkElementInoperable
moClass: network:Element
Type: equipment
```

fltNetworkElementInventoryFailed

Fault Code:F0885

Message

Fabric Interconnect [id] inventory is not complete: [inventoryStatus]

Explanation

Cisco UCS Manager raises this fault when the management subsystem is unable to perform an inventory of the physical components, such as I/O cards or physical ports.

Recommended Action

If you see this fault, take the following actions:

Step 1 Ensure that both fabric interconnects in an HA cluster are running the same software versions.

Step 2 Ensure that the fabric interconnect software is a version that is compatible with the Cisco UCS Manager software.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: inventory-failed
CallHome: diagnostic
mibFaultCode: 885
```

mibFaultName: fltNetworkElementInventoryFailed
moClass: network:Element
Type: equipment

fltStorageItemCapacityExceeded

Fault Code:F0182

Message

Disk usage for partition [name] on fabric interconnect [id] exceeded 70%

Explanation

This fault occurs when the partition disk usage exceeds 70% but is less than 90%.

Recommended Action

If you see this fault, take the following actions:

Step 1 Reduce the partition disk usage to less than 70% by deleting unused and unnecessary files.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: minor
Cause: capacity-exceeded
CallHome: none
mibFaultCode: 182
mibFaultName: fltStorageItemCapacityExceeded
moClass: storage:Item
Type: environmental

fltStorageItemCapacityWarning

Fault Code:F0183

Message

Disk usage for partition [name] on fabric interconnect [id] exceeded 90%

Explanation

This fault occurs when the partition disk usage exceeds 90%.

Recommended Action

If you see this fault, take the following actions:

Step 1 Reduce the partition disk usage to less than 90% by deleting unused and unnecessary files.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: capacity-exceeded
CallHome: none
mibFaultCode: 183
mibFaultName: fltStorageItemCapacityWarning
moClass: storage:Item
Type: environmental
```

Fan-Related Faults

This section contains faults raised as a result of issues related to a fan or fan module in the Cisco UCS instance.

fltEquipmentFanDegraded

Fault Code:F0371

Message

Fan [id] in Fan Module [tray]-[id] under chassis [id] operability: [operability]Fan [id] in fabric interconnect [id] operability: [operability]Fan [id] in fex [id] operability: [operability]Fan [id] in Fan Module [tray]-[id] under server [id] operability: [operability]

Explanation

This fault occurs when one or more fans in a fan module are not operational, but at least one fan is operational.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the fan module.

Step 2 Review the Cisco UCS Site Preparation Guide and ensure the fan module has adequate airflow, including front and back clearance.

Step 3 Verify that the air flows are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace the faulty fan modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: equipment-degraded
CallHome: none
mibFaultCode: 371
mibFaultName: fltEquipmentFanDegraded
moClass: equipment:Fan
Type: equipment
```

fltEquipmentFanInoperable

Fault Code:F0373

Message

Fan [id] in Fan Module [tray]-[id] under chassis [id] operability: [operability]Fan [id] in fabric interconnect [id] operability: [operability]Fan [id] in fex [id] operability: [operability]Fan [id] in Fan Module [tray]-[id] under server [id] operability: [operability]

Explanation

This fault occurs if a fan is not operational.

Recommended Action

If you see this fault, take the following actions:

Step 1 Remove fan module and re-install the fan module again. Remove only one fan module at a time.

Step 2 Replace fan module with a different fan module

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: environmental
mibFaultCode: 373
mibFaultName: fltEquipmentFanInoperable
moClass: equipment:Fan
Type: equipment
```

fltEquipmentFanMissing

Fault Code:F0434

Message

Fan [id] in fabric interconnect [id] presence: [presence]Fan [id] in fex [id] presence: [presence]Fan [id] in Fan Module [tray]-[id] under server [id] presence: [presence]

Explanation

This fault occurs in the unlikely event that a fan in a fan module cannot be detected.

Recommended Action

If you see this fault, take the following actions:

Step 1 Insert/reinsert the fan module in the slot that is reporting the issue.

Step 2 Replace the fan module with a different fan module, if available.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-missing
CallHome: none
mibFaultCode: 434
mibFaultName: fltEquipmentFanMissing
moClass: equipment:Fan
Type: equipment
```

fltEquipmentFanModuleDegraded

Fault Code:F0480

Message

Fan module [tray]-[id] in chassis [id] operability: [operability]Fan module [tray]-[id] in server [id] operability: [operability]Fan module [tray]-[id] in fabric interconnect [id] operability: [operability]

Explanation

This fault occurs when a fan module is not operational.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the fan module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the fan module has adequate airflow, including front and back clearance.

Step 3 Verify that the air flows for the fan module are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: equipment-degraded
CallHome: none
mibFaultCode: 480
mibFaultName: fltEquipmentFanModuleDegraded
moClass: equipment:FanModule
Type: equipment
```

fltEquipmentFanModuleIdentity

Fault Code:F0406

Message

Fan Module [tray]-[id] in chassis [id] has a malformed FRUFan Module [tray]-[id] in server [id] has a malformed FRUFan Module [tray]-[id] in fabric interconnect [id] has a malformed FRU

Explanation

This fault typically occurs when the FRU information for a fan module is corrupted or malformed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: fru-problem
CallHome: diagnostic
mibFaultCode: 406
mibFaultName: fltEquipmentFanModuleIdentity
moClass: equipment:FanModule
Type: equipment
```

fltEquipmentFanModuleInoperable

Fault Code:F0794

Message

Fan module [tray]-[id] in chassis [id] operability: [operability]Fan module [tray]-[id] in server [id] operability: [operability]Fan module [tray]-[id] in fabric interconnect [id] operability: [operability]

Explanation

This fault occurs if a fan module is not operational.

Recommended Action

If you see this fault, take the following actions:

Step 1 Remove and reinstall the fan module. If multiple fans are affected by this fault, remove and reinstall one fan module at a time.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: environmental
mibFaultCode: 794
mibFaultName: fltEquipmentFanModuleInoperable
moClass: equipment:FanModule
Type: equipment
```

fltEquipmentFanModuleMissing

Fault Code:F0377

Message

Fan module [tray]-[id] in chassis [id] presence: [presence]Fan module [tray]-[id] in server [id] presence: [presence]Fan module [tray]-[id] in fabric interconnect [id] presence: [presence]

Explanation

This fault occurs if a fan Module slot is not equipped or removed from its slot

Recommended Action

If you see this fault, take the following actions:

Step 1 If the reported slot is empty, insert a fan module into the slot.

Step 2 If the reported slot contains a fan module, remove and reinsert the fan module.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-missing
CallHome: none
mibFaultCode: 377
mibFaultName: fltEquipmentFanModuleMissing
moClass: equipment:FanModule
Type: equipment
```

fltEquipmentFanModuleThermalThresholdCritical

Fault Code:F0382

Message

Fan module [tray]-[id] in chassis [id] temperature: [thermal]Fan module [tray]-[id] in server [id] temperature: [thermal]Fan module [tray]-[id] in fabric interconnect [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a fan module has exceeded a critical threshold value. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the fan module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the fan modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace faulty fan modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major f
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 382
mibFaultName: fltEquipmentFanModuleThermalThresholdCritical
moClass: equipment:FanModule
Type: environmental
```

fltEquipmentFanModuleThermalThresholdNonCritical

Fault Code:F0380

Message

Fan module [tray]-[id] in chassis [id] temperature: [thermal]Fan module [tray]-[id] in server [id] temperature: [thermal]Fan module [tray]-[id] in fabric interconnect [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a fan module has exceeded a non-critical threshold value, but is still below the critical threshold. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the fan module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the fan modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace faulty fan modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 380
mibFaultName: fltEquipmentFanModuleThermalThresholdNonCritical
moClass: equipment:FanModule
Type: environmental
```

fltEquipmentFanModuleThermalThresholdNonRecoverable

Fault Code:F0384

Message

Fan module [tray]-[id] in chassis [id] temperature: [thermal]Fan module [tray]-[id] in server [id] temperature: [thermal]Fan module [tray]-[id] in fabric interconnect [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a fan module has been out of operating range, and the issue is not recoverable. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the fan module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the fan modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace faulty fan modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 384
mibFaultName: fltEquipmentFanModuleThermalThresholdNonRecoverable
moClass: equipment:FanModule
Type: environmental
```

fltEquipmentFanPerfThresholdCritical

Fault Code:F0396

Message

Fan [id] in Fan Module [tray]-[id] under chassis [id] speed: [perf]Fan [id] in fabric interconnect [id] speed: [perf]Fan [id] in Fan Module [tray]-[id] under server [id] speed: [perf]

Explanation

This fault occurs when the fan speed read from the fan controller does not match the desired fan speed and has exceeded the critical threshold and is in risk of failure. This can indicate a problem with a fan or with the reading from the fan controller.

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor the fan status.

Step 2 If the problem persists for a long period of time or if other fans do not show the same problem, reseat the fan.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file for the chassis and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: performance-problem
CallHome: diagnostic
mibFaultCode: 396
mibFaultName: fltEquipmentFanPerfThresholdCritical
moClass: equipment:Fan
Type: equipment
```

fltEquipmentFanPerfThresholdLowerNonRecoverable

Fault Code:F0484

Message

Fan [id] in Fan Module [tray]-[id] under chassis [id] speed: [perf]Fan [id] in fabric interconnect [id] speed: [perf]Fan [id] in Fan Module [tray]-[id] under server [id] speed: [perf]

Explanation

This fault occurs when the fan speed reading from the fan controller is far below the desired fan speed, and the fan has likely failed.

Recommended Action

If you see this fault, create a detailed **show tech-support** file for the chassis and replace the fan module. If necessary, contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: performance-problem
CallHome: diagnostic
mibFaultCode: 484
mibFaultName: fltEquipmentFanPerfThresholdLowerNonRecoverable
moClass: equipment:Fan
Type: equipment
```

fltEquipmentFanPerfThresholdNonCritical

Fault Code:F0395

Message

Fan [id] in Fan Module [tray]-[id] under chassis [id] speed: [perf]Fan [id] in fabric interconnect [id] speed: [perf]Fan [id] in Fan Module [tray]-[id] under server [id] speed: [perf]

Explanation

This fault occurs when the fan speed reading from the fan controller does not match the desired fan speed and is outside of the normal operating range. This can indicate a problem with a fan or with the reading from the fan controller.

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor the fan status.

Step 2 If the problem persists for a long period of time or if other fans do not show the same problem, reseat the fan.

Step 3 Replace the fan module.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: performance-problem
CallHome: diagnostic
mibFaultCode: 395
mibFaultName: fltEquipmentFanPerfThresholdNonCritical
moClass: equipment:Fan
Type: equipment
```

fltEquipmentFanPerfThresholdNonRecoverable

Fault Code:F0397

Message

Fan [id] in Fan Module [tray]-[id] under chassis [id] speed: [perf]Fan [id] in fabric interconnect [id] speed: [perf]Fan [id] in Fan Module [tray]-[id] under server [id] speed: [perf]

Explanation

This fault occurs when the fan speed read from the fan controller has far exceeded the desired fan speed. It frequently indicates that the fan has failed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Replace the fan.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: performance-problem
CallHome: diagnostic
mibFaultCode: 397
mibFaultName: fltEquipmentFanPerfThresholdNonRecoverable
moClass: equipment:Fan
Type: equipment
```

Fibre Channel-Related Faults

This section contains the following faults raised as a result of issues with the Fibre Channel configuration for a vHBA.

fltVnicFcConfig-failed

Fault Code:F0170

Message

FC vHBA [name], service profile [name] failed to apply configuration

Explanation

This fault typically occurs when Cisco UCS Manager could not place the vHBA on the vCon.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the server was successfully discovered.

Step 2 Verify that the correct type of adapters are installed on the server.

Step 3 Confirm that the vCon assignment is correct.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
```

```
Cause: configuration-failed
CallHome: none
mibFaultCode: 170
mibFaultName: fltVnicFcConfigFailed
moClass: vnic:Fc
Type: configuration
```

Firmware-Related Faults

This section contains faults raised as a result of issues related to a firmware upgrade or to running firmware on a component in the Cisco UCS instance.

fltEquipmentIOCardAutoUpgradingFirmware

Fault Code:F0435

Message

IOM [chassisId]/[id] ([switchId]) is auto upgrading firmware

Explanation

This fault typically occurs when an I/O module is auto upgrading. Auto-upgrade occurs when the firmware version on the IOM is incompatible with the firmware version on the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the IOM and fabric interconnects are not running the same firmware version, wait for the auto-upgrade to complete.

Step 2 When the IOM upgrade is completed, verify that Cisco UCS Manager has cleared this fault.

Step 3 If you see this fault after the IOM overall status changes to operable, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: auto-firmware-upgrade
CallHome: none
mibFaultCode: 435
mibFaultName: fltEquipmentIOCardAutoUpgradingFirmware
moClass: equipment:IOCard
Type: connectivity
```

fltEquipmentIOCardFirmwareUpgrade

Fault Code:F0398

Message

Chassis controller in IOM [chassisId]/[id] ([switchId]) firmware upgrade problem: [upgradeStatus]

Explanation

This fault typically occurs when an IOM upgrade fails.

Recommended Action

If you see this fault, take the following actions:

Step 1 On the FSM tab for the IOM, verify whether FSM for the upgrade completed successfully or failed.

Step 2 If the FSM failed, review the error message in the FSM.

Step 3 If the error message is self explanatory, verify the physical connectivity. For example, an error message could be No Connection to Endpoint or Link Down.

Step 4 If the above action did not resolve the issue and the fault persists, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: firmware-upgrade-problem
CallHome: none
mibFaultCode: 398
mibFaultName: fltEquipmentIOCardFirmwareUpgrade
moClass: equipment:IOCard
Type: equipment
```

fltFirmwareBootUnitActivateStatusFailed

Fault Code:F0856

Message

Activation failed and Activate Status set to failed.

Explanation

This fault typically occurs for the following reasons: when firmware activation fails, or if the after activation running image is not the corresponding startup image.

- Firmware activation failed.
- The version of firmware running on the server after activation is not the version listed in Cisco UCS Manager as the startup image.

Recommended Action

If you see this fault, take the following actions:

Step 1 Go to FSM tab for the endpoint on which the fault is raised and review the error description for the reason that the activation failed.

Step 2 If the FSM failed, review the error message in the FSM.

Step 3 If possible, correct the problem described in the error message.

Step 4 If the problem persists, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: activation-failed
CallHome: none
mibFaultCode: 856
mibFaultName: fltFirmwareBootUnitActivateStatusFailed
moClass: firmware:BootUnit
Type: management
```

fltFirmwareBootUnitCantBoot

Fault Code:F0471

Message

unable to boot the startup image. End point booted with backup image

Explanation

This fault typically occurs when the startup firmware image on an endpoint is corrupted or invalid, and the endpoint cannot boot from that image.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the fault and the error message on the FSM tab for the endpoint to determine why the firmware image is unusable. The error message usually includes an explanation for why the endpoint could not boot from the startup image, such as Bad-Image or Checksum Failed.

Step 2 If the firmware image is bad or corrupted, download another copy from the Cisco website and update the startup version on the endpoint with the new image.

Step 3 If the fault persists, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: image-cannot-boot
CallHome: none
mibFaultCode: 471
mibFaultName: fltFirmwareBootUnitCantBoot
moClass: firmware:BootUnit
Type: management
```

fltFirmwarePackItemImageMissing

Fault Code:F0436

Message

[type] image with vendor [hwVendor], model [hwModel] and version [version] is deleted

Explanation

This fault typically occurs when the image to which a firmware package item refers is missing.

