Intel® Server System R2600SR Product Family

Message and Code Reference Guide

An overview of product error messages and code references.

Rev 1.0

January 2018

Intel® Server Products and Solutions

<Blank page>

Document Revision History

Date	Revision	Changes
January 2018	1.0	Initial release.

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at Intel.com, or from the OEM or retailer.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, and Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

1. Introduction

The Intel® Server System R2600SR Nodes Messages and Code Reference Guide is a comprehensive list of error codes and messages that may be encountered during the normal operation of the system. It covers four major application recording events: System Management Module, BMC, Unified Extensible Firmware Interface (UEFI) and BMC Provisioning Manager.

When attempting to resolve issues with the system, the best practice is to begin with the event log of the application managing the solution using the BMC and BMC Web Console.

The event log contains solution hardware events recorded by the BMC or by UEFI. In addition, events can be generated when diagnostic testing is performed on hard drives or memory through the BMC Provisioning Manager. (These events, however, are not stored in the event log.)

Through this section, view the events that can be generated by BMC, UEFI, or the BMC Provisioning Manager. For each event, a user action gives information for the steps to take to resolve the issue.

2. System Management Module (SMM) Events

The System Management Module provides six (6) management tasks, including:

1. Node status reporting
2. Enclosure power and fan status reporting
3. Enclosure power and fan configuration management
4. Enclosure Vital Product Data (VPD) information reporting
5. Enclosure event log display, save, and clear functions
6. SMM management and settings backup/restore functions

This chapter details event messages related to the functions of the SMM.

2.1 Event Descriptors

The following items are aspects of events that give information for a full picture of each event.

Event Identifier

An identifier that uniquely identifies an event.

Event Description

The logged message string that appears for an event.

Severity

An indication of the level of concern for the condition. The severity is abbreviated in the event log to the first character. The following severities can be displayed:

- **Informational**. The event was recorded for audit purposes, usually a user action or a change of state that is normal behavior.
- **Warning**. The event is not as severe as an error, but, if possible, the condition should be corrected before it becomes an error. It might also be a condition that requires additional monitoring or maintenance.
- **Error**. The event is a failure or critical condition that impairs service or an expected function.
- **Critical**. A key component in the server is no longer functioning.

Alert Category

Similar events are grouped together in categories. The alert category indicates the type of event, such as system or power supply.

The alert category is in the following format: *device-error type*, where *device* is the specific device in the server that caused the event to be generated.

User Response

Indication of the actions to perform to solve the event. Perform the steps listed in this section in the order shown until the problem is solved. Contact Support if the problem is not resolved after all steps are performed.

2.2 System Management Module (SMM) Error Message Handling Detail List

The following are separate error messages with handling details for each.

0201001A : 12V_SENSE: Voltage sensor, warning event was asserted, reading value : %V (Threshold : %V)

Asserted when voltage sensed on 12V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 12V_SENSE warning is still asserted, replace the SMM module.

0201001B: 3V3_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 3.3V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 3V3_SENSE warning is still asserted, replace the SMM module.

0201001C: 5V_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 5V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 5V_SENSE warning is still asserted, replace the SMM module.

0201001D: 2V5_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 2.5V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 2V5_SENSE warning is still asserted, replace the SMM module.

0201001E :1V2_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 1.2V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 1.V2_SENSE warning is still asserted, replace the SMM module.

0201001F: 1V15_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 1.15V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 1.V15_SENSE warning is still asserted, replace the SMM module.

02010020: VBAT_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on coin battery output is lower than lower critical threshold.

Severity Warning

Alert Category System - SMM system event

User Response Procedure

Replace the coin battery on the SMM.

0201021A: 12V_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 12V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 12V_SENSE error is still asserted, replace the SMM module.

0201021B :3V3_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 12V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 3V3_SENSE error is still asserted, replace the SMM module.

0201021C :5V_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 5V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 5V_SENSE error is still asserted, replace the SMM module.

0201021D :2V5_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 2V5 power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 2V5_SENSE error is still asserted, replace the SMM module.

0201021E : 1V2_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 1.2V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 1V2_SENSE error is still asserted, replace the SMM module.

0201021F : 1V15_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on 1.15V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

1. Reseat the SMM module.
2. If 1V15_SENSE error is still asserted, replace the SMM module.

02010020 : VBAT_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold : %V)

Asserted when voltage sensed on coin battery output is lower than lower critical threshold.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Replace coin battery on the SMM.

04010010 : FAN_TACH_1A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010011 : FAN_TACH_1B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010012 : FAN_TACH_2A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010013 : FAN_TACH_2B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010014 : FAN_TACH_3A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010015 : FAN_TACH_3B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010016 : FAN_TACH_4A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010017 : FAN_TACH_4B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010018 : FAN_TACH_5A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010019 : FAN_TACH_5B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 768RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010210 : FAN_TACH_1A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010211 : FAN_TACH_1B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010212 : FAN_TACH_2A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010213 : FAN_TACH_2B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010214 : FAN_TACH_3A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010215 : FAN_TACH_3B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat fan module a couple of times. If errors still persist, replace the fan module.

04010216 : FAN_TACH_4A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat the fan module a couple of times. If errors still persist, replace the fan module.

04010217 : FAN_TACH_4B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM)

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat fan module a couple of times. If errors still persist, replace the fan module.

04010218 : FAN_TACH_5A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM) Asserted when Fan tach reading is below error threshold RPM.

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat fan module a couple of times. If errors still persist, replace the fan module.

04010219 : FAN_TACH_5B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold : 640RPM) Asserted when Fan tach reading is below error threshold RPM.

Asserted when Fan tach reading is below the warning threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal event

User Response Procedure

1. If the warning is not de-asserted after several minutes, check that all five (5) fans are installed.
2. Reseat fan module a couple of times. If errors still persist, replace the fan module.

040701CA : FAN_FFS: Fan sensor, transition to Non-Critical from OK was asserted.

All system fans run at full speed.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

080701CB PSU_FFS: Power Supply sensor, transition to Non-Critical from OK was asserted.

All system fans run at full speed.

Severity Warning

Alert Category Thermal – System Thermal event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

080707E8 : PS1_Throttle: Power Supply sensor, Monitor was asserted.

The power supply needs to lower its power consumption or risk being shut down due to a power supply overcurrent or over-temperature condition.

Severity Critical

Alert Category PSU - Power Supply event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If the fault recurs, please call Service.

080707E9 : PS2_Throttle: Power Supply sensor, Monitor was asserted.

The power supply needs to lower its power consumption or risk being shut down due to a power supply overcurrent or over-temperature condition.

Severity Critical

Alert Category PSU - Power Supply event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If the fault recurs, please call Service.

080708A8 : PS1_AC_LOW_LINE: Power Supply sensor, Informational was asserted.

The power supply is not supporting low-line input but initially applied with a low-line voltage.

Severity Informational

Alert Category PSU - Power Supply event

User Response Procedure

Information only; no action is required.

080708A9 : PS2_AC_LOW_LINE: Power Supply sensor, Informational was asserted.

The power supply is not supporting low-line input but initially applied with a low-line voltage.

Severity Informational

Alert Category PSU - Power Supply event

User Response Procedure

Information only; no action is required.

086F06A4 : PS1_EPOW: Power Supply sensor, Configuration error was asserted.

The power supply has an early power-off caused by input power approach undervoltage or overvoltage condition.

Severity Critical

Alert Category PSU - Power Supply event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If the fault recurs, please call Service.

086F06A5 : PS2_EPOW: Power Supply sensor, Configuration error was asserted.

The power supply has an early power-off caused by input power approach undervoltage or overvoltage condition.

Severity Critical

Alert Category PSU - Power Supply event

User Response Procedure

1. Check power supply LEDs
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If the fault recurs, please call Service.

086F06D8 : EPOW_Out: Power Supply sensor, Configuration error was asserted.

Node is notified of PSU AC lost condition. Node could enter power throttling state and affect performance.

Severity Critical

Alert Category PSU - Power Supply event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If the fault recurs, please call Service.

086F06D9 : Throttle_Out: Power Supply sensor, Configuration error was asserted.

Node is notified of PSU AC lost condition. Node could enter power throttling state and performance could be affected.

Severity Critical

Alert Category PSU - Power Supply event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If the fault recurs, please call Service.

106F0202 : EvtLogDisabled: Event Logging Disabled sensor, Log Area Reset/Cleared was asserted.

SMM System Event Log (SEL) is cleared.

Severity Informational

Alert Category System – SMM system event

User Response Procedure

Information only; no action is required.

106F0402 : EvtLogDisabled: Event Logging Disabled sensor, system event log full was asserted.

Error is asserted when System Event Log (SEL) is 100% full.

Severity Critical

Alert Category System – SMM system event

User Response Procedure

Clear the System Event Log (SEL).

106F0502 : EvtLogDisabled: Event Logging Disabled sensor, system event log almost full was asserted.

Warning is asserted when System Event Log (SEL) is at least 75% full.

Severity Warning

Alert Category System – SMM system event

User Response Procedure

No action is required. Be aware that the System Event Log (SEL) is almost full.

146F0231 : SMM_RESET: Button Or Switch sensor, Reset Button pressed was asserted.

Indicates SMM system reboot.

Severity Informational

Alert Category System – SMM system event

User Response Procedure

Information only. No action is required.

1D6F0030 : SMM_POWER_ON: System Boot Initiated sensor, Initiated by power up was asserted.