Recommended Action

If you see this fault, take the following actions:

Step 1 In Cisco UCS Manager GUI, navigate to the Firmware Management Images tab and determine whether the missing image is available or not.

Step 2 If the image is present, click on it to verify the model and vendor.

Step 3 If the image for the required model and vendor is not present, download that image or bundle from the Cisco.com website.

Step 4 If the image is present and the fault persists, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: image-deleted
CallHome: none
mibFaultCode: 436
mibFaultName: fltFirmwarePackItemImageMissing
moClass: firmware:PackItem
Type: management
```

fltFirmwareUpdatableImageUnusable

Fault Code:F0470

Message

backup image is unusable. reason: [operStateQual]

Explanation

This fault typically occurs when the backup firmware image on an endpoint is unusable.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the fault and the error message on the FSM tab for the endpoint to determine why the firmware image is unusable.

Step 2 If the firmware image is bad or corrupted, download another copy from the Cisco website and update the backup version on the endpoint with the new image.

Step 3 If the image is present and the fault persists, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: image-unusable
CallHome: none
mibFaultCode: 470
mibFaultName: fltFirmwareUpdatableImageUnusable
moClass: firmware:Updatable
Type: management
```

I/O Module-Related Faults

This section contains faults raised as a result of issues related to an I/O module in the Cisco UCS instance.

fltEquipmentIOCardIdentity

Fault Code:F0405

Message

[side] IOM [chassisId]/[id] ([switchId]) has a malformed FRU

Explanation

This fault typically occurs when the FRU information for an I/O module is corrupted or malformed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: fru-problem
CallHome: diagnostic
mibFaultCode: 405
mibFaultName: fltEquipmentIOCardIdentity
moClass: equipment:IOCard
Type: equipment
```

fltEquipmentIOCardInaccessible

Fault Code:F0478

Message

[side] IOM [chassisId]/[id] ([switchId]) is inaccessible

Explanation

This fault typically occurs because an I/O module has lost its connection to the fabric interconnects. In a cluster configuration, the chassis fails over to the other I/O module. For a standalone configuration, the chassis associated with the I/O module loses network connectivity. This is a critical fault because it can result in the loss of network connectivity and disrupt data traffic through the I/O module.

Recommended Action

If you see this fault, take the following actions:

Step 1 Wait a few minutes to see if the fault clears. This is typically a temporary issue, and can occur after a firmware upgrade.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: equipment-inaccessible
CallHome: diagnostic
mibFaultCode: 478
mibFaultName: fltEquipmentIOCardInaccessible
moClass: equipment:IOCard
Type: equipment
```

fltEquipmentIOCardPeerDisconnected

Fault Code:F0403

Message

IOM [chassisId]/[id] ([switchId]) peer connectivity: [peerCommStatus]

Explanation

This fault typically occurs when an I/O module is unable to communicate with its peer I/O module.

Recommended Action

If you see this fault, take the following actions:

Step 1 Wait a few minutes to see if the fault clears. This is typically a temporary issue, and can occur after a firmware upgrade.

Step 2 If the fault does not clear after a few minutes, remove and reinsert the I/O module.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-disconnected
CallHome: none
mibFaultCode: 403
mibFaultName: fltEquipmentIOCardPeerDisconnected
moClass: equipment:IOCard
Type: connectivity
```

fltEquipmentIOCardPost-failure

Fault Code:F0481

Message

[side] IOM [chassisId]/[id] ([switchId]) POST failure

Explanation

This fault typically occurs when an I/O module encounters errors during the Power On Self Test (POST). The impact of this fault varies according to the errors that were encountered during POST.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the POST results for the I/O module. In Cisco UCS Manager GUI, you can access the POST results from the General tab for the I/O module. In Cisco UCS Manager CLI, you can access the POST results through the show post command under the scope for the I/O module.

Step 2 Reboot the I/O module.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-problem
CallHome: diagnostic
mibFaultCode: 481
mibFaultName: fltEquipmentIOCardPostFailure
moClass: equipment:IOCard
Type: equipment
```

fltEquipmentIOCardRemoved

Fault Code:F0376

Message

[side] IOM [chassisId]/[id] ([switchId]) is removed

Explanation

This fault typically occurs because an I/O module is removed from the chassis. In a cluster configuration, the chassis fails over to the other I/O module. For a standalone configuration, the chassis associated with the I/O module loses network connectivity. This is a critical fault because it can result in the loss of network connectivity and disrupt data traffic through the I/O module.

Recommended Action

If you see this fault, take the following actions:

Step 1 Reinsert the I/O module and configure the fabric-interconnect ports connected to it as server ports and wait a few minutes to see if the fault clears.

Step 2 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: equipment-removed
CallHome: none
```

mibFaultCode: 376
mibFaultName: fltEquipmentIOCardRemoved
moClass: equipment:IOCard
Type: equipment

fltEquipmentIOCardThermalProblem

Fault Code:F0379

Message

[side] IOM [chassisId]/[id] ([switchId]) operState: [operState]

Explanation

This fault occurs when there is a thermal problem on an I/O module. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the I/O module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the I/O modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace faulty I/O modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: major
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 379
mibFaultName: fltEquipmentIOCardThermalProblem
moClass: equipment:IOCard

Type: environmental

fltEquipmentIOCardThermalThresholdCritical

Fault Code:F0730

Message

[side] IOM [chassisId]/[id] ([switchId]) temperature: [thermal]

Explanation

This fault occurs when the temperature of an I/O module has exceeded a critical threshold value. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the I/O module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the chassis and I/O modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis and I/O module are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace the faulty I/O modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: major
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 730
mibFaultName: fltEquipmentIOCardThermalThresholdCritical
moClass: equipment:IOCard
Type: environmental

fltEquipmentIOCardThermalThresholdNonCritical

Fault Code:F0729

Message

[side] IOM [chassisId]/[id] ([switchId]) temperature: [thermal]

Explanation

This fault occurs when the temperature of an I/O module has exceeded a non-critical threshold value, but is still below the critical threshold. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the I/O module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the chassis and I/O modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis and I/O module are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 729
mibFaultName: fltEquipmentIOCardThermalThresholdNonCritical
moClass: equipment:IOCard
Type: environmental
```

fltEquipmentIOCardThermalThresholdNonRecoverable

Fault Code:F0731

Message

[side] IOM [chassisId]/[id] ([switchId]) temperature: [thermal]

Explanation

This fault occurs when the temperature of an I/O module has been out of the operating range, and the issue is not recoverable. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the I/O module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the chassis and I/O modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis and I/O module are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace the faulty I/O modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 731
mibFaultName: fltEquipmentIOCardThermalThresholdNonRecoverable
moClass: equipment:IOCard
Type: environmental
```

fltEquipmentIOCardUnacknowledged

Fault Code:F0402

Message

IOM [chassisId]/[id] ([switchId]) connectivity configuration: [configState]

Explanation

This fault typically occurs when an I/O module is unacknowledged.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the state of the I/O module links.

Step 2 Reacknowledge the chassis.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-unacknowledged
CallHome: none
mibFaultCode: 402
mibFaultName: fltEquipmentIOCardUnacknowledged
moClass: equipment:IOCard
Type: connectivity
```

fltEquipmentIOCardUnsupportedConnectivity

Fault Code:F0401

Message

IOM [chassisId]/[id] ([switchId]) current connectivity does not match discovery policy: [configState]

Explanation

This fault typically occurs when the current connectivity for an I/O module does not match the configuration in the chassis discovery policy.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the correct number of links are configured in the chassis discovery policy.

Step 2 Check the state of the I/O module links.

Step 3 Reacknowledge the chassis.

Step 4 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: unsupported-connectivity-configuration
CallHome: none
mibFaultCode: 401
mibFaultName: fltEquipmentIOCardUnsupportedConnectivity
moClass: equipment:IOCard
Type: connectivity
```

License-Related Faults

This section contains faults raised as a result of issues related to licensing.

fltLicenseFileBadLicenseFile

Fault Code:F0677

Message

license file [name] on fabric-interconnect [scope] can not be installed

Explanation

The installation of a license file on the fabric interconnect failed. This fault typically occurs if the license file is badly formatted or its host ID does not match that of the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 In the Cisco UCS Manager CLI, check the host IDs for both fabric interconnects. You can access the host ID information by entering the **show server-host-id detail** command under the license scope.

Step 2 Match the host IDs with the contents of the license file. If the host ID matches that of one of the fabric interconnects, create a **show tech-support** file and contact Cisco TAC. If it does not match, contact Cisco TAC to obtain the correct license File.

Fault Details

```
Severity: critical
Cause: license-file-uninstallable
CallHome: none
mibFaultCode: 677
mibFaultName: fltLicenseFileBadLicenseFile
moClass: license:File
Type: management
```

fltLicenseFileFileNotDeleted

Fault Code:F0678

Message

license file [name] from fabric-interconnect [scope] could not be deleted

Explanation

The deletion of a license file on the fabric interconnect has failed. This fault typically occurs if license framework is not able to delete a file.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: license-file-not-deleted
CallHome: none
mibFaultCode: 678
mibFaultName: fltLicenseFileFileNotDeleted
moClass: license:File
Type: management
```

fltLicenseInstanceGracePeriodWarning1

Fault Code:F0670

Message

license for [feature] on fabric-interconnect [scope] has entered into the grace period.

Explanation

At least one port on the fabric interconnect is running in the grace period. This fault typically occurs if one or more ports on the fixed module are enabled after all default licenses have been assigned to a port.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the number of licenses installed and being used on each fabric interconnect. In the Cisco UCS Manager GUI, you can access the licensing information from the Admin tab for the fabric interconnect. In the Cisco UCS Manager CLI, you can access the licensing information by entering the **show usage detail** command under the license scope.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: license-graceperiod-entered
CallHome: none
mibFaultCode: 670
mibFaultName: fltLicenseInstanceGracePeriodWarning1
moClass: license:Instance
Type: management
```

fltLicenseInstanceGracePeriodWarning2

Fault Code:F0671

Message

license for [feature] on fabric-interconnect [scope] is running in the grace period for more than 10 days

Explanation

At least one port on the fabric interconnect has been running in the grace period for more than 10 days. This fault typically occurs if one or more ports on the fixed module are enabled after all default licenses have been assigned to ports and the unlicensed ports have been running for more than 10 days.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the number of licenses installed and consumed on each fabric interconnect. In the Cisco UCS Manager GUI, you can access the licensing information from the Admin tab for the fabric interconnect. In the Cisco UCS Manager CLI, you can access the licensing information by entering the **show usage detail** command under the license scope.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: license-graceperiod-10days
CallHome: none
mibFaultCode: 671
mibFaultName: fltLicenseInstanceGracePeriodWarning2
moClass: license:Instance
Type: management
```

fltLicenseInstanceGracePeriodWarning3

Fault Code:F0672

Message

license for [feature] on fabric-interconnect [scope] is running in the grace period for more than 30 days

Explanation

At least one port on the fabric interconnect has been running in the grace period for more than 30 days. This fault typically occurs if one or more ports on the fixed module are enabled after all default licenses have been assigned to ports and the unlicensed ports have been running for more than 30 days.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the number of licenses installed and consumed on each fabric interconnect. In the Cisco UCS Manager GUI, you can access the licensing information from the Admin tab for the fabric interconnect. In the Cisco UCS Manager CLI, you can access the licensing information by entering the **show usage detail** command under the license scope.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: license-graceperiod-30days
CallHome: none
mibFaultCode: 672
mibFaultName: fltLicenseInstanceGracePeriodWarning3
moClass: license:Instance
Type: management
```

fltLicenseInstanceGracePeriodWarning4

Fault Code:F0673

Message

license for [feature] on fabric-interconnect [scope] is running in the grace period for more than 60 days

Explanation

At least one port on the fabric interconnect has been running in the grace period for more than 60 days. This fault typically occurs if one or more ports on the fixed module are enabled after all default licenses have been assigned to ports and the unlicensed ports have been running for more than 60 days.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the number of licenses installed and consumed on each fabric interconnect. In the Cisco UCS Manager GUI, you can access the licensing information from the Admin tab for the fabric interconnect. In the Cisco UCS Manager CLI, you can access the licensing information by entering the **show usage detail** command under the license scope.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: license-graceperiod-60days
CallHome: none
mibFaultCode: 673
mibFaultName: fltLicenseInstanceGracePeriodWarning4
moClass: license:Instance
Type: management
```

fltLicenseInstanceGracePeriodWarning5

Fault Code:F0674

Message

license for [feature] on fabric-interconnect [scope] is running in the grace period for more than 90 days

Explanation

At least one port on the fabric interconnect has been running in the grace period for more than 90 days. This fault typically occurs if one or more ports on the fixed module are enabled after all default licenses have been assigned to ports and the unlicensed ports have been running for more than 90 days.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the number of licenses installed and consumed on each fabric interconnect. In the Cisco UCS Manager GUI, you can access the licensing information from the Admin tab for the fabric interconnect. In the Cisco UCS Manager CLI, you can access the licensing information by entering the **show usage detail** command under the license scope.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: license-graceperiod-90days
CallHome: none
mibFaultCode: 674
mibFaultName: fltLicenseInstanceGracePeriodWarning5
moClass: license:Instance
Type: management
```

fltLicenseInstanceGracePeriodWarning6

Fault Code:F0675

Message

license for [feature] on fabric-interconnect [scope] is running in the grace period for more than 119 days

Explanation

At least one port on the fabric interconnect has been running in the grace period for more than 119 days. This fault typically occurs if one or more ports on the fixed module are enabled after all default licenses have been assigned to ports and the unlicensed ports have been running for more than 119 days.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the number of licenses installed and consumed on each fabric interconnect. In the Cisco UCS Manager GUI, you can access the licensing information from the Admin tab for the fabric interconnect. In the Cisco UCS Manager CLI, you can access the licensing information by entering the **show usage detail** command under the license scope.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: license-graceperiod-119days
CallHome: none
mibFaultCode: 675
mibFaultName: fltLicenseInstanceGracePeriodWarning6
moClass: license:Instance
Type: management
```

fltLicenseInstanceGracePeriodWarning7

Fault Code:F0676

Message

Grace period for [feature] on fabric-interconnect [scope] is expired. Please acquire a license for the same.

Explanation

At least one port on the fabric interconnect has been running in the grace period for more than 120 days. This fault typically occurs if one or more ports on the fixed module are enabled after all default licenses have been assigned to ports and the unlicensed ports have been running for more than 120 days. At this stage, the system licensing state is set to expired.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the number of licenses installed and consumed on each fabric interconnect. In the Cisco UCS Manager GUI, you can access the licensing information from the Admin tab for the fabric interconnect. In the Cisco UCS Manager CLI, you can access the licensing information by entering the **show usage detail** command under the license scope.

Step 2 Disable the unlicensed ports to bring the number of enabled ports down to the number of total licenses.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC immediately to procure more licenses.

Fault Details

```
Severity: critical
Cause: license-graceperiod-expired
CallHome: environmental
mibFaultCode: 676
mibFaultName: fltLicenseInstanceGracePeriodWarning7
moClass: license:Instance
```

Type: management

Link-Related Faults

This section contains faults raised as a result of issues related to the links between a chassis or I/O module and a fabric interconnect.

fltEtherSwitchIntFIoSatellite-connection-absent

Fault Code:F0367

Message

No link between IOM port [chassisId]/[slotId]/[portId] and fabric interconnect [switchId]:[peerSlotId]/[peerPortId]

Explanation

This fault is raised when an I/O module fabric port, which links the I/O module port and the fabric interconnect, is not functional

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify the fabric interconnect-chassis topology. Make sure each I/O module is connected to only one fabric interconnect.