Indicates SMM system power-on.

Severity Informational

Alert Category System – SMM system event

User Response Procedure

Information only. No action is required.

21070150 : NODE1_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the node into a ready state.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070151 : NODE2_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the node into a ready state.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070152 : NODE3_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the node into a ready state.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070153 : NODE4_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the node into a ready state.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070154 : NODE1_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the node.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070155 : NODE2_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the node.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070156 : NODE3_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the node.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070157 : NODE4_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the node.

Severity Warning

Alert Category Node – Node event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset the BMC.
4. If error recurs, reseat the node.
5. If error recurs, replace the node.

21070164 : NODE1_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute: system fans are ramped to prevent the node from potential thermal conditions.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

21070165 : NODE2_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute: system fans are ramped to prevent the node from potential thermal conditions.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

21070166 : NODE1_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute: system fans are ramped to prevent the node from potential thermal conditions.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

21070167 : NODE4_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute: system fans are ramped to prevent the node from potential thermal conditions.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

2107016C : NODE1_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute: system fans are ramped to prevent the node from potential thermal conditions.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

2107016D : NODE2_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute: system fans are ramped to prevent the node from potential thermal conditions.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

2107016E : NODE3_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes and the client OS is powered off. Reseat the node to recover it from the fault state.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

2107016F : NODE4_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes and the client OS is powered off. Reseat the node to recover it from the fault state.

Severity Warning

Alert Category Node – Node event

User Response Procedure

Information only. No action is required.

21070192 : PS1_12V_OC_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The 12V output current experiences a current overload condition but lower than the overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070193 : PS2_12V_OC_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The 12V output current experiences a current overload condition but lower than the overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070194 : PS1_VIN_OC_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The input current experiences a current overload condition but lower than the overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070195 : PS2_VIN_OC_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The input current experiences a current overload condition but lower than the overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070196 : PS1_VIN_OV_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The input voltage reaches overvoltage condition but lower than overvoltage lockout limit.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070197 : PS2_VIN_OV_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The input voltage reaches overvoltage condition but lower than overvoltage lockout limit.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070198 : PS1_VIN_UV_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The input voltage drops to the EPOW# active threshold but not down to the Turn-Off voltage.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070199 : PS2_VIN_UV_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The input voltage drops to the EPOW# active threshold but not down to the Turn-Off voltage.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

2107019E : PS1_Thermal_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

2107019F : PS2_Thermal_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

210701A2 : PS1_iShare_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The power supply has a poor current sharing on its main 12V output.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

210701A3 : PS2_iShare_Warn: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The power supply has a poor current sharing on its main 12V output.

Severity Warning

Alert Category PSU - Power Supply event

User Response Procedure

Information only. No action is required.

21070668 : NODE1_FS_NORESP: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Please shut down the OS.
2. Reset the BMC.
3. Check the System Event Log (SEL) if other Fail-Safe SEL is asserted.

21070669 : NODE2_FS_NORESP: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Please shut down the OS.
2. Reset the BMC.
3. Check the System Event Log (SEL) if other Fail-Safe SEL is asserted.

2107066A : NODE3_FS_NORESP: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Please shut down the OS.
2. Reset the BMC.
3. Check the System Event Log (SEL) if other Fail-Safe SEL is asserted.

2107066B : NODE4_FS_NORESP: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Please shut down the OS.
2. Reset the BMC.
3. Check the System Event Log (SEL) if other Fail-Safe SEL is asserted.

21070670 : NODE1_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off; the allocated power budget has be retrieved and the power permission has been rejected.

Severity Critical

Alert Category Node - Node event

User Response Procedure

Replace the node (for more detailed information, please refer to the Intel® Server System R2600SR Setup and Service Guide).

21070671 : NODE2_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off; the allocated power budget has be retrieved and the power permission has been rejected.

Severity Critical

Alert Category Node - Node event

User Response Procedure

Replace the node (for more detailed information, please refer to the Intel® Server System R2600SR Setup and Service Guide).

21070672 : NODE3_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off; the allocated power budget has be retrieved and the power permission has been rejected.

Severity Critical

Alert Category Node - Node event

User Response Procedure

Replace the node (for more detailed information, please refer to the Intel® Server System R2600SR Setup and Service Guide).

21070673 : NODE4_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off; the allocated power budget has be retrieved and the power permission has been rejected.

Severity Critical

Alert Category Node - Node event

User Response Procedure

Replace the node (for more detailed information, please refer to Intel® Server System R2600SR Setup and Service Guide).

21070840 : NODE1_PRESENT: Slot Or Connector sensor, Informational was asserted.

The node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070841 : NODE2_PRESENT: Slot Or Connector sensor, Informational was asserted.

The node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070842 : NODE3_PRESENT: Slot Or Connector sensor, Informational was asserted.

The node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070843 : NODE4_PRESENT: Slot Or Connector sensor, Informational was asserted.

The node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070844 : NODE1_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070845 : NODE2_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070846 : NODE3_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070847 : NODE4_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070848 : NODE1_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to AC; cycle the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

21070849 : NODE2_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to AC; cycle the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

2107084A : NODE3_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to AC; cycle the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

2107084B : NODE4_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to AC; cycle the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

2107084C : NODE1_RESET: Slot Or Connector sensor, Informational was asserted.

Performed BMC reset on the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

2107084D : NODE2_RESET: Slot Or Connector sensor, Informational was asserted.

Performed BMC reset on the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

2107084E : NODE3_RESET: Slot Or Connector sensor, Informational was asserted.

Performed BMC reset on the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

2107084F : NODE4_RESET: Slot Or Connector sensor, Informational was asserted.

Performed BMC reset on the node.

Severity Informational

Alert Category Node - Node event

User Response Procedure

Information only; no action required.

216F002D : PIOR_R_3V3_PG:Slot Or Connector sensor, Fault Status asserted was asserted.

An event indicates right PIOR 3.3V power good fault.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Call Service Support.

216F0035 : SD_Card_No_Exist: Slot Or Connector sensor, Fault Status asserted was asserted.

An event indicates the SMM No SD card existence or fault.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Insert the SMM SD card onto the SMM assembly.

216F0036 : PIOR_R_Fault:Slot Or Connector sensor, Fault Status asserted was asserted.

An event indicates SMM No Right PIOR card existence or fault.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Insert the card into PCIe* 1-B slot.

216F0037 : PIOR_L_Fault:Slot Or Connector sensor, Fault Status asserted was asserted.

An event indicates SMM No Left PIOR card existence or fault.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Insert the card into PCIe* 3-B slot.

216F0038 : EIOM_No_Exist: Slot Or Connector sensor, Fault Status asserted was asserted.

An event indicates SMM No EIOM card existence or fault.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Insert the EIOM card.

216F0058 : NODE1_CAP_LOW: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The restored power cap value is invalid since it is lower than the current power cap boundary.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Re-configure the power cap value of the node from the BMC Web Console or IPMI command.

216F0059 : NODE2_CAP_LOW: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The restored power cap value is invalid since it is lower than the current power cap boundary.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Re-configure the power cap value of the node from the BMC Web Console or IPMI command.

216F005A : NODE3_CAP_LOW: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The restored power cap value is invalid since it is lower than the current power cap boundary.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Re-configure the power cap value of the node from the Web GUI or IPMI command.

216F005B : NODE4_CAP_LOW: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The restored power cap value is invalid since it is lower than the current power cap boundary.

Severity Critical

Alert Category System - SMM system event

User Response Procedure

Re-configure the power cap value of the node from the Web GUI or IPMI command.

216F005C : Node1_Cap_Fail: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

Failed to set power cap to node.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F005D : Node2_Cap_Fail: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

Failed to set power cap to node.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F005E : Node3_Cap_Fail: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

Failed to set power cap to node.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F005F : Node4_Cap_Fail: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

Failed to set power cap to node.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0060 : NODE1_XCC _FAULT: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC failed to start the initialization in 2 minutes after the node was inserted.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Reset the BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0061 : NODE2_XCC_FAULT: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC failed to start the initialization in 2 minutes after the node was inserted.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Reset the BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0062 : NODE3_XCC_FAULT: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC failed to start the initialization in 2 minutes after the node was inserted.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Reset the BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0063 : NODE4_XCC_FAULT: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC failed to start the initialization in 2 minutes after the node was inserted.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Reset the BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0074 : NODE1_PMIN_2_BIG: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The inventory power reports from BMC includes an invalid value whose Pmin is greater than Pmax.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU to run again:
    a. Enable/disable device.
    b. Change memory speed or link disable setting.
    c. Change UPI speed or link disable setting.
    d. Change the C1E, C-state, or P-state setting.
    e. Change the # of enabled CPU cores.
    f. Change Turbo setting.
    g. Change CPU frequency.
2. If the error recurs, replace the node.

216F0075 : NODE2_PMIN_2_BIG: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The inventory power reports from BMC includes an invalid value whose Pmin is greater than Pmax.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU to run again:
    a. Enable/disable device
    b. Change memory speed .or link disable setting.
    c. Change UPI speed or link disable setting.
    d. Change the C1E, C-state, or P-state setting.
    e. Change the # of enabled CPU cores.
    f. Change Turbo setting.
    g. Change CPU frequency.
2. If the error recurs, replace the node.

216F0076 : NODE3_PMIN_2_BIG: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The inventory power reports from BMC includes an invalid value whose Pmin is greater than Pmax.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU to run again:
    a. Enable/disable device.
    b. Change memory speed or link disable setting.
    c. Change UPI speed or link disable setting.
    d. Change the C1E, C-state, or P-state setting.
    e. Change the # of enabled CPU cores.
    f. Change Turbo setting.
    g. Change CPU frequency.
2. If the error recurs, replace the node.

216F0077 : NODE4_PMIN_2_BIG: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The inventory power reports from BMC includes an invalid value whose Pmin is greater than Pmax.

Severity Critical

Alert Category Node - Node event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU to run again:
    a. Enable/disable device.
    b. Change memory speed or link disable setting.
    c. Change UPI speed or link disable setting.
    d. Change the C1E, C-state, or P-state setting.
    e. Change the # of enabled CPU cores.
    f. Change Turbo setting.
    g. Change CPU frequency.
2. If the error recurs, replace the node.

216F0080 : PS1_12Va_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0081 : PS2_12Va_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0082 : PS1_12Va_OV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0083 : PS2_12Va_OV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0084 : PS1_12Va_UV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0085 : PS2_12Va_UV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0086 : PS1_12V_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0087 : PS2_12V_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0088 : PS1_12V_OV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V output voltage reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

216F0089 : PS2_12V_OV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V output voltage reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F008A : PS1_12V_UV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F008B : PS2_12V_UV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The 12V AUX output current drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F008C : PS1_VIN_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F008D : PS2_VIN_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F008E : PS1_VIN_OV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input voltage reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F008F : PS2_VIN_OV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input voltage reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0090 : PS1_VIN_UV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input voltage drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F0091 : PS2_VIN_UV_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input voltage drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F009A : PS1_Thermal_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached and persists over 30 seconds.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F009B : PS2_Thermal_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached and persists over 30 seconds.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F009C : PS1_FAN_Error: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply is cannot maintain a fan speed sufficient to provide necessary cooling for the power supply.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F009D : PS2_FAN_Error: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply is cannot maintain a fan speed sufficient to provide necessary cooling for the power supply.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00A0 : PS1_OVS_Error: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply shutdown due to throttle# assertion over 3 seconds for indicating a load over 105% of the power supply rating.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00A1 : PS2_OVS_Error: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply shutdown due to throttle# assertion over 3 seconds for indicating a load over 105% of the power supply rating.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00A6 : PS1_VIN_UVI_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input power applied does not exceed the Turn-On voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00A7 : PS2_VIN_UVI_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The input power applied does not exceed the Turn-On voltage.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00AC : PS1_INTRL_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply experiences an internal fault that has caused an overcurrent condition.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00AD : PS2_INTRL_OC_Err: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply experiences an internal fault that has caused an overcurrent condition.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check the power cord and input voltage.
    - If DC LED is not lit, remove and reinstall the power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00AE : PS1_INTRMTNT_ERR: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply experiences an internal fault that has caused a non-current condition.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00AF : PS2_INTRMTNT_ERR: Slot Or Connector sensor, Fault Status asserted was asserted.

The power supply experiences an internal fault that has caused a non-current condition.

Severity Critical

Alert Category PSU – Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If a fault recurs, please call Service.

216F00B0 : Fan1_No_Present: Slot Or Connector sensor, Fault Status asserted was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

216F00B1 : Fan2_No_Present: Slot Or Connector sensor, Fault Status asserted was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

216F00B2 : Fan3_No_Present: Slot Or Connector sensor, Fault Status asserted was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

216F00B3 : Fan4_No_Present: Slot Or Connector sensor, Fault Status asserted was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

216F00B4 : Fan5_No_Present: Slot Or Connector sensor, Fault Status asserted was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

216F00D0 : Enclosure_NoPerm: Slot Or Connector sensor, Fault Status asserted was asserted.

The power permission of the whole enclosure has been locked.

Severity Critical

Alert Category System – SSM System Event

User Response Procedure

Make sure that all system fans are installed.

216F00D2 : ENCL_Cap_LOW: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The restored power cap value is invalid since it is lower than current power cap boundary.

Severity Critical

Alert Category System – SSM System Event

User Response Procedure

Re-configure the enclosure power cap value.

216F00D3 : ENCL_Cap_FAIL: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

Failed to set enclosure power cap.

Severity Critical

Alert Category System – SSM System Event

User Response Procedure

1. Re-configure the node power cap value to check which nodes cause the fault.
2. Reseat the node.
3. If the error recurs, replace the node.

216F00D6 : ENCL_PMAX_2_BIG: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The summary of Pmax of existing powered-on nodes is beyond the available power bank.

Severity Critical

Alert Category System – SSM System Event

User Response Procedure

Please contact with the Service team to upgrade PSU to afford the estimated power consumption.

216F00D7 : ENCL_PMIN_2_BIG: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The summary of Pmax of existing powered-on nodes is beyond the available power bank.

Severity Critical

Alert Category System – SSM System Event

User Response Procedure

Please contact with the Service team to upgrade PSU to afford the estimated power consumption.

216F012E : PIOR_L_3V3_PG:Slot Or Connector sensor, Fault Status asserted was asserted.

An event indicates left PIOR 3.3V power good fault.

Severity Critical

Alert Category System – SSM System Event

User Response Procedure

Call Service Support.

21EF00C0 : Thermal_Protect: Slot Or Connector sensor, Fault Status asserted was deasserted.

System has over-heated condition, and enter protection mode. Fans are ramped up to help cooling and node power is capped.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

21EF00C1 : Thermal_OverHeat: Slot Or Connector sensor, Fault Status asserted was asserted.

System has over-heated condition. Fans are ramped up to help cooling.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

2B6F0139 : P_BOOT_FAIL: Version Change sensor, Firmware or software change detected with associated Entity was asserted.

An event indicates booting from Bank 2.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

Call Service Support.

2.3 System Management Module (SMM) Event Codes List

This section details System Management Module (SMM) event codes.

0201001A: 12V_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 12V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 12V_SENSE warning is still asserted, replace the SMM module.

0201001B: 3V3_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 3.3V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 3V3_SENSE warning is still asserted, replace the SMM module.

0201001C: 5V_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 5V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 5V_SENSE warning is still asserted, replace SMM module.

0201001D: 2V5_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 2.5V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If V5_SENSE warning is still asserted, replace SMM module.

0201001E: 1V2_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 1.2V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 1V2_SENSE warning is still asserted, replace SMM module.

0201001F: 1V15_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 1.15V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 1V15_SENSE warning is still asserted, replace SMM module.

02010020: VBAT_SENSE: Voltage sensor, warning event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on coin battery output voltage is lower than lower critical threshold.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

Replace the coin battery on SMM.

0201021A: 12V_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 12V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 12V_SENSE error is still asserted, replace SMM module.

0201021B: 3V3_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 3.3V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 3V3_SENSE error is still asserted, replace SMM module.

0201021C: 5V_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 5V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 5V_SENSE error is still asserted, replace SMM module.

0201021D: 2V5_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 2.5V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 2V5_SENSE error is still asserted, replace SMM module.

0201021E: 1V2_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 1.2V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 1V2_SENSE error is still asserted, replace SMM module.

0201021F: 1V15_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on 1.15V power rail is lower than lower critical threshold or higher than upper critical threshold.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

1. Reseat SMM module.
2. If 1V2_SENSE error is still asserted, replace SMM module.

02010220: VBAT_SENSE: Voltage sensor, critical event was asserted, reading value: %V (Threshold: %V)

Asserted when voltage sensed on coin battery output voltage is lower than lower critical threshold.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Replace the coin battery on SMM.

04010010: FAN_TACH_1A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 68RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010011: FAN_TACH_1B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010012: FAN_TACH_2A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010013: FAN_TACH_2B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010014: FAN_TACH_3A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists replace fan module.

04010015: FAN_TACH_3B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010016: FAN_TACH_4A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010017: FAN_TACH_4B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010018: FAN_TACH_5A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010019: FAN_TACH_5B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold:768RPM)

Asserted when Fan tech reading is below warning threshold RPM.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010210: FAN_TACH_1A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If warning is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010211: FAN_TACH_1B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010212: FAN_TACH_2A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010213: FAN_TACH_2B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010214: FAN_TACH_3A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010215: FAN_TACH_3B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010216: FAN_TACH_4A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010217: FAN_TACH_4B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010218: FAN_TACH_5A: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

04010219: FAN_TACH_5B: Fan sensor, warning event was asserted, reading value: %RPM (Threshold: 640RPM)

Asserted when Fan tech reading is below error threshold RPM.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. If critical is not de-asserted after several minutes, check all five (5) fans are installed.
2. Reseat fan module a couple of times. If error still persists, replace fan module.

040701CA: FAN_FFS: Fan sensor, transition to Non-Critical from OK was asserted.

All system fans run at full speed.

Severity Warning

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

040800B0: FAN1_NO_PRESENT: Fan sensor, Device Removed/Device Absent was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

040800B1: FAN2_NO_PRESENT: Fan sensor, Device Removed/Device Absent was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

040800B2: FAN3_NO_PRESENT: Fan sensor, Device Removed/Device Absent was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

040800B3: FAN4_NO_PRESENT: Fan sensor, Device Removed/Device Absent was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

040800B4: FAN5_NO_PRESENT: Fan sensor, Device Removed/Device Absent was asserted.

Indicated fan module is missing from the fan slot.