Step 2 Ensure that the fabric interconnect server port is configured and enabled.

Step 3 Ensure that the links are plugged in properly and reacknowledge the chassis.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: major
Cause: satellite-connection-absent
CallHome: none
mibFaultCode: 367
mibFaultName: fltEtherSwitchIntFIoSatelliteConnectionAbsent
moClass: ether:SwitchIntFIo
Type: connectivity

Memory-Related Faults

This section contains faults raised as issues with memory units or DIMMs in a server.

fltMemoryArrayVoltageThresholdCritical

Fault Code:F0190

Message

Memory array [id] on server [chassisId]/[slotId] voltage: [voltage]Memory array [id] on server [id] voltage: [voltage]

Explanation

This fault occurs when the memory array voltage exceeds the specified hardware voltage rating

Recommended Action

If you see this fault, take the following actions:

Step 1 If the SEL is enabled, look at the SEL statistics on the DIMM to determine which threshold was crossed.

Step 2 Monitor the memory array for further degradation.

Step 3 If the fault occurs on a blade server memory array, remove the blade and re-insert into the chassis.

Step 4 In Cisco UCS Manager, decommission and recommission the server.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 190
mibFaultName: fltMemoryArrayVoltageThresholdCritical
moClass: memory:Array
Type: environmental
```

fltMemoryArrayVoltageThresholdNonCritical

Fault Code:F0189

Message

Memory array [id] on server [chassisId]/[slotId] voltage: [voltage]Memory array [id] on server [id] voltage: [voltage]

Explanation

This fault occurs when the memory array voltage is out of normal operating range, but hasn't yet reached a critical stage. Typically the memory array recovers itself from this situation.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the SEL is enabled, look at the SEL statistics on the DIMM to determine which threshold was crossed.

Step 2 Monitor the memory array for further degradation.

Step 3 If the fault occurs on a blade server memory array, remove the blade and re-insert into the chassis.

Step 4 In Cisco UCS Manager, decommission and recommission the server.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 189
mibFaultName: fltMemoryArrayVoltageThresholdNonCritical
moClass: memory:Array
Type: environmental
```

fltMemoryArrayVoltageThresholdNonRecoverable

Fault Code:F0191

Message

Memory array [id] on server [chassisId]/[slotId] voltage: [voltage]Memory array [id] on server [id] voltage: [voltage]

Explanation

This fault occurs when the memory array voltage exceeded the specified hardware voltage rating and potentially memory hardware may be in damage or jeopardy

Recommended Action

If you see this fault, take the following actions:

Step 1 If the SEL is enabled, review the SEL statistics on the DIMM to determine which threshold was crossed.

Step 2 Monitor the memory array for further degradation.

Step 3 If the fault occurs on a blade server memory array, remove the server from the chassis and re-insert it.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 191
mibFaultName: fltMemoryArrayVoltageThresholdNonRecoverable
moClass: memory:Array
Type: environmental
```

fltMemoryBufferUnitThermalThresholdCritical

Fault Code:F0536

Message

Buffer Unit [id] on server [chassisId]/[slotId] temperature: [thermal]Buffer Unit [id] on server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a memory buffer unit on a blade or rack server exceeds a critical threshold value. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 536
mibFaultName: fltMemoryBufferUnitThermalThresholdCritical
moClass: memory:BufferUnit
Type: environmental
```

fltMemoryBufferUnitThermalThresholdNonCritical

Fault Code:F0535

Message

Buffer Unit [id] on server [chassisId]/[slotId] temperature: [thermal]Buffer Unit [id] on server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a memory buffer unit on a blade or rack server exceeds a non-critical threshold value, but is still below the critical threshold. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 535
mibFaultName: fltMemoryBufferUnitThermalThresholdNonCritical
moClass: memory:BufferUnit
Type: environmental
```

fltMemoryBufferUnitThermalThresholdNonRecoverable

Fault Code:F0537

Message

Buffer Unit [id] on server [chassisId]/[slotId] temperature: [thermal]Buffer Unit [id] on server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a memory buffer unit on a blade or rack server has been out of the operating range, and the issue is not recoverable. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 537
mibFaultName: fltMemoryBufferUnitThermalThresholdNonRecoverable
moClass: memory:BufferUnit
Type: environmental
```

fltMemoryUnitDegraded

Fault Code:F0184

Message

DIMM [location] on server [chassisId]/[slotId] operability: [operability]DIMM [location] on server [id] operability: [operability]

Explanation

This fault occurs when a DIMM is in a degraded operability state. This state typically occurs when an excessive number of correctable ECC errors are reported on the DIMM by the server BIOS.

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor the error statistics on the degraded DIMM through Cisco UCS Manager. If the high number of errors persists, there is a high possibility of the DIMM becoming inoperable.

Step 2 If the DIMM becomes inoperable, replace the DIMM.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: equipment-degraded
CallHome: none
mibFaultCode: 184
mibFaultName: fltMemoryUnitDegraded
moClass: memory:Unit
Type: equipment
```

fltMemoryUnitDisabled

Fault Code:F0844

Message

DIMM [location] on server [chassisId]/[slotId] operState: [operState]DIMM [location] on server [id] operaState: [operState]

Explanation

This fault is raised when the server BIOS disables a DIMM. The BIOS could disable a DIMM for several reasons, including incorrect location of the DIMM or incompatible speed.

Recommended Action

If you see this fault, refer to the Cisco UCS B-Series Troubleshooting Guide for information on how to resolve the DIMM issues.

Fault Details

```
Severity: major
Cause: equipment-disabled
CallHome: diagnostic
mibFaultCode: 844
mibFaultName: fltMemoryUnitDisabled
moClass: memory:Unit
Type: equipment
```

fltMemoryUnitIdentity-unestablishable

Fault Code:F0502

Message

DIMM [location] on server [chassisId]/[slotId] has an invalid FRUDIMM [location] on server [id] has an invalid FRU

Explanation

This fault typically occurs because Cisco UCS Manager has detected unsupported DIMM in the server. For example, the model, vendor, or revision is not recognized.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, you may have unsupported DIMMs or DIMM configuration in the server. Create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: identity-unestablishable
CallHome: none
mibFaultCode: 502
mibFaultName: fltMemoryUnitIdentityUnestablishable
moClass: memory:Unit
Type: equipment
```

fltMemoryUnitInoperable

Fault Code:F0185

Message

DIMM [location] on server [chassisId]/[slotId] operability: [operability]DIMM [location] on server [id] operability: [operability]

Explanation

This fault typically occurs because an above threshold number of correctable or uncorrectable errors has occurred on a DIMM. The DIMM may be inoperable.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the SEL is enabled, review the SEL statistics on the DIMM to determine which threshold was crossed.

Step 2 If necessary, replace the DIMM.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 185
mibFaultName: fltMemoryUnitInoperable
moClass: memory:Unit
Type: equipment
```

fltMemoryUnitThermalThresholdCritical

Fault Code:F0187

Message

DIMM [location] on server [chassisId]/[slotId] temperature: [thermal]DIMM [location] on server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a memory unit on a blade or rack server exceeds a critical threshold value. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 187
mibFaultName: fltMemoryUnitThermalThresholdCritical
moClass: memory:Unit
Type: environmental
```

fltMemoryUnitThermalThresholdNonCritical

Fault Code:F0186

Message

DIMM [location] on server [chassisId]/[slotId] temperature: [thermal]DIMM [location] on server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a memory unit on a blade or rack server exceeds a non-critical threshold value, but is still below the critical threshold. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 186
mibFaultName: fltMemoryUnitThermalThresholdNonCritical
moClass: memory:Unit
Type: environmental
```

fltMemoryUnitThermalThresholdNonRecoverable

Fault Code:F0188

Message

DIMM [location] on server [chassisId]/[slotId] temperature: [thermal]DIMM [location] on server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a memory unit on a blade or rack server has been out of the operating range, and the issue is not recoverable.Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 188
mibFaultName: fltMemoryUnitThermalThresholdNonRecoverable
moClass: memory:Unit
Type: environmental
```

Pin Group-Related Faults

This section contains faults raised as a result of issues related to a pin groups in the Cisco UCS instance.

fltFabricLanPinGroupEmpty

Fault Code:F0621

Message

LAN Pin Group [name] is empty

Explanation

This fault typically occurs when a LAN pin group does not contain any targets.

Recommended Action

If you see this fault, add a target to the LAN pin group.

Fault Details

```
Severity: minor
Cause: empty-pin-group
CallHome: none
mibFaultCode: 621
mibFaultName: fltFabricLanPinGroupEmpty
moClass: fabric:LanPinGroup
Type: server
```

fltFabricSanPinGroupEmpty

Fault Code:F0622

Message

SAN Pin Group [name] is empty

Explanation

This fault typically occurs when a SAN pin group does not contain any targets.

Recommended Action

If you see this fault, add a target to the SAN pin group.

Fault Details

```
Severity: minor
Cause: empty-pin-group
CallHome: none
mibFaultCode: 622
mibFaultName: fltFabricSanPinGroupEmpty
moClass: fabric:SanPinGroup
Type: server
```

fltVnicEtherPinningMisconfig

Fault Code:F0841

Message

Hard pinning target for eth vNIC [name], service profile [name] is missing or misconfigured

Explanation

This fault occurs when one or more vNIC target uplink ports or port channels for a hard-pinned LAN pin group are either missing or misconfigured as the wrong port type.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the LAN pin group configuration.

Step 2 Correct the configuration of the port and port channels in the pin group.

Step 3 Ensure that all required vLANs are allowed on the target ports or port channels.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: pinning-misconfig
CallHome: none
mibFaultCode: 841
```

```
mibFaultName: fltVnicEtherPinningMisconfig
moClass: vnic:Ether
Type: configuration
```

fltVnicEtherPinningMismatch

Fault Code:F0840

Message

Hard pinning target for eth vNIC [name], service profile [name] does not have all the required vlans configured

Explanation

This fault occurs when one or more VLANs required by vNIC in a service profile are not configured on the target uplink port or port channel for a hard-pinned LAN pin group.

Recommended Action

If you see this fault, take the following actions:

Step 1 In the LAN Uplinks Manager of the Cisco UCS Manager GUI, configure all of the VLANs in the vNIC in the target uplink port or port channel for the LAN pin group. If you prefer to use the Cisco UCS Manager CLI, navigate to scope **/eth-uplink/vlan** and create the required member ports for the LAN pin group.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: pinning-mismatch
CallHome: none
mibFaultCode: 840
mibFaultName: fltVnicEtherPinningMismatch
moClass: vnic:Ether
Type: configuration
```

Pool-Related Faults

This section contains faults raised as a result of issues related to a server pool, UUID suffix pool, or other pool in the Cisco UCS instance.

fltComputePoolEmpty

Fault Code:F0463

Message

server pool [name] is empty

Explanation

This fault typically occurs when the selected server pool does not contain any servers.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify the qualifier settings in the server pool policy qualifications. If the policy was modified after the server was discovered, reacknowledge the server.

Step 2 Manually associate the service profile with a server.

Step 3 If the server pool is not used, ignore the fault.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: empty-pool
CallHome: none
mibFaultCode: 463
mibFaultName: fltComputePoolEmpty
moClass: compute:Pool
Type: server
```

fltFcpoolInitiatorsEmpty

Fault Code:F0476

Message

FC pool [purpose] [name] is empty

Explanation

This fault typically occurs when a WWN pool does not contain any WWNs.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the pool is in use, add a block of WWNs to the pool.

Step 2 If the pool is not in use, ignore the fault.

Fault Details

```
Severity: minor
Cause: empty-pool
CallHome: none
mibFaultCode: 476
mibFaultName: fltFcpoolInitiatorsEmpty
moClass: fcpool:Initiators
Type: server
```

fltIppoolPoolEmpty

Fault Code:F0465

Message

IP pool [name] is empty

Explanation

This fault typically occurs when an IP address pool does not contain any IP addresses.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the pool is in use, add a block of IP addresses to the pool.

Step 2 If the pool is not in use, ignore the fault.

Fault Details

```
Severity: minor
Cause: empty-pool
CallHome: none
mibFaultCode: 465
mibFaultName: fltIppoolPoolEmpty
moClass: ippool:Pool
Type: server
```

fltIqnpoolPoolEmpty

Fault Code:F0821

Message

iqn pool [name] is empty

Explanation

This fault typically occurs when an IQN pool does not contain any IQNs.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the pool is in use, add a block of IQNs to the pool.

Step 2 If the pool is not in use, ignore the fault.

Fault Details

```
Severity: minor
Cause: empty-pool
CallHome: none
mibFaultCode: 821
```

mibFaultName: fltIqnpoolPoolEmpty
moClass: iqnpool:Pool
Type: server

fltMacpoolPoolEmpty

Fault Code:F0466

Message

MAC pool [name] is empty

Explanation

This fault typically occurs when a MAC address pool does not contain any MAC addresses.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the pool is in use, add a block of MAC addresses to the pool.

Step 2 If the pool is not in use, ignore the fault.

Fault Details

Severity: minor
Cause: empty-pool
CallHome: none
mibFaultCode: 466
mibFaultName: fltMacpoolPoolEmpty
moClass: macpool:Pool
Type: server

fltUuidpoolPoolEmpty

Fault Code:F0464

Message

UUID suffix pool [name] is empty

Explanation

This fault typically occurs when a UUID suffix pool does not contain any UUID suffixes.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the pool is in use, add a block of UUID suffixes to the pool.

Step 2 If the pool is not in use, ignore the fault.

Fault Details

```
Severity: minor
Cause: empty-pool
CallHome: none
mibFaultCode: 464
mibFaultName: fltUuidpoolPoolEmpty
moClass: uuidpool:Pool
Type: server
```

Port-Related Faults

This section contains faults raised as a result of issues with one or more ports in a Cisco UCS instance.

fltFabricEpMgrEpTransModeFail

Fault Code:F0832

Message

Port constraint violation on switch [id]: [confQual]

Explanation

This fault occurs when at least one logical interface is misconfigured. This can happen when upgrading to a different type or series of fabric interconnect or when importing a configuration.The configuration must meet the following constraints:

- The first Fibre Channel port must be an odd port number. This constraint cannot be violated when upgrading from a Cisco UCS 6100 series fabric interconnect to a Cisco UCS 6200 series fabric interconnect.
- All FC ports must be configured contiguously with intervening unconfigured FC ports. This can happen during an upgrade from a Cisco UCS 6100 series fabric interconnect when you import the configuration from a Cisco UCS 6100 series fabric interconnect configuration into a Cisco UCS 6200 series fabric interconnect. For example, the Cisco UCS 6100 series fabric interconnect has an FC expansion module with ports FC2/1 through FC2/6 configured. When you import that configuration into a Cisco UCS 6200 series fabric interconnect, FC ports 2/7 through 2/16 remain unconfigured. You can correct this problem by configuring the missing FC ports.
- Ethernet and FC port ranges cannot overlap. This can happen when upgrading from a Cisco UCS 6100 series fabric interconnect to a Cisco UCS 6200 series fabric interconnect. For example, some Cisco UCS 6100 expansion modules have FC and Ethernet ports with the same ID, such as FC port 2/1 and Ethernet port 2/1.
- There must be at most one logical port per fabric interconnect ID/module ID/port ID. For example, a port cannot be configured as both Ethernet and FC. This can happen during an upgrade from a Cisco UCS 6100 series fabric interconnect. For example, some Cisco UCS 6100 expansion modules have FC and Ethernet ports with the same ID, such as FC port 2/1 and Ethernet port 2/1.
- Within a module, the port IDs of Ethernet ports must be lower than the smallest FC port ID. This means that all Ethernet ports must be on the left and all FC ports on the right. This can happen during an upgrade from a Cisco UCS 6140 fabric interconnect with 40 ports on the fixed module to a Cisco UCS 6248 fabric interconnect with 32 ports on the fixed module. For example, if the Cisco UCS 6248 is initially configured with Ethernet ports 1/1 through 1/16 and FC ports 1/17 through 1/32, and you import a a configuration from the Cisco UCS 6140 with Ethernet ports 1/1 through 1/32

unconfigured and Ethernet ports 1/33 through 1/40, the resulting configuration is Ethernet 1/1 through 1/16, FC 1/17 through 1/32, and Ethernet 1/33 through 1/40. This is not a valid configuration. You must delete ports 1/33 through 1/40 to correct the configuration.

- A non-unified Ethernet port cannot be configured as an FC port. Please note the following:
  - This constraint cannot be violated when upgrading from a Cisco UCS 6100 series fabric interconnect to a Cisco UCS 6200 series fabric interconnect.
  - This constraint can be violated when downgrading from a Cisco UCS 6200 series fabric interconnect to a Cisco UCS 6100 series fabric interconnect.
  - This constraint can be violated when pre-provisioning a port on a Cisco UCS 6100 series fabric interconnect and then inserting an expansion module that does not match the requirement.
- A non-unified FC port cannot be configured as an Ethernet port. Please note the following:
  - This constraint cannot be violated when upgrading from a Cisco UCS 6100 series fabric interconnect to a Cisco UCS 6200 series fabric interconnect.
  - This constraint can be violated when downgrading from a Cisco UCS 6200 series fabric interconnect to a Cisco UCS 6100 series fabric interconnect.
  - This constraint can be violated when pre-provisioning a port on a Cisco UCS 6100 series fabric interconnect and then inserting an expansion module that does not match the requirement.
- On a Cisco UCS 6100 series fabric interconnect, server ports cannot be configured on expansion modules. This constraint can be violated when downgrading from a Cisco UCS 6200 series fabric interconnect to a Cisco UCS 6100 series fabric interconnect.

Recommended Action

If you see this fault, take the following action:

Step 1 Create a list of all logical interfaces that are misconfigured and have caused an 'error-misconfigured' fault.

Step 2 For each logical interface, note the reason listed in the fault for the misconfiguration.

Step 3 Log into Cisco UCS Manager and correct each misconfigured logical interface. If you used the Cisco UCS Manager CLI, commit all changes.

Step 4 Review any faults or error messages that describe additional misconfigurations and correct those errors.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: config-error
CallHome: none
mibFaultCode: 832
mibFaultName: fltFabricEpMgrEpTransModeFail
moClass: fabric:EpMgr
Type: network
```

fltFabricPIoEpErrorMisconfigured

Fault Code:F0834

Message

Interface [name] is [operState]. Reason: [operStateReason]

Explanation

This fault occurs when a logical interface is misconfigured. This can happen when upgrading to a different type or series of fabric interconnect or when importing a configuration.

Recommended Action

If you see this fault, take the following action:

Step 1 Create a list of all logical interfaces that are misconfigured and have caused an 'error-misconfigured' fault.

Step 2 For each logical interface, note the reason listed in the fault for the misconfiguration.

Step 3 Log into Cisco UCS Manager and correct each misconfigured logical interface. If you used the Cisco UCS Manager CLI, commit all changes.

Step 4 Review any faults or error messages that describe additional misconfigurations and correct those errors.

Step 5 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: interface-misconfigured
CallHome: none
mibFaultCode: 834
mibFaultName: fltFabricPIoEpErrorMisconfigured
moClass: fabric:PIoEp
Type: network
```

fltPortPIoFailed

Fault Code:F0277

Message

[transport] port [portId] on chassis [id] oper state: [operState], reason: [stateQual][transport] port [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual]

Explanation

This fault is raised on fabric interconnect ports and on server-facing ports on an IOM or a FEX module when the system detects an indeterminate fault.

Recommended Action

If you see this fault, create a **show tech-support** file for Cisco UCS Manager and the chassis or FEX module, and then contact Cisco TAC.

Fault Details

```
Severity: major
Cause: port-failed
CallHome: diagnostic
mibFaultCode: 277
mibFaultName: fltPortPIoFailed
moClass: port:PIo
Type: network
```

fltPortPIoHardware-failure

Fault Code:F0278

Message

[transport] port [portId] on chassis [id] oper state: [operState], reason: hardware-failure[transport] port [portId] on fabric interconnect [id] oper state: [operState], reason: hardware-failure

Explanation

This fault is raised on fabric interconnect ports and server-facing ports on an IOM or a FEX module when the system detects a hardware failure.

Recommended Action

If you see this fault, create a **show tech-support** file for Cisco UCS Manager and the chassis or FEX module, and then contact Cisco TAC.

Fault Details

```
Severity: major
Cause: port-failed
CallHome: diagnostic
mibFaultCode: 278
mibFaultName: fltPortPIoHardwareFailure
moClass: port:PIo
Type: network
```

fltPortPIoInvalid-sfp

Fault Code:F0713

Message

[transport] port [portId] on chassis [id] role : [ifRole] transceiver type:[xcvrType][transport] port [portId] on fabric interconnect [id] role : [ifRole] transceiver type:[xcvrType]

Explanation

This fault is raised against a fabric interconnect port, network-facing IOM port, or FEX module port if an unsupported transceiver type is inserted. The port cannot be used if it has an unsupported transceiver.

Recommended Action

If you see this fault, replace the transceiver with a supported SFP type. Refer to the documentation on the Cisco website for a list of supported SFPs.

Fault Details

```
Severity: major
Cause: unsupported-transceiver
CallHome: none
mibFaultCode: 713
mibFaultName: fltPortPIoInvalidSfp
moClass: port:PIo
Type: network
```

fltPortPIoLink-down

Fault Code:F0276

Message

[transport] port [portId] on chassis [id] oper state: [operState], reason: [stateQual][transport] port [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual]

Explanation

This fault occurs when a fabric interconnect port is in link-down state. This state impacts the traffic destined for the port.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the physical link is properly connected between the fabric interconnect and the peer component.

Step 2 Verify that the configuration on the peer entity is properly configured and matches the fabric interconnect port configuration.

Step 3 Unconfigure and re-configure the port.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: link-down
CallHome: diagnostic
mibFaultCode: 276
mibFaultName: fltPortPIoLinkDown
moClass: port:PIo
Type: network
```

fltPortPIoSfp-not-present

Fault Code:F0279

Message

[transport] port [portId] on chassis [id] oper state: [operState][transport] port [portId] on fabric interconnect [id] oper state: [operState]

Explanation

When a fabric interconnect port is not in an unconfigured state, an SFP is required for its operation. This fault is raised to indicate that the SFP is missing from a configured port.

Recommended Action

If you see this fault, insert a supported SFP into the port on the fabric interconnect. A list of supported SFPs can be found on www.Cisco.com.

Fault Details

```
Severity: info
Cause: port-failed
CallHome: none
mibFaultCode: 279
mibFaultName: fltPortPIoSfpNotPresent
moClass: port:PIo
Type: network
```

Port Channel-Related Faults

This section contains faults raised as a result of issues with one or more port channels in a Cisco UCS instance.

fltFabricDceSwSrvPcEpDown

Fault Code:F0831

Message

[type] Member [slotId]/[portId] of Port-Channel [portId] on fabric interconnect [id] is down, membership: [membership]

Explanation

This fault typically occurs when a member port in a fabric port channel is down.

Recommended Action

If you see this fault, take the following action:

Step 1 Check the link connectivity between the FEX or IOM and the fabric interconnect.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: membership-down
CallHome: none
mibFaultCode: 831
mibFaultName: fltFabricDceSwSrvPcEpDown
moClass: fabric:DceSwSrvPcEp
Type: network
```

fltFabricFcSanPcEpIncompatibleSpeed

Fault Code:F0734

Message

Member [slotId]/[portId] cannot be added to SAN Port-Channel [portId] on fabric interconnect [id], reason: [membership]

Explanation

This fault typically occurs when the maximum supported Fibre Channel speed of a port in a Fibre Channel port channel is incompatible with the admin speed configured for the port channel.

Recommended Action

If you see this fault, take one of the following actions:

- Change the admin speed of the port channel to match the maximum supported speed of the member ports in the port channel.
- Replace the expansion module in the fabric interconnect with one that matches the admin speed configured for the port channel.

Fault Details

```
Severity: major
Cause: incompatible-speed
CallHome: none
mibFaultCode: 734
mibFaultName: fltFabricFcSanPcEpIncompatibleSpeed
moClass: fabric:FcSanPcEp
Type: network
```

fltFabricFcSanPcIncompatibleSpeed

Fault Code:F0735

Message

Cannot set admin speed to the requested value, Speed incompatible with member ports in the port-channel

Explanation

This fault typically occurs when the maximum supported Fibre Channel speed of a port in a Fibre Channel port channel is incompatible with the admin speed configured for the port channel.

Recommended Action

If you see this fault, take one of the following actions:

- Change the admin speed of the port channel to match the maximum supported speed of the member ports in the port channel.
- Replace the expansion module in the fabric interconnect with one that matches the admin speed configured for the port channel.

Fault Details

```
Severity: major
Cause: incompatible-speed
CallHome: none
mibFaultCode: 735
mibFaultName: fltFabricFcSanPcIncompatibleSpeed
moClass: fabric:FcSanPc
Type: network
```

fltFabricExternalPcDown

Fault Code:F0282

Message

[type] port-channel [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual][type] port-channel [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual]

Explanation

This fault typically occurs when a fabric interconnect reports that a fabric port channel is operationally down.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the member ports in the fabric port channel are administratively up and operational. Check the link connectivity for each port.

Step 2 If connectivity seems correct, check the operational states on the peer switch ports of the port channel members.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: operational-state-down
CallHome: none
mibFaultCode: 282
mibFaultName: fltFabricExternalPcDown
```

moClass: fabric:ExternalPc
Type: network

fltFabricFcSanPcEpDown

Fault Code:F0728

Message

[type] Member [slotId]/[portId] of Port-Channel [portId] on fabric interconnect [id] is down, membership: [membership]

Explanation

This fault typically occurs when a member port in a Fibre Channel port channel is down.

Recommended Action

If you see this fault, take the following action:

Step 1 Check the link connectivity on the upstream Fibre Channel switch

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: major
Cause: membership-down
CallHome: none
mibFaultCode: 728
mibFaultName: fltFabricFcSanPcEpDown
moClass: fabric:FcSanPcEp
Type: network

Power-Related Faults

This section contains faults raised as a result of issues related to the power configuration in the Cisco UCS instance.

fltPowerBudgetChassisPsuInsufficient

Fault Code:F0764

Message

Chassis [id] has had PSU failures. Please correct the problem by checking input power or replace the PSU

Explanation

This fault typically occurs when at least two PSUs are not powered on.

Recommended Action

If you see this fault, insert at least two PSUs and power them on.

Fault Details

```
Severity: major
Cause: psu-failure
CallHome: none
mibFaultCode: 764
mibFaultName: fltPowerBudgetChassisPsuInsufficient
moClass: power:Budget
Type: environmental
```

fltPowerBudgetFirmwareMismatch

Fault Code:F0798

Message

Firmware on blade [chassisId]/[slotId] does not allow chassis level power capping. Please consider upgrading to at least 1.4 version

Explanation

This fault typically occurs when the CIMC or BIOS firmware on a server is an earlier release than Cisco UCS, Release 1.4.

Recommended Action

If you see this fault, consider upgrading the CIMC firmware, and the entire Cisco UCS instance if necessary, to Cisco UCS, Release 1.4 or later.

Fault Details

```
Severity: major
Cause: old-firmware
CallHome: none
mibFaultCode: 798
mibFaultName: fltPowerBudgetFirmwareMismatch
moClass: power:Budget
Type: environmental
```

fltPowerBudgetPowerBudgetBmcProblem

Fault Code:F0637

Message

Power cap application failed for server [chassisId]/[slotId]Power cap application failed for server [id]

Explanation

This fault typically occurs when the server CIMC or BIOS has failed to enforce the configured power cap.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the power consumption of the blade server. If the server is consuming significantly more power than configured in the power cap, switch to a manual per blade cap configuration. If the power consumption is still too high, consider reducing the group cap so that the power consumption of other chassis consumption can be reduced to make up for the increase.

Step 2 If the power consumption is still too high, the CIMC or BIOS software is likely faulty.

Step 3 Create a **show tech-support** file for Cisco UCS Manager and the chassis and then contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-cap-fail
CallHome: none
mibFaultCode: 637
mibFaultName: fltPowerBudgetPowerBudgetBmcProblem
moClass: power:Budget
Type: environmental
```

fltPowerBudgetPowerBudgetCmcProblem

Fault Code:F0635

Message

Power cap application failed for chassis [id]

Explanation

This fault typically occurs when the server CIMC has failed to enforce the configured power cap.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the power consumption of the chassis. If the chassis is consuming significantly more power than configured in the power cap, consider reducing the group cap so that the power consumption of other chassis consumption can be reduced to make up for the increase.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file for Cisco UCS Manager and the chassis and then contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-cap-fail
CallHome: none
mibFaultCode: 635
mibFaultName: fltPowerBudgetPowerBudgetCmcProblem
moClass: power:Budget
Type: environmental
```

fltPowerBudgetPowerBudgetDiscFail

Fault Code:F0640

Message

Insufficient power available to discover server [chassisId]/[slotId]Insufficient power available to discover server [id]

Explanation

This fault typically occurs when discovery fails due to unavailable power in the group.

Recommended Action

If you see this fault, take the following actions:

Step 1 Consider increasing the group cap.