Severity Critical

Alert Category Thermal – System Thermal Event

User Response Procedure

1. Ensure all ten (10) fans are installed.
2. Reseat the indicated missing fans.
3. Replace the indicated missing fans.

080701AA: PSU_POLICY_LOST: Power Supply sensor, transition to Non-Critical from OK was asserted.

The configured PSU policy has been disabled.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check the inventory power of all powered-on nodes to see if the summary over current power bank.
2. Replace the node with light configuration.
3. Install the PSU with higher capacity.

080701CB: PSU_FFS: Power Supply sensor, transition to Non-Critical from OK was asserted.

All power supply fans run at full speed.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

080701D8: PS_EPOW_OUT: Power Supply sensor, transition to Non-Critical from OK was asserted.

Node is notified of PSU AC lost condition. Node could enter power throttling state and performance could be affected.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

080701D9: PS_THROTTLE_OUT: Power Supply sensor, transition to Non-Critical from OK was asserted.

Node is notified of PSU Overcurrent condition. Node could enter power throttling state and performance could be affected.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

080701E8: PS1_THROTTLE: Power Supply sensor, transition to Non-Critical from OK was asserted.

The power supply needs to lower its power consumption or risk being shut down due to a power supply overcurrent or over-temperature condition.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

080701E9: PS2_THROTTLE: Power Supply sensor, transition to Non-Critical from OK was asserted.

The power supply needs to lower its power consumption or risk being shut down due to a power supply overcurrent or over-temperature condition.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

080702E2: PSU_MISMATCH: Power Supply sensor, transition to Critical from less severe was asserted.

Installed PSUs are of mixed types/ratings.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check the PSU type of each installed PSU.
2. Make sure the PSUs are the same type.

080707A4: PS1_EPOW: Power Supply sensor, Monitor was asserted.

The power supply has an early power-off caused by input power approach undervoltage or overvoltage condition.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

080707A5: PS2_EPOW: Power Supply sensor, Monitor was asserted.

The power supply has an early power-off caused by input power approach undervoltage or overvoltage condition.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

080708A8: PS1_AC_LOW_LINE: Power Supply sensor, Informational was asserted.

The power supply is not supporting low-line input although a low-line voltage was initially applied to the PSU.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

080708A9: PS2_AC_LOW_LINE: Power Supply sensor, Informational was asserted.

The power supply is not supporting low-line input although a low-line voltage was initially applied to the PSU.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

080708AB: PS_0_OUTPUT_FAIL: Power Supply sensor, Informational was asserted.

The zero output functions abnormally.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

080801E0: PS1: Power Supply sensor, Device Inserted/Device Present was asserted.

The PSU is installed in the indicated slot.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

080801E1: PS2: Power Supply sensor, Device Inserted/Device Present was asserted.

The PSU is installed in the indicated slot.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F0180: PS1_12Va_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0181: PS2_12Va_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0182: PS1_12Va_OV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0183: PS2_12Va_OV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0184: PS1_12Va_UV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0185: PS2_12Va_UV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0186: PS1_12V_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0187: PS2_12V_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0188: PS1_12V_OV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V AUX output current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0189: PS2_12V_OV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V output voltage reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F018A: PS1_12V_UV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V output voltage drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F018B: PS2_12V_UV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The 12V output voltage drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F018C: PS1_VIN_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F018D: PS2_VIN_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input current experiences a current load greater than the current limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F018E: PS1_VIN_OV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input voltage reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F018F: PS2_VIN_OV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input voltage reaches overvoltage lockout limit.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0190: PS1_VIN_UV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input voltage drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0191: PS2_VIN_UV_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input voltage drops to the Turn-Off voltage.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F019A: PS1_THERMAL_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached and persists over 30 seconds.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F019B: PS2_THERMAL_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached and persists over 30 seconds.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F019C: PS1_FAN_ERROR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply cannot maintain a fan speed sufficient to provide necessary cooling for the power supply.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F019D: PS2_FAN_ERROR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply cannot maintain a fan speed sufficient to provide necessary cooling for the power supply.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01A0: PS1_OVS_ERROR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply shutdown was due to a throttle# assertion over 3 seconds and for indicating a load over 105% of the power supply rating.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01A1: PS2_OVS_ERROR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply shutdown was due to a throttle# assertion over 3 seconds and for indicating a load over 105% of the power supply rating.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01A6: PS1_VIN_UVI_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input power applied does not exceed the Turn-On voltage.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01A7: PS2_VIN_UVI_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The input power applied does not exceed the Turn-On voltage.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01AC: PS1_INTRL_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply experiences an internal fault-caused overcurrent condition.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01AD: PS2_INTRL_OC_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply experiences an internal fault-caused overcurrent condition.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01AE: PS1_INTRMTNT_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply experiences an internal fault caused overcurrent condition.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F01AF: PS2_INTRMTNT_ERR: Power Supply sensor, Power Supply Failure detected was asserted.

The power supply experiences an internal fault caused overcurrent condition.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0292: PS1_12V_OC_WARN: Power Supply sensor, Predictive Failure was asserted.

The 12V output current experiences a current overload condition but lower than overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check power supply LEDs:
    - If AC LED is not lit, check power cord and input voltage.
    - If DC LED is not lit, remove and reinstall power supply.
    - If error LED is lit, replace the power supply.
2. If fault recurs, please call Service.

086F0293: PS2_12V_OC_WARN: Power Supply sensor, Predictive Failure was asserted.

The 12V output current experiences a current overload condition but lower than overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F0294: PS1_VIN_OC_WARN: Power Supply sensor, Predictive Failure was asserted.

The input current experiences a current overload condition but lower than overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F0295: PS2_VIN_OC_WARN: Power Supply sensor, Predictive Failure was asserted.

The input current experiences a current overload condition but lower than overcurrent limit.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F0296: PS1_VIN_OV_WARN: Power Supply sensor, Predictive Failure was asserted.

The input voltage reaches overvoltage condition but lower than overvoltage lockout limit.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F0297: PS2_VIN_OV_WARN: Power Supply sensor, Predictive Failure was asserted.

The input voltage reaches overvoltage condition but lower than overvoltage lockout limit.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F0298: PS1_VIN_UV_WARN: Power Supply sensor, Predictive Failure was asserted.

The input voltage drops to the EPOW# active threshold but not down to the Turn-Off voltage.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F0299: PS2_VIN_UV_WARN: Power Supply sensor, Predictive Failure was asserted.

The input voltage drops to the EPOW# active threshold but not down to the Turn-Off voltage.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F029E: PS1_THERMAL_WARN: Power Supply sensor, Predictive Failure was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F029F: PS2_THERMAL_WARN: Power Supply sensor, Predictive Failure was asserted.

The temperature-sensing device internal to the power supply reports the warning temperature is reached.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F02A2: PS1_iSHARE_WARN: Power Supply sensor, Predictive Failure was asserted.

The power supply has a poor current sharing on its main 12V output.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F02A3: PS1_iSHARE_WARN: Power Supply sensor, Predictive Failure was asserted.

The power supply has a poor current sharing on its main 12V output.

Severity Warning

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F03E0: PS1: Power Supply sensor, Power Supply input lost (AC/DC) was asserted.

The line cord input of indicated PSU is lost.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F03E1: PS2: Power Supply sensor, Power Supply input lost (AC/DC) was asserted.

The line cord input of indicated PSU is lost.

Severity Informational

Alert Category PSU - Power Supply Event

User Response Procedure

Information only; no action is required.

086F06E0: PS1: Power Supply sensor, Configuration error was asserted.

The installed PSU is not supported.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check the PSU type installed.
2. Make sure the PSU is on the support list.

086F06E1: PS2: Power Supply sensor, Configuration error was asserted.

The installed PSU is not supported.

Severity Critical

Alert Category PSU - Power Supply Event

User Response Procedure

1. Check the PSU type installed.
2. Make sure the PSU is in the supportlist.

106F0202: EvtLogDisabled: Event Logging Disabled sensor, Log Area Reset/Cleared was asserted.

SMM System Event Log (SEL) is cleared.

Severity Informational

Alert Category System – SMM System Event

User Response Procedure

Information only; no action is required.

106F0402: EvtLogDisabled: Event Logging Disabled sensor, system event log full was asserted.

Error is asserted when System Event Log (SEL) is 100% full.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Clear the SMM System Event Log (SEL).

106F0502: EvtLogDisabled: Event Logging Disabled sensor, system event log almost full was asserted.

Warning is asserted when System Event Log (SEL) is at least 75% full.

Severity Warning

Alert Category System – SMM System Event

User Response Procedure

No action is required. Be aware that the System Event Log is almost full.

146F0231: SMM_RESET: Button Or Switch sensor, Reset Button pressed was asserted.

An event indicates an SMM system reboot.

Severity Informational

Alert Category System – SMM System Event

User Response Procedure

Information only; no action is required.

146F0232: USER_RST_DEFAULT: Button Or Switch sensor, Reset Button pressed was asserted.

User reset the system configuration to default setting.

Severity Informational

Alert Category System – SMM System Event

User Response Procedure

Information only; no action is required.

1509002D: PIOR_R_3V3_PG: Module Or Board sensor, Device Disabled was asserted.

An event indicates that the right PIOR 3.3V power good has a fault.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Call Service Support.

1509002E: PIOR_L_3V3_PG: Module Or Board sensor, Device Disabled was asserted.

An event indicates that the left PIOR 3.3V power good has a fault.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Call Service Support.