Step 2 Reduce the number of blade servers or chassis in the Cisco UCS instance.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-cap-fail
CallHome: none
mibFaultCode: 640
```

fltPowerBudgetPowerCapReachedCommit

Fault Code:F0744

Message

P-State lowered as consumption hit power cap for server [chassisId]/[slotId]P-State lowered as consumption hit power cap for server [id]

Explanation

This fault typically occurs when Cisco UCS Manager is actively capping the power for a blade server.

Recommended Action

If you see this fault, no action is needed.

Fault Details

```
Severity: info
Cause: power-consumption-hit-limit
CallHome: none
mibFaultCode: 744
mibFaultName: fltPowerBudgetPowerCapReachedCommit
moClass: power:Budget
Type: environmental
mibFaultName: fltPowerBudgetPowerBudgetDiscFail
```

moClass: power:Budget
Type: environmental

fltPowerBudgetTStateTransition

Fault Code:F0765

Message

Blade [chassisId]/[slotId] has been severely throttled. CIMC can recover if budget is redeployed to the blade or by rebooting the blade. If problem persists, please ensure that OS is ACPI compliantRack server [id] has been severely throttled. CIMC can recover if budget is redeployed to the blade or by rebooting the blade. If problem persists, please ensure that OS is ACPI compliant

Explanation

This fault typically occurs when the processor T-state is used to severely throttle the CPU.

Recommended Action

If you see this fault, take the following actions:

Step 1 Redeploy the power budget for the affected power group, blade server, or chassis.

Step 2 If the problem persists, reboot the blade server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: critical
Cause: no-ack-from-bios
CallHome: none
mibFaultCode: 765
mibFaultName: fltPowerBudgetTStateTransition
moClass: power:Budget
Type: environmental

fltPowerChassisMemberChassisFirmwareProblem

Fault Code:F0741

Message

Chassis [id] cannot be capped as at least one of the CMC or CIMC or BIOS firmware version is less than 1.4. Please upgrade the firmware for cap to be applied.

Explanation

This fault typically occurs when the CIMC firmware on a server is an earlier release than Cisco UCS, Release 1.4.

Recommended Action

If you see this fault, consider upgrading the CIMC firmware, and the entire Cisco UCS instance if necessary, to Cisco UCS, Release 1.4 or later.

Fault Details

```
Severity: major
Cause: old-chassis-component-firmware
CallHome: none
mibFaultCode: 741
mibFaultName: fltPowerChassisMemberChassisFirmwareProblem
moClass: power:ChassisMember
Type: environmental
```

fltPowerChassisMemberChassisPsuInsufficient

Fault Code:F0742

Message

Chassis [id] cannot be capped as at least two PSU need to be powered

Explanation

This fault typically occurs when at least two PSUs are not powered on.

Recommended Action

If you see this fault, insert at least two PSUs and power them on.

Fault Details

```
Severity: major
Cause: psu-insufficient
CallHome: none
mibFaultCode: 742
mibFaultName: fltPowerChassisMemberChassisPsuInsufficient
moClass: power:ChassisMember
Type: environmental
```

fltPowerChassisMemberChassisPsuRedundanceFailure

Fault Code:F0743

Message

Chassis [id] was configured for redundancy, but running in a non-redundant configuration.

Explanation

This fault typically occurs when chassis power redundancy has failed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Consider adding more PSUs to the chassis.

Step 2 Replace any non-functional PSUs.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: psu-redundancy-fail
CallHome: none
mibFaultCode: 743
mibFaultName: fltPowerChassisMemberChassisPsuRedundanceFailure
moClass: power:ChassisMember
Type: environmental
```

fltPowerChassisMemberPowerGroupCapInsufficient

Fault Code:F0740

Message

Chassis [id] cannot be capped as group cap is low. Please consider raising the cap.

Explanation

This fault typically occurs when an updated group cap is insufficient to meet the minimum hardware requirements and a chassis that has just been added to the power group cannot be capped as a result.

Recommended Action

If you see this fault, take the following actions:

Step 1 Consider increasing the group cap.

Step 2 Reduce the number of blade servers or chassis in the Cisco UCS instance.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: group-cap-insufficient
CallHome: none
mibFaultCode: 740
mibFaultName: fltPowerChassisMemberPowerGroupCapInsufficient
moClass: power:ChassisMember
Type: environmental
```

fltPowerGroupPowerGroupBudgetIncorrect

Fault Code:F0643

Message

admin committed insufficient for power group [name], using previous value [operCommitted]

Explanation

This fault typically occurs when the group cap is insufficient to meet the minimum hardware requirements. Under these circumstances, Cisco UCS Manager uses the previously entered group cap for provisioning.

Recommended Action

If you see this fault, take the following actions:

Step 1 Consider increasing the group cap.

Step 2 Reduce the number of blade servers or chassis in the Cisco UCS instance.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-cap-fail
CallHome: none
mibFaultCode: 643
mibFaultName: fltPowerGroupPowerGroupBudgetIncorrect
moClass: power:Group
Type: environmental
```

fltPowerGroupPowerGroupInsufficientBudget

Fault Code:F0642

Message

insufficient budget for power group [name]

Explanation

This fault typically occurs when the group cap is insufficient to meet the minimum hardware requirements.

Recommended Action

If you see this fault, take the following actions:

Step 1 Consider increasing the group cap.

Step 2 Reduce the number of blade servers or chassis in the Cisco UCS instance.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-cap-fail
CallHome: none
mibFaultCode: 642
mibFaultName: fltPowerGroupPowerGroupInsufficientBudget
moClass: power:Group
```

Type: environmental

fltPowerPolicyPowerPolicyApplicationFail

Fault Code:F0766

Message

Insufficient budget to apply no-cap priority through policy [name]. Blades will continue to be capped

Explanation

This fault occurs when a power policy cannot be applied to one or more blade servers. The affected blade servers cannot operate normally without power capping due to the limited power budget for those servers.

Recommended Action

If you see this fault, take the following actions:

Step 1 Increase the power budget for the blade servers in the power policy.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: minor
Cause: no-cap-fail
CallHome: none
mibFaultCode: 766
mibFaultName: fltPowerPolicyPowerPolicyApplicationFail
moClass: power:Policy
Type: environmental

Power Supply-Related Faults

This section contains faults raised as a result of issues related to a power supply unit in the Cisco UCS instance.

fltEquipmentPsuIdentity

Fault Code:F0407

Message

Power supply [id] on chassis [id] has a malformed FRUPower supply [id] on server [id] has a malformed FRU

Explanation

This fault typically occurs when the FRU information for a power supply unit is corrupted or malformed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: fru-problem
CallHome: diagnostic
mibFaultCode: 407
mibFaultName: fltEquipmentPsuIdentity
moClass: equipment:Psu
Type: equipment
```

fltEquipmentPsuInoperable

Fault Code:F0374

Message

Power supply [id] in chassis [id] operability: [operability]Power supply [id] in fabric interconnect [id] operability: [operability]Power supply [id] in fex [id] operability: [operability]Power supply [id] in server [id] operability: [operability]

Explanation

This fault typically occurs when Cisco UCS Manager detects a problem with a power supply unit in a chassis, fabric interconnect or a FEX. For example, the PSU is not functional.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the power cord is properly connected to the PSU and the power source.

Step 2 Verify that the power source is 220 volts.

Step 3 Verify that the PSU is properly installed in the chassis or fabric interconnect.

Step 4 Remove the PSU and reinstall it.

Step 5 Replace the PSU.

Step 6 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: environmental
mibFaultCode: 374
mibFaultName: fltEquipmentPsuInoperable
moClass: equipment:Psu
Type: equipment
```

fltEquipmentPsuInputError

Fault Code:F0883

Message

Power supply [id] on chassis [id] has disconnected cable or bad input voltagePower supply [id] on server [id] has disconnected cable or bad input voltage

Explanation

This fault occurs when a power cable is disconnected or input voltage is incorrect.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: power-problem
CallHome: none
mibFaultCode: 883
mibFaultName: fltEquipmentPsuInputError
moClass: equipment:Psu
Type: equipment
```

fltEquipmentPsuMissing

Fault Code:F0378

Message

Power supply [id] in chassis [id] presence: [presence]Power supply [id] in fabric interconnect [id] presence: [presence]Power supply [id] in fex [id] presence: [presence]Power supply [id] in server [id] presence: [presence]

Explanation

This fault typically occurs when Cisco UCS Manager detects a problem with a power supply unit in a chassis, fabric interconnect, or a FEX. For example, the PSU is missing.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the PSU is physically present in the slot, remove and then reinsert it.

Step 2 If the PSU is not physically present in the slot, insert a new PSU.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-missing
```

CallHome: none
mibFaultCode: 378
mibFaultName: fltEquipmentPsuMissing
moClass: equipment:Psu
Type: equipment

fltEquipmentPsuOffline

Fault Code:F0528

Message

Power supply [id] in chassis [id] power: [power]Power supply [id] in fabric interconnect [id] power: [power]Power supply [id] in fex [id] power: [power]Power supply [id] in server [id] power: [power]

Explanation

This fault typically occurs when Cisco UCS Manager detects that a power supply unit in a chassis, fabric interconnect, or FEX is offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the power cord is properly connected to the PSU and the power source.

Step 2 Verify that the power source is 220 volts.

Step 3 Verify that the PSU is properly installed in the chassis or fabric interconnect.

Step 4 Remove the PSU and reinstall it.

Step 5 Replace the PSU.

Step 6 If the above actions did not resolve the issue, note down the type of PSU, execute the **show tech-support** command, and contact Cisco Technical Support.

Fault Details

Severity: warning
Cause: equipment-offline
CallHome: environmental
mibFaultCode: 528
mibFaultName: fltEquipmentPsuOffline
moClass: equipment:Psu
Type: environmental

fltEquipmentPsuPerfThresholdCritical

Fault Code:F0393

Message

Power supply [id] in chassis [id] output power: [perf]Power supply [id] in fabric interconnect [id] output power: [perf]Power supply [id] in server [id] output power: [perf]

Explanation

This fault occurs if the current output of the PSU in a chassis, fabric interconnect, or rack server is far below or above the desired output value.

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor the PSU status.

Step 2 Plan to replace the PSU as soon as possible.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file for the chassis and Cisco UCS Manager, and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: performance-problem
CallHome: diagnostic
mibFaultCode: 393
mibFaultName: fltEquipmentPsuPerfThresholdCritical
moClass: equipment:Psu
Type: equipment
```

fltEquipmentPsuPerfThresholdNonCritical

Fault Code:F0392

Message

Power supply [id] in chassis [id] output power: [perf]Power supply [id] in fabric interconnect [id] output power: [perf]Power supply [id] in server [id] output power: [perf]

Explanation

This fault is raised as a warning if the current output of the PSU in a chassis, fabric interconnect, or rack server does not match the desired output value.

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor the PSU status.

Step 2 If possible, remove and reseat the PSU.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file for the chassis and Cisco UCS Manager, and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: performance-problem
CallHome: diagnostic
mibFaultCode: 392
```

mibFaultName: fltEquipmentPsuPerfThresholdNonCritical
moClass: equipment:Psu
Type: equipment

fltEquipmentPsuPerfThresholdNonRecoverable

Fault Code:F0394

Message

Power supply [id] in chassis [id] output power: [perf]Power supply [id] in fabric interconnect [id] output power: [perf]Power supply [id] in server [id] output power: [perf]

Explanation

This fault occurs if the current output of the PSU in a chassis, fabric interconnect, or rack server is far above or below the non-recoverable threshold value.

Recommended Action

If you see this fault, plan to replace the PSU as soon as possible.

Fault Details

Severity: critical
Cause: performance-problem
CallHome: diagnostic
mibFaultCode: 394
mibFaultName: fltEquipmentPsuPerfThresholdNonRecoverable
moClass: equipment:Psu
Type: equipment

fltEquipmentPsuPowerSupplyProblem

Fault Code:F0369

Message

Power supply [id] in chassis [id] power: [power]Power supply [id] in fabric interconnect [id] power: [power]Power supply [id] in fex [id] power: [power]Power supply [id] in server [id] power: [power]

Explanation

This fault typically occurs when Cisco UCS Manager detects a problem with a power supply unit in a chassis, fabric interconnect or a FEX. For example, the PSU is not functional.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the power cord is properly connected to the PSU and the power source.

Step 2 Verify that the power source is 220 volts.

Step 3 Verify that the PSU is properly installed in the chassis or fabric interconnect.

Step 4 Remove the PSU and reinstall it.

Step 5 Replace the PSU.

Step 6 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-problem
CallHome: environmental
mibFaultCode: 369
mibFaultName: fltEquipmentPsuPowerSupplyProblem
moClass: equipment:Psu
Type: environmental
```

fltEquipmentPsuPowerSupplyShutdown

Fault Code:F0881

Message

Power supply [id] in chassis [id] shutdown reason:[powerStateQualifier]

Explanation

This fault typically occurs when a power supply unit in a chassis, fabric interconnect, or a FEX is shut down, either due to higher than expected power current, higher than expected temperatures, or the failure of a fan.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Verify that the power cord is properly connected to the PSU and the power source.

Step 7 Verify that the power source is 220 volts.

Step 8 Verify that the PSU is properly installed in the chassis or fabric interconnect.

Step 9 Remove the PSU and reinstall it.

Step 10 Replace the PSU.

Step 11 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-offline
CallHome: environmental
```

mibFaultCode: 881
mibFaultName: fltEquipmentPsuPowerSupplyShutdown
moClass: equipment:Psu
Type: environmental

fltEquipmentPsuPowerThreshold

Fault Code:F0882

Message

Power supply [id] on chassis [id] has exceeded its power thresholdPower supply [id] on server [id] has exceeded its power threshold

Explanation

This fault occurs when a power supply unit is drawing too much current.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: critical
Cause: power-problem
CallHome: none
mibFaultCode: 882
mibFaultName: fltEquipmentPsuPowerThreshold
moClass: equipment:Psu
Type: equipment

fltEquipmentPsuThermalThresholdCritical

Fault Code:F0383

Message

Power supply [id] in chassis [id] temperature: [thermal]Power supply [id] in fabric interconnect [id] temperature: [thermal]Power supply [id] in server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a PSU module has exceeded a critical threshold value. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the PSU module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the PSU modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace faulty PSU modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 383
mibFaultName: fltEquipmentPsuThermalThresholdCritical
moClass: equipment:Psu
Type: environmental
```

fltEquipmentPsuThermalThresholdNonCritical

Fault Code:F0381

Message

Power supply [id] in chassis [id] temperature: [thermal]Power supply [id] in fabric interconnect [id] temperature: [thermal]Power supply [id] in server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a PSU module has exceeded a non-critical threshold value, but is still below the critical threshold. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the PSU module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the PSU modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace faulty PSU modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 381
mibFaultName: fltEquipmentPsuThermalThresholdNonCritical
moClass: equipment:Psu
Type: environmental
```

fltEquipmentPsuThermalThresholdNonRecoverable

Fault Code:F0385

Message

Power supply [id] in chassis [id] temperature: [thermal]Power supply [id] in fabric interconnect [id] temperature: [thermal]Power supply [id] in server [id] temperature: [thermal]

Explanation

This fault occurs when the temperature of a PSU module has been out of operating range, and the issue is not recoverable. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the PSU module.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the PSU modules have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Replace faulty PSU modules.

Step 8 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 9 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 385
mibFaultName: fltEquipmentPsuThermalThresholdNonRecoverable
moClass: equipment:Psu
Type: environmental
```

fltEquipmentPsuVoltageThresholdCritical

Fault Code:F0389

Message

Power supply [id] in chassis [id] voltage: [voltage]Power supply [id] in fabric interconnect [id] voltage: [voltage]Power supply [id] in fex [id] voltage: [voltage]Power supply [id] in server [id] voltage: [voltage]

Explanation

This fault occurs when the PSU voltage has exceeded the specified hardware voltage rating.

Recommended Action

If you see this fault, take the following actions:

Step 1 Remove and reseat the PSU.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 389
mibFaultName: fltEquipmentPsuVoltageThresholdCritical
moClass: equipment:Psu
```

Type: environmental

fltEquipmentPsuVoltageThresholdNonCritical

Fault Code:F0387

Message

Power supply [id] in chassis [id] voltage: [voltage]Power supply [id] in fabric interconnect [id] voltage: [voltage]Power supply [id] in fex [id] voltage: [voltage]Power supply [id] in server [id] voltage: [voltage]

Explanation

This fault occurs when the PSU voltage is out of normal operating range, but hasn't reached to a critical stage yet. Normally the PSU will recover itself from this situation.

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor the PSU for further degradation.

Step 2 Remove and reseat the PSU.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: minor
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 387
mibFaultName: fltEquipmentPsuVoltageThresholdNonCritical
moClass: equipment:Psu
Type: environmental

fltEquipmentPsuVoltageThresholdNonRecoverable

Fault Code:F0391

Message

Power supply [id] in chassis [id] voltage: [voltage]Power supply [id] in fabric interconnect [id] voltage: [voltage]Power supply [id] in fex [id] voltage: [voltage]Power supply [id] in server [id] voltage: [voltage]

Explanation

This fault occurs when the PSU voltage has exceeded the specified hardware voltage rating and PSU hardware may have been damaged as a result or may be at risk of being damaged.

Recommended Action

If you see this fault, take the following actions:

Step 1 Remove and reseat the PSU.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 391
mibFaultName: fltEquipmentPsuVoltageThresholdNonRecoverable
moClass: equipment:Psu
Type: environmental
```

Processor-Related Faults

This section contains faults raised as a result of issues with a server processor.

fltProcessorUnitDisabled

Fault Code:F0842

Message

Processor [id] on server [chassisId]/[slotId] operState: [operState]Processor [id] on server [id] operState: [operState]

Explanation

This fault occurs in the unlikely event that a processor is disabled.

Recommended Action

If you see this fault, take the following actions:

Step 1 If this fault occurs on a blade server, remove and reinsert the server into the chassis.

Step 2 In Cisco UCS Manager, decommission and recommission the blade server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: equipment-disabled
CallHome: none
mibFaultCode: 842
mibFaultName: fltProcessorUnitDisabled
moClass: processor:Unit
Type: environmental
```

fltProcessorUnitIdentity-unestablishable

Fault Code:F0801

Message

Processor [id] on server [chassisId]/[slotId] has an invalid FRUProcessor [id] on server [id] has an invalid FRU

Explanation

This fault typically occurs because Cisco UCS Manager has detected an unsupported CPU in the server. For example, the model, vendor, or revision is not recognized.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the capability catalog in Cisco UCS Manager is up to date. If necessary, update the catalog.

Step 2 If the above action did not resolve the issue, you may have an unsupported CPU configuration in the server. Create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: identity-unestablishable
CallHome: none
mibFaultCode: 801
mibFaultName: fltProcessorUnitIdentityUnestablishable
moClass: processor:Unit
Type: equipment
```

fltProcessorUnitInoperable

Fault Code:F0174

Message

Processor [id] on server [chassisId]/[slotId] operability: [operability]

Explanation

This fault occurs in the unlikely event that processor is inoperable.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the fault occurs on a blade server processor, remove the server from the chassis and then reinsert it.

Step 2 In Cisco UCS Manager, decommission and then recommission the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 174
mibFaultName: fltProcessorUnitInoperable
moClass: processor:Unit
Type: equipment
```

fltProcessorUnitThermalNonCritical

Fault Code:F0175

Message

Processor [id] on server [chassisId]/[slotId] temperature: [thermal]Processor [id] on server [id] temperature: [thermal]

Explanation

This fault occurs when the processor temperature on a blade or rack server exceeds a non-critical threshold value, but is still below the critical threshold. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 175
mibFaultName: fltProcessorUnitThermalNonCritical
moClass: processor:Unit
Type: environmental
```

fltProcessorUnitThermalThresholdCritical

Fault Code:F0176

Message

Processor [id] on server [chassisId]/[slotId] temperature: [thermal]Processor [id] on server [id] temperature: [thermal]

Explanation

This fault occurs when the processor temperature on a blade or rack server exceeds a critical threshold value. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
```

```
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 176
mibFaultName: fltProcessorUnitThermalThresholdCritical
moClass: processor:Unit
Type: environmental
```

fltProcessorUnitThermalThresholdNonRecoverable

Fault Code:F0177

Message

Processor [id] on server [chassisId]/[slotId] temperature: [thermal]Processor [id] on server [id] temperature: [thermal]

Explanation

This fault occurs when the processor temperature on a blade or rack server has been out of the operating range, and the issue is not recoverable. Be aware of the following possible contributing factors:

- Temperature extremes can cause Cisco UCS equipment to operate at reduced efficiency and cause a variety of problems, including early degradation, failure of chips, and failure of equipment. In addition, extreme temperature fluctuations can cause CPUs to become loose in their sockets.
- Cisco UCS equipment should operate in an environment that provides an inlet air temperature not colder than 50F (10C) nor hotter than 95F (35C).
- If sensors on a CPU reach 179.6F (82C), the system will take that CPU offline.

Recommended Action

If you see this fault, take the following actions:

Step 1 Review the product specifications to determine the temperature operating range of the server.

Step 2 Review the Cisco UCS Site Preparation Guide to ensure the servers have adequate airflow, including front and back clearance.

Step 3 Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed.

Step 4 Verify that the site cooling system is operating properly.

Step 5 Power off unused blade servers and rack servers.

Step 6 Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat.

Step 7 Use the Cisco UCS power capping capability to limit power usage. Power capping can limit the power consumption of the system, including blade and rack servers, to a threshold that is less than or equal to the system's maximum rated power. Power-capping can have an impact on heat dissipation and help to lower the installation site temperature.

Step 8 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
```

```
mibFaultCode: 177
mibFaultName: fltProcessorUnitThermalThresholdNonRecoverable
moClass: processor:Unit
Type: environmental
```

fltProcessorUnitVoltageThresholdCritical

Fault Code:F0179

Message

Processor [id] on server [chassisId]/[slotId] voltage: [voltage]

Explanation

This fault occurs when the processor voltage has exceeded the specified hardware voltage rating.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the fault occurs on a blade server processor, remove the server from the chassis and then reinsert it.

Step 2 In Cisco UCS Manager, decommission and then recommission the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 179
mibFaultName: fltProcessorUnitVoltageThresholdCritical
moClass: processor:Unit
Type: environmental
```

fltProcessorUnitVoltageThresholdNonCritical

Fault Code:F0178

Message

Processor [id] on server [chassisId]/[slotId] voltage: [voltage]

Explanation

This fault occurs when the processor voltage is out of normal operating range, but hasn't yet reached a critical stage. Normally the processor recovers itself from this situation

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor the processor for further degradation.

Step 2 If the fault occurs on a blade server processor, remove the server from the chassis and then reinsert it.

Step 3 In Cisco UCS Manager, decommission and then recommission the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 178
mibFaultName: fltProcessorUnitVoltageThresholdNonCritical
moClass: processor:Unit
Type: environmental
```

fltProcessorUnitVoltageThresholdNonRecoverable

Fault Code:F0180

Message

Processor [id] on server [chassisId]/[slotId] voltage: [voltage]

Explanation

This fault occurs when the processor voltage has exceeded the specified hardware voltage rating and may cause processor hardware damage or jeopardy.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the fault occurs on a blade server processor, remove the server from the chassis and then reinsert it.

Step 2 In Cisco UCS Manager, decommission and then recommission the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: voltage-problem
CallHome: environmental
mibFaultCode: 180
mibFaultName: fltProcessorUnitVoltageThresholdNonRecoverable
moClass: processor:Unit
Type: environmental
```

Server-Related Faults

This section contains faults raised as a result of issues related to a server.

fltComputeBoardCmosVoltageThresholdCritical

Fault Code:F0424

Message

Possible loss of CMOS settings: CMOS battery voltage on server [chassisId]/[slotId] is [cmosVoltage]Possible loss of CMOS settings: CMOS battery voltage on server [id] is [cmosVoltage]

Explanation

This fault is raised when the CMOS battery voltage has dropped to lower than the normal operating range. This could impact the clock and other CMOS settings.

Recommended Action

If you see this fault, replace the battery.

Fault Details

```
Severity: minor
Cause: voltage-problem
CallHome: none
mibFaultCode: 424
mibFaultName: fltComputeBoardCmosVoltageThresholdCritical
moClass: compute:Board
Type: environmental
```

fltComputeBoardCmosVoltageThresholdNonRecoverable

Fault Code:F0425

Message

Possible loss of CMOS settings: CMOS battery voltage on server [chassisId]/[slotId] is [cmosVoltage]Possible loss of CMOS settings: CMOS battery voltage on server [id] is [cmosVoltage]

Explanation

This fault is raised when the CMOS battery voltage has dropped quite low and is unlikely to recover. This impacts the clock and other CMOS settings.

Recommended Action

If you see this fault, replace the battery.

Fault Details

```
Severity: major
Cause: voltage-problem
CallHome: none
```

```
mibFaultCode: 425
mibFaultName: fltComputeBoardCmosVoltageThresholdNonRecoverable
moClass: compute:Board
Type: environmental
```

fltComputeBoardPowerError

Fault Code:F0310

Message

Motherboard of server [chassisId]/[slotId] (service profile: [assignedToDn]) power: [operPower]Motherboard of server [id] (service profile: [assignedToDn]) power: [operPower]

Explanation

This fault typically occurs when the server power sensors have detected a problem.

Recommended Action

If you see this fault, take the following actions:

Step 1 Make sure that the server is correctly installed in the chassis and that all cables are secure.

Step 2 If you reinstalled the server, reacknowledge it.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-problem
CallHome: none
mibFaultCode: 310
mibFaultName: fltComputeBoardPowerError
moClass: compute:Board
Type: environmental
```

fltComputeBoardPowerFail

Fault Code:F0868

Message

Motherboard of server [chassisId]/[slotId] (service profile: [assignedToDn]) power: [power]Motherboard of server [id] (service profile: [assignedToDn]) power: [power]

Explanation

This fault typically occurs when the power sensors on a blade server detect a problem.

Recommended Action

If you see this fault, take the following actions:

Step 1 Remove the blade server from the chassis.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: power-problem
CallHome: diagnostic
mibFaultCode: 868
mibFaultName: fltComputeBoardPowerFail
moClass: compute:Board
Type: environmental
```

fltComputeBoardThermalProblem

Fault Code:F0869

Message

Motherboard of server [chassisId]/[slotId] (service profile: [assignedToDn]) thermal: [thermal]Motherboard of server [id] (service profile: [assignedToDn]) thermal: [thermal]

Explanation

This fault typically occurs when the motherboard thermal sensors on a server detect a problem.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the server fans are working properly.

Step 2 Wait for 24 hours to see if the problem resolves itself.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 869
mibFaultName: fltComputeBoardThermalProblem
moClass: compute:Board
Type: environmental
```

fltComputeIOHubThermalNonCritical

Fault Code:F0538

Message

IO Hub on server [chassisId]/[slotId] temperature: [thermal]

Explanation

This fault is raised when the IO controller temperature is outside the upper or lower non-critical threshold.

Recommended Action

If you see this fault, monitor other environmental events related to this server and ensure the temperature ranges are within recommended ranges.

Fault Details

```
Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 538
mibFaultName: fltComputeIOHubThermalNonCritical
moClass: compute:IOHub
Type: environmental
```

fltComputeIOHubThermalThresholdCritical

Fault Code:F0539

Message

IO Hub on server [chassisId]/[slotId] temperature: [thermal]

Explanation

This fault is raised when the IO controller temperature is outside the upper or lower critical threshold.

Recommended Action

If you see this fault, take the following actions:

Step 1 Monitor other environmental events related to the server and ensure the temperature ranges are within recommended ranges.

Step 2 Consider turning off the server for a while if possible.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 539
mibFaultName: fltComputeIOHubThermalThresholdCritical
moClass: compute:IOHub
Type: environmental
```

fltComputeIOHubThermalThresholdNonRecoverable

Fault Code:F0540

Message

IO Hub on server [chassisId]/[slotId] temperature: [thermal]

Explanation

This fault is raised when the IO controller temperature is outside the recoverable range of operation.

Recommended Action

If you see this fault, take the following actions:

Step 1 Shut down the server immediately.

Step 2 Create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 540
mibFaultName: fltComputeIOHubThermalThresholdNonRecoverable
moClass: compute:IOHub
Type: environmental
```

fltComputePhysicalAssignedInaccessible

Fault Code:F0322

Message

Server [id] (service profile: [assignedToDn]) inaccessibleServer [chassisId]/[slotId] (service profile: [assignedToDn]) inaccessible

Explanation

This fault typically occurs when the server, which is associated with a service profile, has lost connection to the fabric interconnects. This fault occurs if there are communication issues between the server CIMC and the fabric interconnects.

Recommended Action

If you see this fault, take the following actions:

Step 1 Wait a few minutes to see if the fault clears. This is typically a temporary issue, and can occur after a firmware upgrade.

Step 2 If the fault does not clear after a brief time, remove the server and then reinsert it.

Step 3 Reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: equipment-inaccessible
CallHome: diagnostic
mibFaultCode: 322
mibFaultName: fltComputePhysicalAssignedInaccessible
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalAssignedMissing

Fault Code:F0319

Message

Server [id] (service profile: [assignedToDn]) missingServer [chassisId]/[slotId] (service profile: [assignedToDn]) missing

Explanation

This fault typically occurs when the server, which is associated with a service profile, was previously physically inserted in the slot, but cannot be detected by Cisco UCS Manager.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the server is physically present in the slot, remove and then reinsert it.

Step 2 If the server is not physically present in the slot, reinsert it.

Step 3 Reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-missing
CallHome: none
mibFaultCode: 319
mibFaultName: fltComputePhysicalAssignedMissing
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalAssociationFailed

Fault Code:F0315

Message

Service profile [assignedToDn] failed to associate with server [id]Service profile [assignedToDn] failed to associate with server [chassisId]/[slotId]

Explanation

This fault typically occurs for one of the following reasons:

- The service profile could not be associated with the server.
- The server is down.
- The data path is not working.
- Cisco UCS Manager cannot communicate with one or more of the fabric interconnect, the server, or a component on the server.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the FSM tab and the current state of the server and any FSM operations.

Step 2 If the server is stuck in an inappropriate state, such as booting, power cycle the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: association-failed
CallHome: none
mibFaultCode: 315
mibFaultName: fltComputePhysicalAssociationFailed
moClass: compute:Physical
Type: configuration
```

fltComputePhysicalBiosPostTimeout

Fault Code:F0313

Message

Server [id] (service profile: [assignedToDn]) BIOS failed power-on self testServer [chassisId]/[slotId] (service profile: [assignedToDn]) BIOS failed power-on self test

Explanation

This fault typically occurs when the server has encountered a diagnostic failure.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the POST results for the server. In Cisco UCS Manager GUI, you can access the POST results from the General tab for the server. In Cisco UCS Manager CLI, you can access the POST results through the show post command under the scope for the server.

Step 2 Reacknowledge the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 313
mibFaultName: fltComputePhysicalBiosPostTimeout
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalDiscoveryFailed

Fault Code:F0314

Message

Server [id] (service profile: [assignedToDn]) discovery: [discovery]Server [chassisId]/[slotId] (service profile: [assignedToDn]) discovery: [discovery]

Explanation

This fault typically occurs for one of the following reasons:

- The shallow discovery that occurs when the server associated with service profile failed.
- The server is down.
- The data path is not working.
- Cisco UCS Manager cannot communicate with the CIMC on the server.
- The server cannot communicate with the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the FSM tab and the current state of the server and any FSM operations.

Step 2 Check the error descriptions and see if any server components indicate a failure.

Step 3 If the server or a server component has failed, do the following:

a. Check the operational state of the server.

b. If the server is not operable, re-acknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: discovery-failed
CallHome: diagnostic
mibFaultCode: 314
mibFaultName: fltComputePhysicalDiscoveryFailed
moClass: compute:Physical
Type: operational
```

fltComputePhysicalIdentityUnestablishable

Fault Code:F0306

Message

Server [id] (service profile: [assignedToDn]) has an invalid FRUServer [chassisId]/[slotId] (service profile: [assignedToDn]) has an invalid FRU

Explanation

This fault typically occurs because Cisco UCS Manager has detected an unsupported server or CPU.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that a supported server and/or CPU is installed.

Step 2 Verify that the Cisco UCS Manager capability catalog is up to date.

Step 3 Reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: identity-unestablishable
CallHome: diagnostic
mibFaultCode: 306
mibFaultName: fltComputePhysicalIdentityUnestablishable
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalInoperable

Fault Code:F0317

Message

Server [id] (service profile: [assignedToDn]) health: [operability]Server [chassisId]/[slotId] (service profile: [assignedToDn]) health: [operability]

Explanation

This fault typically occurs when the server has encountered a diagnostic failure.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the POST results for the server.In Cisco UCS Manager GUI, you can access the POST results from the General tab for the server. In Cisco UCS Manager CLI, you can access the POST results through the show post command under the scope for the server.