15090035: SD_CARD_FAULT: Module Or Board sensor, Device Disabled was asserted.

An event indicates an SMM No SD card existence or fault.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Insert the SMM SD card into the SMM assembly.

15090036: PIOR_R_FAULT: Module Or Board sensor, Device Disabled was asserted.

An event indicates an SMM No Right PIOR card existence or fault.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Insert the card into PCIe* 1-B slot.

15090037: PIOR_L_FAULT: Module Or Board sensor, Device Disabled was asserted.

An event indicates an SMM No Left PIOR card existence or fault.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Insert the card into PCIe* 3-B slot.

15090038: EIOM_FAULT: Module Or Board sensor, Device Disabled was asserted.

An event indicates an SMM No EIOM card existence or fault.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Insert the EIOM card.

180702C0: THERMAL_OVERHEAT: Chassis sensor, transition to Critical from less severe was asserted.

System has over-heated condition. Fans are ramped up to help cooling.

Severity Critical

Alert Category Thermal - System Thermal Event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

180702C1: THERMAL_PROTECT: Chassis sensor, transition to Critical from less severe was asserted.

System has had or is in an over-heated condition. Fans speed has been increased to help cooling and node power has been throttled.

Severity Critical

Alert Category Thermal - System Thermal Event

User Response Procedure

1. Ensure the room temperature remains at the required level.
2. Ensure all fan modules are installed and operating properly.

180702D0: ENCL_NO_PERM: Chassis sensor, transition to Critical from less severe was asserted.

The power permission of whole chassis has been locked.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Make sure that all system fans are installed.

180702D2: ENCL_CAP_LOW: Chassis sensor, transition to Critical from less severe was asserted.

The restored power cap value is invalid since it is lower than the current power cap boundary.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Reconfigure the enclosure power cap value.

180702D3: ENCL_CAP_FAIL: Chassis sensor, transition to Critical from less severe was asserted.

Failed to set chassis power cap.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

1. Re-configure the node power cap value to check which nodes cause the fault.
2. Reseat the node.
3. If the error recurs, replace the node.

180702D6: ENCL_PMAX_2_BIG: Chassis sensor, transition to Critical from less severe was asserted.

The summary of PMax of existing powered on nodes are above the available power bank.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Please contact the Service team to upgrade PSU to afford the estimated power consumption.

180702D7: ENCL_PMIN_2_BIG: Chassis sensor, transition to Critical from less severe was asserted.

The summary of PMax of existing powered on nodes are above the available power bank.

Severity Critical

Alert Category System – SMM System Event

User Response Procedure

Please contact the Service team to upgrade PSU to afford the estimated power consumption.

180708CE: HI_PCI_NOACSTIC: Chassis sensor, Informational was asserted.

The acoustic mode has been disabled due to the installation of a high power PCIe* card.

Severity Informational

Alert Category System – SMM System Event

User Response Procedure

Information only; no action is required.

1D6F0030: SMM_POWER_ON: System Boot Initiated sensor, Initiated by power up was asserted.

An event indicates SMM system power is on.

Severity Informational

Alert Category System – SMM System Event

User Response Procedure

Information only; no action is required.

21070150: NODE1_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the compute node into ready state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070151: NODE2_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the compute node into ready state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070152: NODE3_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the compute node into ready state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070153: NODE4_1ST_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

BMC failed to get the power permission to put the compute node into ready state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070154: NODE1_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the compute node.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070155: NODE2_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the compute node.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070156: NODE3_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the compute node.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070157: NODE4_2ND_NOPERM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

OS failed to get the power permission to power on the compute node.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

1. Check the PSU configuration.
2. Check FAN status.
3. Reset BMC.
4. If error recurs, reseat the compute node.
5. If after reseating the compute node the error recurs, replace the compute node.

21070164: NODE1_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute; system fans are ramped to prevent the compute node from potential thermal conditions.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070165: NODE2_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute; system fans are ramped to prevent the compute node from potential thermal conditions.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070166: NODE1_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute; system fans are ramped to prevent the compute node from potential thermal conditions.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070167: NODE4_NO_COMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 1 minute; system fans are ramped to prevent the compute node from potential thermal conditions.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107016C: NODE1_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes and the client OS is power off, reseat the compute node to recover it from fault state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107016D: NODE2_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes and the client OS is powered off, reseat the compute node to recover it from fault state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107016E: NODE3_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes and the client OS is powered off, reseat the compute node to recover it from fault state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107016F: NODE4_RESEAT_SMM: Slot Or Connector sensor, transition to Non-Critical from OK was asserted.

The BMC has no response over 7 minutes and the client OS is powered off, reseat the compute node to recover it from fault state.

Severity Warning

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070668: NODE1_FS_NORESP: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Shut down the OS.
2. Reset the BMC.
3. Check the SEL if other Fail-Safe SEL asserted.

21070669: NODE2_FS_NORESP: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Shut down the OS.
2. Reset the BMC.
3. Check the SEL if other Fail-Safe SEL asserted.

2107066A: NODE3_FS_NORESP: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Shut down the OS.
2. Reset the BMC.
3. Check the SEL if other Fail-Safe SEL asserted.

2107066B: NODE4_FS_NORESP: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 7 minutes after the client OS is powered on; no further action will be taken.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Shut down the OS.
2. Reset the BMC.
3. Check the SEL if other Fail-Safe SEL asserted.

21070670: NODE1_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off. The allocated power budget has be retrieved; the power permission and the power permission has been rejected.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Replace the compute node (For more detailed information, please refer to the Intel® Server System R2600SR Setup and Service Guide).

21070671: NODE2_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off. The allocated power budget has be retrieved; the power permission and the power permission has been rejected.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Replace the compute node (For more detailed information, please refer to the Intel® Server System R2600SR Setup and Service Guide).

21070672: NODE3_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off. The allocated power budget has be retrieved; the power permission and the power permission has been rejected.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Replace the compute node(for more detailed information, please refer to the Intel® Server System R2600SR Setup and Service Guide).

21070673: NODE4_FS_NOPERM: Slot Or Connector sensor, transition to Non-recoverable was asserted.

The BMC has no response over 14 minutes and the client OS is powered off. The allocated power budget has be retrieved; the power permission and the power permission has been rejected.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Replace the compute node (For more detailed information, please refer to the Intel® Server System R2600SR Setup and Service Guide).

21070844: NODE1_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The compute node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070845: NODE2_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The compute node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070846: NODE3_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The compute node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070847: NODE4_DC_OFF: Slot Or Connector sensor, Informational was asserted.

The compute node is turned off (DC-Off).

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070848: NODE1_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to the AC cycle on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070849: NODE2_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to the AC cycle on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107084A: NODE3_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to the AC cycle on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107084B: NODE4_RESEAT: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to the AC cycle on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107084C: NODE1_RESET: Slot Or Connector sensor, Informational was asserted.

Performed a virtual reseat to the AC cycle on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107084D: NODE2_RESET: Slot Or Connector sensor, Informational was asserted.

Performed BMC reset on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107084E: NODE3_RESET: Slot Or Connector sensor, Informational was asserted.

Performed BMC reset on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107084F: NODE4_RESET: Slot Or Connector sensor, Informational was asserted.

Performed BMC reset on the compute node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070878: NODE1_HI_PCI: Slot Or Connector sensor, Informational was asserted.

The high-power PCIe* card is installed in the indicated node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21070879: NODE2_HI_PCI: Slot Or Connector sensor, Informational was asserted.

The high-power PCIe* card is installed in the indicated node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107087A: NODE3_HI_PCI: Slot Or Connector sensor, Informational was asserted.

The high-power PCIe* card is installed in the indicated node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

2107087B: NODE4_HI_PCI: Slot Or Connector sensor, Informational was asserted.

The high-power PCIe* card is installed in the indicated node.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21080140: NODE1_PRESENT: Slot Or Connector sensor, Device Inserted/Device Present was asserted.

The compute node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21080141: NODE2_PRESENT: Slot Or Connector sensor, Device Inserted/Device Present was asserted.

The compute node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21080142: NODE3_PRESENT: Slot Or Connector sensor, Device Inserted/Device Present was asserted.

The compute node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

21080143: NODE4_PRESENT: Slot Or Connector sensor, Device Inserted / Device Present was asserted.

The compute node is installed in the indicated slot.

Severity Informational

Alert Category Node - Node Event

User Response Procedure

Information only; no action is required.

216F0058: NODE1_CAP_LOW: Slot Or Connector sensor, Fault Status asserted was asserted.

The restored power cap value is invalid since it is lower than current power cap boundary.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Re-configure the power cap value of the compute node from Web GUI or IPMI command.

216F0059: NODE2_CAP_LOW: Slot Or Connector sensor, Fault Status asserted was asserted.

The restored power cap value is invalid since it is lower than current power cap boundary.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Re-configure the power cap value of the compute node from the Web GUI or IPMI command.

216F005A: NODE3_CAP_LOW: Slot Or Connector sensor, Fault Status asserted was asserted.

The restored power cap value is invalid since it is lower than current power cap boundary.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Re-configure the power cap value of the compute node from the Web GUI or IPMI command.

216F005B: NODE4_CAP_LOW: Slot Or Connector sensor, Fault Status asserted was asserted.

The restored power cap value is invalid since it is lower than current power cap boundary.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

Re-configure the power cap value of the compute node from the Web GUI or IPMI command.