Step 2 Reacknowledge the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 317
mibFaultName: fltComputePhysicalInoperable
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalInsufficientlyEquipped

Fault Code:F0305

Message

Server [id] (service profile: [assignedToDn]) has insufficient number of DIMMs, CPUs and/or adaptersServer [chassisId]/[slotId] (service profile: [assignedToDn]) has insufficient number of DIMMs, CPUs and/or adapters

Explanation

This fault typically occurs because Cisco UCS Manager has detected that the server has an insufficient number of DIMMs, CPUs, and/or adapters.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the DIMMs are installed in a supported configuration.

Step 2 Verify that an adapter and CPU are installed.

Step 3 Reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: insufficiently-equipped
CallHome: none
mibFaultCode: 305
mibFaultName: fltComputePhysicalInsufficientlyEquipped
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalPost-failure

Fault Code:F0517

Message

Server [id] POST or diagnostic failureServer [chassisId]/[slotId] POST or diagnostic failure

Explanation

This fault typically occurs when the server has encountered a diagnostic failure or an error during POST.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the POST results for the server. In Cisco UCS Manager GUI, you can access the POST results from the General tab for the server. In Cisco UCS Manager CLI, you can access the POST results through the show post command under the scope for the server.

Step 2 Reboot the server.

Step 3 If the above actions did not resolve the issue, execute the **show tech-support** command and contact Cisco Technical Support.

Fault Details

```
Severity: major
Cause: equipment-problem
CallHome: none
mibFaultCode: 517
mibFaultName: fltComputePhysicalPostFailure
moClass: compute:Physical
Type: server
```

fltComputePhysicalPowerProblem

Fault Code:F0311

Message

Server [id] (service profile: [assignedToDn]) oper state: [operState]Server [chassisId]/[slotId] (service profile: [assignedToDn]) oper state: [operState]

Explanation

This fault typically occurs when the server power sensors have detected a problem.

Recommended Action

If you see this fault, take the following actions:

Step 1 Make sure that the server is correctly installed in the chassis and that all cables are secure.

Step 2 If you reinstalled the server, reacknowledge it.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: power-problem
CallHome: none
mibFaultCode: 311
mibFaultName: fltComputePhysicalPowerProblem
```

moClass: compute:Physical
Type: environmental

fltComputePhysicalThermalProblem

Fault Code:F0312

Message

Server [id] (service profile: [assignedToDn]) oper state: [operState]Server [chassisId]/[slotId] (service profile: [assignedToDn]) oper state: [operState]

Explanation

This fault typically occurs when the server thermal sensors have detected a problem.

Recommended Action

If you see this fault, take the following actions:

Step 1 Make sure that the server fans are working properly.

Step 2 Wait for 24 hours to see if the problem resolves itself.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: minor
Cause: thermal-problem
CallHome: environmental
mibFaultCode: 312
mibFaultName: fltComputePhysicalThermalProblem
moClass: compute:Physical
Type: environmental

fltComputePhysicalUnassignedInaccessible

Fault Code:F0321

Message

Server [id] (no profile) inaccessibleServer [chassisId]/[slotId] (no profile) inaccessible

Explanation

This fault typically occurs when the server, which is not associated with a service profile, has lost connection to the fabric interconnects. This fault occurs if there are communication issues between the server CIMC and the fabric interconnects.

Recommended Action

If you see this fault, take the following actions:

Step 1 Wait a few minutes to see if the fault clears. This is typically a temporary issue, and can occur after a firmware upgrade.

Step 2 If the fault does not clear after a brief time, remove the server and then reinsert it.

Step 3 Reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: equipment-inaccessible
CallHome: diagnostic
mibFaultCode: 321
mibFaultName: fltComputePhysicalUnassignedInaccessible
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalUnassignedMissing

Fault Code:F0318

Message

Server [id] (no profile) missingServer [chassisId]/[slotId] (no profile) missing

Explanation

This fault typically occurs when the server, which is not associated with a service profile, was previously physically inserted in the slot, but cannot be detected by Cisco UCS Manager.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the server is physically present in the slot, remove and then reinsert it.

Step 2 If the server is not physically present in the slot, insert it.

Step 3 Reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: equipment-missing
CallHome: none
mibFaultCode: 318
mibFaultName: fltComputePhysicalUnassignedMissing
moClass: compute:Physical
Type: equipment
```

fltComputePhysicalUnidentified

Fault Code:F0320

Message

Server [id] (service profile: [assignedToDn]) has an invalid FRU: [presence]Server [chassisId]/[slotId] (service profile: [assignedToDn]) has an invalid FRU: [presence]

Explanation

This fault typically occurs because Cisco UCS Manager has detected an unsupported server or CPU.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that a supported server and/or CPU is installed.

Step 2 Verify that the Cisco UCS Manager capability catalog is up to date.

Step 3 Reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: identity-unestablishable
CallHome: none
mibFaultCode: 320
mibFaultName: fltComputePhysicalUnidentified
moClass: compute:Physical
Type: equipment
```

fltComputeRtcBatteryInoperable

Fault Code:F0533

Message

RTC Battery on server [chassisId]/[slotId] operability: [operability]

Explanation

This fault is raised when the CMOS battery voltage is below the normal operating range. This impacts the system clock.

Recommended Action

If you see this fault, replace the CMOS battery.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: diagnostic
```

mibFaultCode: 533
mibFaultName: fltComputeRtcBatteryInoperable
moClass: compute:RtcBattery
Type: equipment

fltMgmtIfMisConnect

Fault Code:F0688

Message

Management Port [id] in server [id] is mis connected

Explanation

This fault occurs when the server and FEX connectivity changes.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the connectivity between the server and FEX.

Step 2 If the connectivity was changed by mistake, restore it to its previous configuration.

Step 3 If the connectivity change was intentional, reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: warning
Cause: link-misconnected
CallHome: none
mibFaultCode: 688
mibFaultName: fltMgmtIfMisConnect
moClass: mgmt:If
Type: operational

fltMgmtIfMissing

Fault Code:F0717

Message

Connection to Management Port [id] in server [id] is missing

Explanation

This fault occurs when the connectivity between a server and FEX is removed or unconfigured.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the connectivity between the server and FEX.

Step 2 If the connectivity was changed by mistake, restore it to its previous configuration.

Step 3 If the connectivity change was intentional, reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: link-missing
CallHome: none
mibFaultCode: 717
mibFaultName: fltMgmtIfMissing
moClass: mgmt:If
Type: operational
```

fltMgmtIfNew

Fault Code:F0772

Message

New connection discovered on Management Port [id] in server [id]

Explanation

This fault occurs when the connectivity between a server and a FEX is added or changed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the connectivity between the server and FEX.

Step 2 If the connectivity was changed by mistake, restore it to its previous configuration.

Step 3 If the connectivity change was intentional, reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: new-link
CallHome: none
mibFaultCode: 772
mibFaultName: fltMgmtIfNew
moClass: mgmt:If
Type: operational
```

fltStorageLocalDiskInoperable

Fault Code:F0181

Message

Local disk [id] on server [chassisId]/[slotId] operability: [operability]Local disk [id] on server [id] operability: [operability]

Explanation

This fault occurs when the local disk has become inoperable.

Recommended Action

If you see this fault, take the following actions:

Step 1 Insert the disk in a supported slot.

Step 2 Remove and reinsert the local disk.

Step 3 Replace the disk, if an additional disk is available.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: none
mibFaultCode: 181
mibFaultName: fltStorageLocalDiskInoperable
moClass: storage:LocalDisk
Type: equipment
```

fltStorageLocalDiskSlotEpUnusable

Fault Code:F0776

Message

Local disk [id] on server [serverId] is not usable by the operating system

Explanation

This fault occurs when the server disk drive is in a slot that is not supported by the storage controller.

Recommended Action

If you see this fault, take the following actions:

Step 1 Insert the server disk drive in a supported slot.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: equipment-inoperable
CallHome: diagnostic
mibFaultCode: 776
mibFaultName: fltStorageLocalDiskSlotEpUnusable
moClass: storage:LocalDiskSlotEp
Type: equipment
```

fltStorageLocalLunInoperable

Fault Code:F0843

Message

Local LUN [id] on server [chassisId]/[slotId] operability: [operability]Local LUN [id] on server [id] operability: [operability]

Explanation

This fault occurs when a LUN has become inoperable

Recommended Action

If you see this fault, take the following actions:

Step 1 Make sure the remote storage LUN is accessible to the server.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
CallHome: none
mibFaultCode: 843
mibFaultName: fltStorageLocalLunInoperable
moClass: storage:LocalLun
Type: equipment
```

fltStorageRaidBatteryInoperable

Fault Code:F0531

Message

RAID Battery on server [chassisId]/[slotId] operability: [operability]RAID Battery on server [id] operability: [operability]

Explanation

This fault occurs when the RAID battery voltage is below the normal operating range.

Recommended Action

If you see this fault, take the following actions:

Step 1 Replace the RAID battery.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-inoperable
```

CallHome: diagnostic
mibFaultCode: 531
mibFaultName: fltStorageRaidBatteryInoperable
moClass: storage:RaidBattery
Type: equipment

Service Profile-Related Faults

This section contains faults raised as a result of issues related to the service profile associated with a server.

fltLsComputeBindingAssignmentRequirementsNotMet

Fault Code:F0689

Message

Assignment of service profile [name] to server [pnDn] failed

Explanation

The server could not be assigned to the selected service profile. This fault typically occurs as a result of one of the following issues:

- The selected server does not meet the requirements of the service profile.
- If the service profile was configured for restricted migration, the selected server does not match the currently or previously assigned server.

Recommended Action

If you see this fault, select a different server that meets the requirements of the service profile or matches the currently or previously assigned server.

Fault Details

Severity: minor
Cause: assignment-failed
CallHome: none
mibFaultCode: 689
mibFaultName: fltLsComputeBindingAssignmentRequirementsNotMet
moClass: ls:ComputeBinding
Type: server

fltLsServerAssociationFailed

Fault Code:F0332

Message

Service profile [name] association failed for [pnDn]

Explanation

The service profile could not be associated with the server. This fault typically occurs because Cisco UCS Manager cannot communicate with one or more of the following:

- Fabric interconnect
- CIMC on the server
- SAS controller driver
- Server

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the FSM tab for the server and service profile to determine why the association failed.

Step 2 If the server is stuck in an inappropriate state, such as booting, power cycle the server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: association-failed
CallHome: diagnostic
mibFaultCode: 332
mibFaultName: fltLsServerAssociationFailed
moClass: ls:Server
Type: server
```

fltLsServerConfigFailure

Fault Code:F0327

Message

Service profile [name] configuration failed due to [configQualifier]

Explanation

The named configuration qualifier is not available. This fault typically occurs because Cisco UCS Manager cannot successfully deploy the service profile due to a lack of resources that meet the named qualifier. For example, this fault can occur if the following occurs:

- The service profile is configured for a server adapter with vHBAs, and the adapter on the server does not support vHBAs.
- The service profile is created from a template which includes a server pool, and the server pool is empty.
- The local disk configuration policy in the service profile specifies the No Local Storage mode, but the server contains local disks.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the status of the server pool associated with the service profile. If the pool is empty, add more blade servers to it.

Step 2 Check the state of the server and ensure that it is in either the discovered or unassociated state.

Step 3 If the server is associated or undiscovered, do one of the following:

- Discover the server.
- Disassociate the server from the current service profile.
- Select another server to associate with the service profile.

Step 4 Review each policy in the service profile and verify that the selected server meets the requirements in the policy.

Step 5 If the server does not meet the requirements of the service profile, do one of the following:

- Modify the service profile to match the server.
- Select another server that does meet the requirements to associate with the service profile.

Step 6 If you can verify that the server meets the requirements of the service profile, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: configuration-failure
CallHome: diagnostic
mibFaultCode: 327
mibFaultName: fltLsServerConfigFailure
moClass: ls:Server
Type: server
```

fltLsServerDiscoveryFailed

Fault Code:F0326

Message

Service profile [name] discovery failed

Explanation

The shallow discovery that occurs when the server associated with service profile fails. If the server is up and the data path is working, this fault typically occurs as a result of one of the following issues:

- Cisco UCS Manager cannot communicate with the CIMC on the server.
- The server cannot communicate with the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the FSM tab and view the current state of the server and any FSM operations.

Step 2 Check the error descriptions and see if any server components indicate a failure.

Step 3 If the server or a server component has failed, do the following:

a. Check the operational state of the server.

b. If the server is not operable, reacknowledge the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: discovery-failed
CallHome: none
mibFaultCode: 326
mibFaultName: fltLsServerDiscoveryFailed
moClass: ls:Server
Type: server
```

fltLsServerFailed

Fault Code:F0324

Message

Service profile [name] failed

Explanation

Server has failed. This fault typically occurs if the adapter power on self-test results in major and critical errors.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the POST results for the server. In Cisco UCS Manager GUI, you can access the POST results from the General tab for the server. In Cisco UCS Manager CLI, you can access the POST results through the **show post** command under the scope for the server.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: server-failed
CallHome: none
mibFaultCode: 324
mibFaultName: fltLsServerFailed
moClass: ls:Server
Type: server
```

fltLsServerInaccessible

Fault Code:F0331

Message

Service profile [name] cannot be accessed

Explanation

Cisco UCS Manager cannot communicate with the CIMC on the server. This fault typically occurs as a result of one of the following issues:

- The server port or ports have failed.
- The I/O module is offline.
- The BMC has failed.

Recommended Action

If you see this fault, take the following actions:

Step 1 If Cisco UCS Manager shows that the CIMC is down, physically reseat the server.

Step 2 If Cisco UCS Manager shows that the server ports have failed, attempt to enable them.

Step 3 If the I/O module is offline, check for faults on that component.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: server-inaccessible
CallHome: none
mibFaultCode: 331
mibFaultName: fltLsServerInaccessible
moClass: ls:Server
Type: server
```

fltLsServerMaintenanceFailed

Fault Code:F0329

Message

Service profile [name] maintenance failed

Explanation

Cisco UCS Manager currently does not use this fault.

Recommended Action

If you see this fault, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: maintenance-failed
CallHome: none
mibFaultCode: 329
mibFaultName: fltLsServerMaintenanceFailed
moClass: ls:Server
Type: server
```

fltLsServerRemoved

Fault Code:F0330

Message

Service profile [name] underlying resource removed

Explanation

Cisco UCS Manager cannot access the server associated with the service profile. This fault typically occurs as a result of one of the following issues:

- The server has been physically removed from the slot.
- The server is not available.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the server was removed from the slot, reinsert the server in the slot.

Step 2 If the server was not removed, remove and reinsert the server.**NOTE:** If the server is operable, this action can be disruptive to current operations.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: equipment-removed
CallHome: none
mibFaultCode: 330
mibFaultName: fltLsServerRemoved
moClass: ls:Server
Type: server
```

fltLsServerServer-unfulfilled

Fault Code:F0337

Message

Server [pnDn] does not fulfill Service profile [name] due to [configQualifier]

Explanation

The server no longer meets the qualification requirements of the service profile. This fault typically occurs as a result of one of the following issues:

- The server has been physically changed.
- A required component of the server has failed.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the server inventory compare to the service profile qualifications.

Step 2 If the server inventory does not match the service profile qualifications, do one of the following:

- Associate the server with a different service profile.
- Ensure the server has sufficient resources to qualify for the current service profile.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: server-failed
CallHome: none
mibFaultCode: 337
mibFaultName: fltLsServerServerUnfulfilled
moClass: ls:Server
Type: server
```

fltLsServerUnassociated

Fault Code:F0334

Message

Service profile [name] is not associated

Explanation

The service profile has not yet been associated with a server or a server pool. This fault typically occurs as a result of one of the following issues:

- There is no acceptable server in the server pool.
- The association failed.