216F005C: NODE1_CAP_FAIL: Slot Or Connector sensor, Fault Status asserted was asserted.

Failed to set power cap to the compute node.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs after reseating the node, replace the node.

216F005D: NODE2_CAP_FAIL: Slot Or Connector sensor, Fault Status asserted was asserted.

Failed to set power cap to the compute node.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs after reseating the node, replace the node.

216F005E: NODE3_CAP_FAIL: Slot Or Connector sensor, Fault Status asserted was asserted.

Failed to set power cap to the compute node.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs after reseating the node, replace the node.

216F005F: NODE4_CAP_FAIL: Slot Or Connector sensor, Fault Status asserted was asserted.

Failed to set power cap to the compute node.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Re-configure the node power cap value.
2. If the error recurs, reseat the node.
3. If the error recurs after reseating the node, replace the node.

216F0060: NODE1_XCC_FAULT: Slot Or Connector sensor, Fault Status asserted was asserted.

The BMC failed to start the initialization in 2 minutes since the compute node was inserted.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Reset BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0061: NODE2_XCC_FAULT: Slot Or Connector sensor, Fault Status asserted was asserted.

The BMC failed to start the initialization in 2 minutes since the compute node was inserted.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Reset BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0062: NODE3_ XCC_FAULT: Slot Or Connector sensor, Fault Status asserted was asserted.

The BMC failed to start the initialization in 2 minutes since the compute node was inserted.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Reset BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0063: NODE4_XCC_FAULT: Slot Or Connector sensor, Fault Status asserted was asserted.

The BMC failed to start the initialization in 2 minutes since the compute node was inserted.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Reset BMC.
2. If the error recurs, reseat the node.
3. If the error recurs, replace the node.

216F0074: NODE1_PMIN_2_BIG: Slot Or Connector sensor, Fault Status asserted was asserted.

The inventory power reports from BMC includes invalid value, whose PMin is greater than Pmax.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU into running again.
    a. Device is enabled/disabled
    b. Memory speed or link disable setting changed
    c. UPI speed or link disable setting changed
    d. C1E, C-state, or P-state setting changed
    e. # of enabled CPU cores changed
    f. Turbo setting changed
    g. CPU frequency limit changed
2. If the error recurs, replace the node.

216F0075: NODE2_PMIN_2_BIG: Slot Or Connector sensor, Fault Status asserted was asserted.

The inventory power reports from BMC includes invalid value, whose PMin is greater than Pmax.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU into running again.
    a. Device is enabled/disabled
    b. Memory speed or link disable setting changed
    c. UPI speed or link disable setting changed
    d. C1E, C-state, or P-state setting changed
    e. # of enabled CPU cores changed
    f. Turbo setting changed
    g. CPU frequency limit changed
2. If the error recurs, replace the node.

216F0076: NODE3_PMIN_2_BIG: Slot Or Connector sensor, Fault Status asserted was asserted.

The inventory power reports from BMC includes invalid value, whose Pmin is greater than Pmax.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU into running again.
    a. Device is enabled/disabled
    b. Memory speed or link disable setting changed
    c. UPI speed or link disable setting changed
    d. C1E, C-state, or P-state setting changed
    e. # of enabled CPU cores changed
    f. Turbo setting changed
    g. CPU frequency limit changed
2. If the error recurs, replace the node.

216F0077: NODE4_PMIN_2_BIG: Slot Or Connector sensor, Fault Status asserted was asserted.

The inventory power reports from BMC includes invalid value, whose Pmin is greater than Pmax.

Severity Critical

Alert Category Node - Node Event

User Response Procedure

1. Change items in UEFI F1 Setup to force PTU into running again.
    a. Device is enabled/disabled
    b. Memory speed or link disable setting changed
    c. UPI speed or link disable setting changed
    d. C1E, C-state, or P-state setting changed
    e. # of enabled CPU cores changed
    f. Turbo setting changed
    g. CPU frequency limit changed
2. If the error recurs, replace the node.

2B6F0139: PRIMRY_BOOT_FAIL: Version Change sensor, Firmware or software change detected with associated Entity was asserted.

An event which indicates booting from Bank 2.

Severity Warning

Alert Category System - SMM System Event

User Response Procedure

Call Service Support.

3. BMC Events

When a hardware event is detected by the BMC on the server, the BMC writes that event to the System Event Log (SEL) on the server.

For information about viewing the event log, see the Intel® Server System R2600SR System Management Module Users Guide.

3.1 Event Descriptors

The following items are aspects of events that give information for a full picture of each event.

Event Identifier

An identifier that uniquely identifies an event.

Event Description

The logged message string that appears for an event. When the event string is displayed in the event log, information such as a specific component is displayed. In this documentation, that additional information appears as variables, such as [arg1] or [arg2].

Explanation

Phrase which provides additional information to detail why the event occurred.

Severity

An indication of the level of concern for the condition. The severity is abbreviated in the event log to the first character. The following severities can be displayed:

- **Informational**. The event was recorded for audit purposes, usually a user action or a change of state that is normal behavior.
- **Warning**. The event is not as severe as an error, but, if possible, the condition should be corrected before it becomes an error. It might also be a condition that requires additional monitoring or maintenance.
- **Error**. The event is a failure or critical condition that impairs service or an expected function.
- **Critical**. A key component in the server is no longer functioning.

Alert Category

Similar events are grouped together in categories. The alert category indicates the type of event, such as system or power supply.

The alert category is in the following format: *device-error type*, where *device* is the specific device in the server that caused the event to be generated.

User Response

Indication of the actions to perform to solve the event. Perform the steps listed in this section in the order shown until the problem is solved. Contact Support if the problem is not resolved after all steps are performed.

Serviceable

Indicates whether user action is required to correct the problem.

CIM Information

Provides the prefix of the message ID and the sequence number used by the CIM message registry.

SNMP Trap ID

The SNMP Trap ID found in the SNMP Alert Management Information Base (MIB).

3.2 BMC Event List

This section lists all messages that can be sent from the BMC.

FQXSPBR4000I: Management Controller [arg1]: Configuration restored from a file by user [arg2].

This message is for the use case where a user restores a Management Controller configuration from a file.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0027

User Response Procedure

Information only; no action is required.

FQXSPBR4001I: Running the backup Management Controller [arg1] main application.

This message is for the use case where a Management Controller has resorted to running the backup main application.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category System - other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0030

User Response Procedure

Update the BMC firmware to a version that the server supports.

Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before update the code.

FQXSPBR4002I: Management Controller [arg1] Reset was caused by restoring default values.

This message is for the use case where a Management Controller has been reset due to a user restoring the configuration to default values.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0032

User Response Procedure

Information only; no action is required.

FQXSPBR4003I: Platform Watchdog Timer expired for [arg1].

This message is for the use case when an implementation has detected a Platform Watchdog Timer Expired.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - OS Timeout **SNMP Trap ID: 21**

CIM Prefix: IMM CIM ID: 0039

User Response Procedure

Complete the following steps until the problem is solved:

1. Reconfigure the Watchdog timer to a higher value.
2. Make sure that the BMC Ethernet-over-USB interface is enabled.
3. Reinstall the RNDIS or cdc_ether device driver for the operating system.
4. Disable the Watchdog.
5. Check the integrity of the installed operating system.

FQXSPBR4004I: Server timeouts set by user [arg1]: EnableOSWatchdog=[arg2], OSWatchdogTimout=[arg3], EnableLoaderWatchdog=[arg4], LoaderTimeout=[arg5].

A user configures Server Timeouts.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0095

User Response Procedure

Information only; no action is required.

FQXSPBR4005I: Management Controller [arg1]: Configuration saved to a file by user [arg2].

A user saves a Management Controller configuration to a file.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0109

User Response Procedure

Information only; no action is required.

FQXSPBR4006I: Management Controller [arg1]: Configuration restoration from a file by user [arg2] completed.

This message is for the use case where a user restores a Management Controller configuration from a file and it completes.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0136

User Response Procedure

Information only; no action is required.

FQXSPBR4007I: Management Controller [arg1]: Configuration restoration from a file by user [arg2] failed to complete.

This message is for the use case where a user restores a Management Controller configuration from a file and the restoration fails to complete.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0137

User Response Procedure

Complete the following steps until the problem is solved:

1. Turn off the server and disconnect it from the power source.
2. Disconnect the server from AC power cycle to reset the BMC.
3. After 45 seconds, reconnect the server to the power source and turn on the server.
4. Retry the operation.

FQXSPBR4008I: Management Controller [arg1]: Configuration restoration from a file by user [arg2] failed to start.

This message is for the use case where a user restores a Management Controller configuration from a file and the restoration fails to start.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0138

User Response Procedure

Complete the following steps until the problem is solved:

1. Turn off the server and disconnect it from the power source.
2. Disconnect the server from AC power cycle to reset the BMC.
3. After 45 seconds, reconnect the server to the power source and turn on the server.
4. Retry the operation.

FQXSPBT0007I: No bootable media available for system [ComputerSystemElementName].

This message is for the use case when an implementation has detected a system with No Bootable Media.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: PLAT CIM ID: 0286

User Response Procedure

Please ensure bootable media is installed correctly.

FQXSPCA0002M: Numeric sensor [NumericSensorElementName] going low (lower critical) has asserted.

This message is for the use case when an implementation has detected a Lower Critical sensor going low has asserted.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category Critical - Fan Failure **SNMP Trap ID: 11**

CIM Prefix: PLAT CIM ID: 0480

User Response Procedure

Complete the following steps:

1. Check the event log of the System Management Module (SMM) and BMC for any fan or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.

FQXSPCA0007J: Numeric sensor [NumericSensorElementName] going high (upper non-critical) has asserted.

This message is for the use case when an implementation has detected an Upper Non-critical sensor going high has asserted.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - Temperature **SNMP Trap ID: 12**

CIM Prefix: PLAT CIM ID: 0490

User Response Procedure

Complete the following steps:

1. Check the event log of the System Management Module (SMM) and BMC for any fan- or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.

FQXSPCA0009M: Numeric sensor [NumericSensorElementName] going high (upper critical) has asserted.

This message is for the use case when an implementation has detected an Upper Critical sensor going high has asserted.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0494

User Response Procedure

Complete the following steps:

1. Check the event log of the System Management Module (SMM) and BMC for any fan- or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.

FQXSPCA0011N: Numeric sensor [NumericSensorElementName] going high (upper non-recoverable) has asserted.

This message is for the use case when an implementation has detected an Upper Critical sensor going high has asserted.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0498

User Response Procedure

Complete the following steps:

1. Check the event log of the System Management Module (SMM) and BMC for any fan- or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.

FQXSPCA0015J: Sensor [SensorElementName] has transitioned from normal to non-critical state.

This message is for the use case when an implementation has detected a Sensor transitioned to non-critical from normal.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - Temperature **SNMP Trap ID: 12**

CIM Prefix: PLAT CIM ID: 0520

User Response Procedure

Complete the following steps:

1. Check the event log of the System Management Module (SMM) and BMC for any fan- or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.

FQXSPCA0017M: Sensor [SensorElementName] has transitioned to critical from a less severe state.

This message is for the use case when an implementation has detected a Sensor transitioned to critical from less severe.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0522

User Response Procedure

Complete the following steps:

1. Check the event log of the System Management Module (SMM) and BMC for any fan- or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.

FQXSPCA0019N: Sensor [SensorElementName] has transitioned to non-recoverable from a less severe state.

This message is for the use case when an implementation has detected a Sensor transitioned to non-recoverable from less severe.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0524

User Response Procedure

Complete the following steps:

1. Check the event log of the System Management Module (SMM) and BMC for any fan- or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.

FQXSPCA2002I: Numeric sensor [NumericSensorElementName] going low (lower critical) has deasserted.

This message is for the use case when an implementation has detected a Lower Critical sensor going low has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Fan Failure **SNMP Trap ID: 11**

CIM Prefix: PLAT CIM ID: 0481

User Response Procedure

Information only; no action is required.

FQXSPCA2007I: Numeric sensor [NumericSensorElementName] going high (upper non-critical) has deasserted.

This message is for the use case when an implementation has detected an Upper Non-critical sensor going high has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Temperature **SNMP Trap ID: 12**

CIM Prefix: PLAT CIM ID: 0491

User Response Procedure

Information only; no action is required.

FQXSPCA2009I: Numeric sensor [NumericSensorElementName] going high (upper critical) has deasserted.

This message is for the use case when an implementation has detected an Upper Critical sensor going high has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0495

User Response Procedure

Information only; no action is required.

FQXSPCA2011I: Numeric sensor [NumericSensorElementName] going high (upper non-recoverable) has deasserted.

This message is for the use case when an implementation has detected an Upper Non-recoverable sensor going high has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0499

User Response Procedure

Information only; no action is required.

FQXSPCA2015I: Sensor [SensorElementName] has deasserted the transition from normal to non-critical state.

This message is for the use case when an implementation has detected that a Sensor has deasserted a transition to non-critical from normal.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Temperature **SNMP Trap ID: 12**

CIM Prefix: PLAT CIM ID: 0521

User Response Procedure

Information only; no action is required.

FQXSPCA2017I: Sensor [SensorElementName] has transitioned to a less severe state from critical.

This message is for the use case when an implementation has detected a Sensor transition to less severe from critical.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0523

User Response Procedure

Information only; no action is required.

FQXSPCA2019I: Sensor [SensorElementName] has deasserted the transition to non-recoverable from a less severe state.

This message is for the use case when an implementation has detected that the Sensor transition to non-recoverable from less severe has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0525

User Response Procedure

Information only; no action is required.

FQXSPCN4000I: Serial Redirection set by user [arg1]: Mode=[arg2], BaudRate=[arg3], StopBits=[arg4], Parity=[arg5], SessionTerminateSequence=[arg6].

A user configured the Serial Port mode.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0078

User Response Procedure

Information only; no action is required.

FQXSPCN4001I: Remote Control session started by user [arg1] in [arg2] mode.

Remote Control session started.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0128

User Response Procedure

Information only; no action is required.

FQXSPCN4002I: User [arg1] has terminated an active console session.

A user has terminated an active console session.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0145

User Response Procedure

Information only; no action is required.

FQXSPCN4003I: Remote Control session started by user [arg1] in [arg2] mode has been closed.

Remote Control session closed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0194

User Response Procedure

Information only; no action is required.

FQXSPDM4000I: Inventory data changed for device [arg1], new device data hash=[arg2], new master data hash=[arg3] .

Something has caused the physical inventory to change.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0072

User Response Procedure

Information only; no action is required.

FQXSPDM4001I: Storage [arg1] has changed.

This message is for the use case where an IP address for the Storage Management has changed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - IMM Network **SNMP Trap ID: 37**

CIM Prefix: IMM CIM ID: 0139

User Response Procedure

Information only; no action is required.

FQXSPDM4002I: Device [arg1] VPD is not valid.

The VPD for a device is invalid.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0142

User Response Procedure

Information only; no action is required.

FQXSPDM4003I: TKLM servers set by user [arg1]: TKLMServer1=[arg2] Port=[arg3], TKLMServer2= [arg4] Port=[arg5], TKLMServer3=[arg6] Port=[arg7], TKLMServer4=[arg8] Port=[arg9].

A user configured the TKLM servers.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0146

User Response Procedure

Information only; no action is required.

FQXSPDM4004I: TKLM servers device group set by user [arg1]: TKLMServerDeviceGroup=[arg2] .

A user configured the TKLM device group.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0147

User Response Procedure

Information only; no action is required.

FQXSPDM4005I: User [arg1] has generated a new encryption key pair and installed a self-signed certificate for the TKLM client.

User generated a new encryption key pair and installed a self-signed certificate for the TKLM client.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0148

User Response Procedure

Information only; no action is required.

FQXSPDM4006I: User [arg1] has generated a new encryption key and certificate signing request for the TKLM client.

User generated a new encryption key and certificate signing request for the TKLM client.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0149

User Response Procedure

Information only; no action is required.

FQXSPDM4007I: User [arg1] has imported a signed certificate for the TKLM client from [arg2].

User imported a signed certificate for the TKLM client.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0150

User Response Procedure

Information only; no action is required.

FQXSPDM4008I: User [arg1] has imported a server certificate for the TKLM server.

User imported a server certificate for the TKLM client.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0150

User Response Procedure

Information only; no action is required.

FQXSPDM4009I: User [arg1] has [arg2] file [arg3] from [arg4].

User has mounted/unmounted file from URL or server.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0162

User Response Procedure

Information only; no action is required.

FQXSPDM4010I: Inventory data collecting and processing complete for [arg1], sequence number is [arg2].

Inventory data collecting and processing complete.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0192

User Response Procedure

Information only; no action is required.

FQXSPEM0003I: The Log [RecordLogElementName] has been cleared.

This message is for the use case when an implementation has detected that a Log was Cleared.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0200

User Response Procedure

Information only; no action is required.

FQXSPEM0004I: The Log [RecordLogElementName] is full.

This message is for the use case when an implementation has detected that a Log was Full.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0202

User Response Procedure

Information only; no action is required.

FQXSPEM0005I: The Log [RecordLogElementName] is almost full.

This message is for the use case when an implementation has detected that a Log is Almost Full.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0202

User Response Procedure

Information only; no action is required.

FQXSPEM0009I: The System [ComputerSystemElementName] has generated an auxiliary Log Entry in Log [RecordLogElement].

This message is for the use case when an implementation has detected an Auxiliary Log Entry Event.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0202

User Response Procedure

Information only; no action is required.

FQXSPEM4000I: The [arg1] on system [arg2] cleared by user [arg3].

This message is for the use case where a Management Controller Event Log on a system is cleared by a user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0020

User Response Procedure

Information only; no action is required.

FQXSPEM4001I: The [arg1] on system [arg2] is 75% full.

This message is for the use case where a Management Controller Event Log on a system is 75% full.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Event Log Fullness **SNMP Trap ID: 35**

CIM Prefix: IMM CIM ID: 0037

User Response Procedure

Information only; no action is required.

FQXSPEM4002I: The [arg1] on system [arg2] is 100% full.

This message is for the use case where a Management Controller Event Log on a system is 100% full.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Event Log Fullness **SNMP Trap ID: 35**

CIM Prefix: IMM CIM ID: 0037

User Response Procedure

To avoid losing older log entries, save the log as a text file and clear the log.

FQXSPEM4003I: LED [arg1] state changed to [arg2] by [arg3].

A user has modified the state of an LED.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0071

User Response Procedure

Information only; no action is required.

FQXSPEM4004I: SNMP [arg1] enabled by user [arg2] .

A user enabled SNMPv1 or SNMPv3 or Traps.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0073

User Response Procedure

Information only; no action is required.