Recommended Action

If you see this fault, take the following actions:

Step 1 If you did not intend to associate the service profile, ignore the fault.

Step 2 If you did intend to associate the service profile, check the association failure fault.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: unassociated
CallHome: none
mibFaultCode: 334
mibFaultName: fltLsServerUnassociated
moClass: ls:Server
Type: server
```

fltLsmaintMaintPolicyUnresolvableScheduler

Fault Code:F0795

Message

Schedule [schedName] referenced by maintenance policy [name] does not exist

Explanation

The schedule that is referenced by the maintenance policy does not exist. This fault typically occurs as a result of one of the following issues:

- The schedule does not exist.
- The schedule was deleted.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check if the named schedule exists. If it is deleted or missing, try to create it.

Step 2 If the named schedule is deleted or missing, recreate it.

Step 3 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: non-existent-scheduler
CallHome: none
mibFaultCode: 795
mibFaultName: fltLsmaintMaintPolicyUnresolvableScheduler
moClass: lsmaint:MaintPolicy
Type: server
```

System Event Log-Related Faults

This section contains faults raised as a result of issues related to the system event log (SEL) in the Cisco UCS instance.

fltSysdebugAutoCoreFileExportTargetAutoCoreTransferFailure

Fault Code:F0747

Message

Auto core transfer failure at remote server [hostname]:[path] [exportFailureReason]

Explanation

This fault occurs when Cisco UCS Manager cannot transfer a core file to a remote TFTP server. This is typically the result of one of the following issues:

- The remote TFTP server is not accessible.
- One or more of the parameters for the TFTP server that are specified for the core export target, such as path, port, and server name, are incorrect.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify the connectivity to the remote server.

Step 2 Verify the path information of the remote server.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: warning
Cause: tftp-server-error
CallHome: none
mibFaultCode: 747
mibFaultName: fltSysdebugAutoCoreFileExportTargetAutoCoreTransferFailure
moClass: sysdebug:AutoCoreFileExportTarget
Type: sysdebug
```

fltSysdebugMEpLogMEpLogFull

Fault Code:F0462

Message

Log capacity on [side] IOM [chassisId]/[id] is [capacity]Log capacity on Management Controller on server [chassisId]/[slotId] is [capacity]Log capacity on Management Controller on server [id] is [capacity]

Explanation

This fault typically occurs because Cisco UCS Manager could not transfer the SEL file to the location specified in the SEL policy. This is an info-level fault and can be ignored if you do not want to clear the SEL at this time.

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify the configuration of the SEL policy to ensure that the location, user, and password provided are correct.

Step 2 If you do want to transfer and clear the SEL and the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: log-capacity
CallHome: none
mibFaultCode: 462
mibFaultName: fltSysdebugMEpLogMEpLogFull
moClass: sysdebug:MEpLog
Type: operational
```

fltSysdebugMEpLogMEpLogLog

Fault Code:F0460

Message

Log capacity on [side] IOM [chassisId]/[id] is [capacity]Log capacity on Management Controller on server [chassisId]/[slotId] is [capacity]Log capacity on Management Controller on server [id] is [capacity]

Explanation

This fault typically occurs because Cisco UCS Manager has detected that the system event log (SEL) on the server is approaching full capacity. The available capacity in the log is low. This is an info-level fault and can be ignored if you do not want to clear the SEL at this time.

Recommended Action

If you see this fault, you can clear the SEL in Cisco UCS Manager if desired.

Fault Details

```
Severity: info
Cause: log-capacity
CallHome: none
mibFaultCode: 460
mibFaultName: fltSysdebugMEpLogMEpLogLog
moClass: sysdebug:MEpLog
Type: operational
```

fltSysdebugMEpLogMEpLogVeryLow

Fault Code:F0461

Message

Log capacity on [side] IOM [chassisId]/[id] is [capacity]Log capacity on Management Controller on server [chassisId]/[slotId] is [capacity]Log capacity on Management Controller on server [id] is [capacity]

Explanation

This fault typically occurs because Cisco UCS Manager has detected that the system event log (SEL) on the server is almost full. The available capacity in the log is very low. This is an info-level fault and can be ignored if you do not want to clear the SEL at this time.

Recommended Action

If you see this fault, you can clear the SEL in Cisco UCS Manager if desired.

Fault Details

```
Severity: info
Cause: log-capacity
CallHome: none
mibFaultCode: 461
mibFaultName: fltSysdebugMEpLogMEpLogVeryLow
moClass: sysdebug:MEpLog
Type: operational
```

fltSysdebugMEpLogTransferError

Fault Code:F0532

Message

Server [chassisId]/[slotId] [type] transfer failed: [operState]Server [id] [type] transfer failed: [operState]

Explanation

This fault occurs when the transfer of a managed endpoint log file, such as the SEL, fails.

Recommended Action

If you see this fault, take the following actions:

Step 1 If the fault is related to the SEL, verify the connectivity to the CIMC on the server.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: info
Cause: file-transfer-failed
CallHome: none
mibFaultCode: 532
```

mibFaultName: fltSysdebugMEpLogTransferError
moClass: sysdebug:MEpLog
Type: operational

Traffic Monitoring-related Faults

This section contains faults caused by issues related to traffic monitoring.

fltFabricMonSpanConfigFail

Fault Code:F0757

Message

Configuration for traffic monitor [name] failed, reason: [configFailReason]

Explanation

This fault typically occurs when the configuration of a traffic monitoring session is incorrect.

Recommended Action

If you see this fault, correct the configuration problem provided in the fault description.

Fault Details

Severity: major
Cause: config-error
CallHome: none
mibFaultCode: 757
mibFaultName: fltFabricMonSpanConfigFail
moClass: fabric:Mon
Type: network

Virtual Network Interface-Related Faults

This section contains faults caused by issues related to a virtual network interface allocation in a service profile.

fltDcxNsFailed

Fault Code:F0304

Message

Server [chassisId]/[slotId] (service profile: [assignedToDn]) virtual network interface allocation failed.Server [id] (service profile: [assignedToDn]) virtual network interface allocation failed.

Explanation

The adapter's vif-namespace activation failed due to insufficient resources. Cisco UCS Manager raises this fault when the number of deployed VIF resources exceeds the maximum VIF resources available on the adapter connected to the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 Check the NS "size" and "used" resources to determine by how many vNICs the adapter exceeded the maximum.

Step 2 Unconfigure or delete all vNICs on the adapter above the maximum number.

Step 3 Add additional fabric uplinks from the IOM to the corresponding fabric interconnect and reacknowledge the chassis. This increases the "NS size" on the adapter.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: insufficient-resources
CallHome: none
mibFaultCode: 304
mibFaultName: fltDcxNsFailed
moClass: dcx:Ns
Type: server
```

fltDcxVIfLinkState

Fault Code:F0479

Message

Virtual interface [id] link state is down

Explanation

This fault occurs when Cisco UCS cannot send or receive data through an uplink port.

Recommended Action

If you see this fault, take the following actions:

Step 1 Reenable the uplink port that failed.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: vif-down
CallHome: none
mibFaultCode: 479
mibFaultName: fltDcxVIfLinkState
```

moClass: dcx:VIf
Type: management

fltDcxVcDown

Fault Code:F0283

Message

[transport] VIF [chassisId] / [slotId] [switchId]-[id] down, reason: [stateQual][transport] VIF [chassisId] / [id] [switchId]-[id] down, reason: [stateQual]

Explanation

This fault typically occurs when a fabric interconnect reports one of the following connectivity states for a virtual interface:

- Down
- Errored
- Unavailable

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the uplink physical interface is up.

Step 2 If the vNIC/vHBA is configured for a pin group, verify that the pin group targets are configured correctly.

Step 3 In the Network Control Policy for the vNIC, verify that the 'Action on Uplink Fail' field is set to 'warning'.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

Severity: major
Cause: link-down
CallHome: none
mibFaultCode: 283
mibFaultName: fltDcxVcDown
moClass: dcx:Vc
Type: network

fltDcxVcMgmt-vif-down

Fault Code:F0459

Message

IOM [chassisId] / [slotId] ([switchId]) management VIF [id] down, reason [stateQual]

Explanation

This fault occurs when the transport VIF for an I/O module is down. Cisco UCS Manager raises this fault when a fabric interconnect reports the connectivity state on virtual interface as one of the following:

- Down
- Errored
- Unavailable

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the chassis discovery has gone through successfully. Check the states on all communicating ports from end to end.

Step 2 If connectivity seems correct, decommission and recommission the chassis.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: cmc-vif-down
CallHome: none
mibFaultCode: 459
mibFaultName: fltDcxVcMgmtVifDown
moClass: dcx:Vc
Type: network
```

fltFabricInternalPcDown

Fault Code:F0858

Message

[type] port-channel [portId] on fabric interconnect [id] oper state: [operState], reason: [stateQual]

Explanation

This fault occurs when the transport VIF for a server is down. Cisco UCS Manager raises this fault when a fabric interconnect reports the connectivity state on virtual interface as one of the following:

- Down
- Errored
- Unavailable

Recommended Action

If you see this fault, take the following actions:

Step 1 Verify that the blade server discovery was successful.

Step 2 Check the states on all communicating ports from end to end.

Step 3 If connectivity seems correct, decommission and recommission the server.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: operational-state-down
CallHome: none
mibFaultCode: 858
mibFaultName: fltFabricInternalPcDown
moClass: fabric:InternalPc
Type: network
```

fltVmVifLinkState

Fault Code:F0876

Message

Virtual interface [vifId] link is down; reason [stateQual]

Explanation

This fault occurs when Cisco UCS cannot send or receive data through an uplink port.

Recommended Action

If you see this fault, take the following actions:

Step 1 Enable the failed uplink port.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: vif-down
CallHome: none
mibFaultCode: 876
mibFaultName: fltVmVifLinkState
moClass: vm:Vif
Type: management
```

VLAN-Related Faults

This section contains faults caused by issues related to a VLAN.

fltFabricEthLanEpMissingPrimaryVlan

Fault Code:F0835

Message

Primary vlan missing from fabric: [switchId], port: [slotId]/[portId].

Explanation

This fault occurs when an uplink port or port channel is configured with a primary VLAN that does not exist in the Cisco UCS instance.

Recommended Action

If you see this fault, take the following action:

Step 1 Update the configuration of the port or port channel to include a primary VLAN.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: missing-primary-vlan
CallHome: none
mibFaultCode: 835
mibFaultName: fltFabricEthLanEpMissingPrimaryVlan
moClass: fabric:EthLanEp
Type: management
```

fltFabricEthLanPcMissingPrimaryVlan

Fault Code:F0836

Message

Primary vlan missing from fabric: [switchId], port-channel: [portId].

Explanation

This fault occurs when an uplink port or port channel is configured with a primary VLAN that does not exist in the Cisco UCS instance.

Recommended Action

If you see this fault, take the following action:

Step 1 Update the configuration of the port or port channel to include a primary VLAN.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: missing-primary-vlan
CallHome: none
mibFaultCode: 836
mibFaultName: fltFabricEthLanPcMissingPrimaryVlan
moClass: fabric:EthLanPc
Type: management
```

fltFabricVlanMisconfigured

Fault Code:F0833

Message

VLAN [name] is [operState] because of conflicting vlan-id with an fcoe-vlan

Explanation

This fault typically occurs when VLAN has the same ID as an FCoE VLAN. This issue can cause disruption of traffic.

Recommended Action

If you see this fault, take the following action:

Step 1 Check the VLAN ID.

Step 2 If the ID of the VLAN matches the ID of the FCoE VLAN assigned to a VLAN in the same fabric interconnect, change the ID of either the VLAN or the FCoE VLAN.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: vlan-misconfigured
CallHome: none
mibFaultCode: 833
mibFaultName: fltFabricVlanMisconfigured
moClass: fabric:Vlan
Type: network
```

fltFabricVlanPrimaryVlanMissingIsolated

Fault Code:F0620

Message

Primary Vlan can not be resolved for isolated vlan [name]

Explanation

This fault typically occurs when Cisco UCS Manager encounters a problem resolving the primary VLAN ID corresponding to a particular isolated VLAN.

Recommended Action

If you see this fault, take the following actions:

Step 1 Associate the isolated VLAN with a valid primary VLAN.

Step 2 If the above action did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: minor
Cause: primary-vlan-missing-isolated
CallHome: none
mibFaultCode: 620
mibFaultName: fltFabricVlanPrimaryVlanMissingIsolated
moClass: fabric:Vlan
Type: network
```

fltSwVlanPortNsResourceStatus

Fault Code:F0549

Message

Vlan-Port Resource exceeded

Explanation

This fault occurs when the total number of configured VLANs in the Cisco UCS instance has exceeded the allowed maximum number of configured VLANs on the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 In the Cisco UCS Manager CLI or Cisco UCS Manager GUI, check the port VLAN count to determine by how many VLANs the system is over the maximum.

Step 2 Reduce the VLAN port count in one of the following ways:

- Delete VLANs configured on the LAN cloud.
- Delete VLANs configured on vNICs.
- Unconfigure one or more vNICs.
- Unconfigure one or more uplink Ethernet ports on the fabric interconnect.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: critical
Cause: limit-reached
CallHome: diagnostic
mibFaultCode: 549
mibFaultName: fltSwVlanPortNsResourceStatus
moClass: sw:VlanPortNs
Type: management
```

VSAN-Related Faults

This section contains faults caused by issues related to a VSAN.

fltFabricVsanEpErrorDisabled

Fault Code:F0797

Message

[type] Port [slotId]/[portId] on fabric interconnect [switchId] has VSAN [id] in error disabled statePort channel [portId] on fabric interconnect [switchId] has VSAN [id] in error disabled state

Explanation

This fault typically occurs when a port is assigned to a VSAN that has an ID in the restricted range between 3840 and 4078) or is VSAN 4079, which is reserved.

Recommended Action

If you see this fault, take the following action:

Step 1 If the VSAN ID is in the restricted range between 3840 and 4078, do the following:

a. Delete the port channels on the fabric interconnect.

b. Disable uplink trunking on the fabric-interconnect.

c. Configure the fabric interconnect for fibre channel switch mode.

Step 2 If the VSAN is VSAN 4079, which is reserved, assign the port to a non-reserved VSAN.

Step 3 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: vsan-misconfigured
CallHome: none
mibFaultCode: 797
mibFaultName: fltFabricVsanEpErrorDisabled
moClass: fabric:VsanEp
Type: network
```

fltFabricVsanErrorDisabled

Fault Code:F0796

Message

VSAN [name] is [operState]

Explanation

This fault typically occurs when the VSAN has an ID in the restricted range between 3840 and 4078, and Fibre Channel end host mode is enabled on the fabric interconnect.

Recommended Action

If you see this fault, take the following actions:

Step 1 Delete the port channels on the fabric interconnect.

Step 2 Disable uplink trunking on the fabric-interconnect.

Step 3 Configure the fabric interconnect for fibre channel switch mode.

Step 4 If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Fault Details

```
Severity: major
Cause: vsan-misconfigured
CallHome: none
mibFaultCode: 796
mibFaultName: fltFabricVsanErrorDisabled
moClass: fabric:Vsan
Type: network
```