FQXSPEM4005I: SNMP [arg1] disabled by user [arg2] .

A user enabled SNMPv1 or SNMPv3 or Traps.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0073

User Response Procedure

Information only; no action is required.

FQXSPEM4006I: Alert Configuration Global Event Notification set by user [arg1]: RetryLimit=[arg2], RetryInterval=[arg3], EntryInterval=[arg4].

A user changes the Global Event Notification settings.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0110

User Response Procedure

Information only; no action is required.

FQXSPEM4007I: Alert Recipient Number [arg1] updated: Name=[arg2], DeliveryMethod=[arg3], Address=[arg4], IncludeLog=[arg5], Enabled=[arg6], EnabledAlerts=[arg7], AllowedFilters=[arg8].

A user adds or updates an Alert Recipient.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0111

User Response Procedure

Information only; no action is required.

FQXSPEM4008I: SNMP Traps enabled by user [arg1]: EnabledAlerts=[arg2], AllowedFilters=[arg3].

A user enabled the SNMP Traps configuration.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0112

User Response Procedure

Information only; no action is required.

FQXSPEM4009I: The UEFI Definitions have been changed.

A UEFI Definitions change has been detected.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0152

User Response Procedure

Information only; no action is required.

FQXSPEM4010I: UEFI Reported: [arg1].

A UEFI audit event has been logged.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0161

User Response Procedure

Information only; no action is required.

FQXSPEM4011I: XCC failed to log previous event [arg1].

BMC failed to log a previous event.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0196

User Response Procedure

Information only; no action is required.

FQXSPEM4012I: User [arg1] made system [arg2] Encapsulation lite Mode.

Encapsulation lite mode status change.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0201

User Response Procedure

Information only; no action is required.

FQXSPEM4018I: Enclosure issue detected with one or more units. Please check the enclosure units to repair the problem.([arg1],[arg2],[arg3],[arg4],[arg5])

Enclosure issue detected with one or more units.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0207

User Response Procedure

Information only; no action is required.

FQXSPEM4019I: Connectivity issue detected with the enclosure. Please check your cable configurations to repair the problem.([arg1],[arg2],[arg3],[arg4],[arg5])

Connectivity issue detected with the enclosure.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0208

User Response Procedure

Information only; no action is required.

FQXSPEM4020I: Fan problem detected with the enclosure. Please check the enclosure unit fan for correct operation.([arg1],[arg2],[arg3],[arg4],[arg5])

Fan problem detected with the enclosure.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0209

User Response Procedure

Information only; no action is required.

FQXSPEM4022I: Enclosure power supply has problem. Please check the enclosure unit power supply for correctoperation.([arg1],[arg2],[arg3],[arg4],[arg5])

Enclosure power supply has problem.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0210

User Response Procedure

Information only; no action is required.

FQXSPEM4023I: One or more virtual drive are in abnormal status that may cause unavailable virtual drive. Please check the event logs and if events are targeted to the same disk then replace the drive. If necessary, contact technical support for additional assistance.([arg1],[arg2],[arg3],[arg4], [arg5])

One or more virtual drive are in abnormal status that may cause an unavailable virtual drive.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0211

User Response Procedure

Information only; no action is required.

FQXSPEM4025I: One or more virtual drives has a problem. Please contact technical support to resolve this issue.([arg1],[arg2],[arg3],[arg4],[arg5])

One or more virtual drives has a problem.

Severity Informational

Serviceable No

Automatically Notify Support Yes

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0213

User Response Procedure

Information only; no action is required.

FQXSPEM4028I: The port [arg1] of PCIe device [arg2] at [arg3] has link [arg4].

The port [arg1] of PCIe* device [arg2] at [arg3] has link [arg4]. PCI device link.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0220

User Response Procedure

Information only; no action is required.

FQXSPEM4029I: All PCIe slots on [arg1] may not be functional based upon your current CPU population.

PCIe* may not be functional.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0221

User Response Procedure

Information only; no action is required.

FQXSPFC4000I: The bare metal connection process has been started.

The bare metal connection process has been started.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0143

User Response Procedure

Information only; no action is required.

FQXSPFC4001I: The bare metal update application reports a status of [arg1].

The bare metal update application is reporting a status of [arg1].

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0144

User Response Procedure

Information only; no action is required.

FQXSPFC4002I: System running in setup.

System running in setup.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0193

User Response Procedure

Information only; no action is required.

FQXSPFC4003I: UEFI deployment boot mode is enabled for NextBoot.

UEFI deployment boot mode is enabled for NextBoot.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0197

User Response Procedure

Information only; no action is required.

FQXSPFC4004I: UEFI deployment boot mode is enabled for NextAc.

UEFI deployment boot mode is enabled for NextAC.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0198

User Response Procedure

Information only; no action is required.

FQXSPFC4005I: UEFI deployment boot mode has been disabled.

UEFI deployment boot mode has been disabled.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0199

User Response Procedure

Information only; no action is required.

FQXSPFW0003I: The System [ComputerSystemElementName] encountered firmware progress.

This message is for the use case when an implementation has detected that system firmware progress has occurred.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0188

User Response Procedure

Information only; no action is required.

FQXSPFW2001I: The System [ComputerSystemElementName] has detected a POST Error deassertion.

This message is for the use case when an implementation has detected that Post Error has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0185

User Response Procedure

Information only; no action is required.

FQXSPIO0003N: A diagnostic interrupt has occurred on system [ComputerSystemElementName].

This message is for the use case when an implementation has detected a Front Panel NMI/Diagnostic Interrupt.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: IMM PLAT ID: 0222

User Response Procedure

If the NMI button on the operator information panel has not been pressed, complete the following steps:

1. Reseat the identified compute node.
2. If the problem still exists, replace the compute node.
3. (Trained technician only) Replace the system board. Reseat the identified compute node.
4. If the error still exists, then replace the compute node.

FQXSPIO0004L: A bus timeout has occurred on bus [SensorElementName].

This message is for the use case when an implementation has detected a Bus Timeout.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0224

User Response Procedure

Please reseat the processor and reboot the compute node. If the problem still exists, please replace the identified processor in the compute node.

FQXSPIO0006N: A software NMI has occurred on system [ComputerSystemElementName].

This message is for the use case when an implementation has detected a Software NMI.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0228

User Response Procedure

Check the event log in System Management Module (SMM) to resolve any issues related to the NMI.

FQXSPIO0011N: An Uncorrectable Error has occurred on [SensorElementName].

This message is for the use case when an implementation has detected a Bus Uncorrectable Error.

Severity Error

Serviceable Yes

Automatically Notify Support Yes

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0240

User Response Procedure

1. Make sure that all I/O expansion adapters have correct and matching levels of device drivers and firmware.
2. Check the event log of the System Management Module (SMM) or BMC for additional information about failing components.
3. If there are no entries related to the error in the event log, contact Service.

FQXSPIO2003I: System [ComputerSystemElementName] has recovered from a diagnostic interrupt.

This message is for the use case when an implementation has detected a recovery from a Front Panel NMI/ Diagnostic Interrupt.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: IMM PLAT ID: 0223

User Response Procedure

Information only; no action is required.

FQXSPIO2004I: Bus [SensorElementName] has recovered from a bus timeout.

This message is for the use case that a system has recovered from a Bus Timeout.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: IMM PLAT ID: 0225

User Response Procedure

Information only; no action is required.

FQXSPIO2006I: System [ComputerSystemElementName] has recovered from an NMI.

This message is for the use case when a Software NMI has been detected and recovered.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0230

User Response Procedure

Information only; no action is required.

FQXSPMA0010J: [PhysicalMemoryElementName] on Subsystem [MemoryElementName] Throttled.

This message is for the use case when an implementation has detected Memory has been throttled.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: PLAT CIM ID: 0142

User Response Procedure

Complete the following steps:

1. Check the System Event Log (SEL) of the System Management Module (SMM) and BMC for any fan or cooling-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.
4. Make sure that the DIMM baffles are in place if applicable.
5. If the problem persists and there are no other DIMMs with the same indication, replace the DIMM.

FQXSPMA0012M: An Over-Temperature Condition has been detected on the [PhysicalMemoryElementName] on Subsystem [MemoryElementName].

This message is for the use case when an implementation has detected an Over-Temperature Condition for Memory.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0146

User Response Procedure

Complete the following steps until the problem is solved:

1. Check the event log of the System Management Module (SMM) and BMC for any fan- or cooling-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.
4. Make sure that the DIMM baffles are in place correctly.
5. If the problem remains and no other DIMMs have the same indication, replace the DIMM.

FQXSPMA2005I: The System [ComputerSystemElementName] has detected a POST Error deassertion.

This message is for the use case when an implementation has detected a Post Error has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Memory **SNMP Trap ID: 41**

CIM Prefix: PLAT CIM ID: 0185

User Response Procedure

Information only; no action is required.

FQXSPMA2007I: Scrub Failure for [PhysicalMemoryElementName] on Subsystem [MemoryElementName] has recovered.

This message is for the use case when an implementation has detected a Memory Scrub failure recovery.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Memory **SNMP Trap ID: 41**

CIM Prefix: PLAT CIM ID: 0137

User Response Procedure

Information only; no action is required.

FQXSPMA2010I: [PhysicalMemoryElementName] on Subsystem [MemoryElementName] is no longer Throttled.

This message is for the use case when an implementation has detected Memory is no longer throttled.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0143

User Response Procedure

Information only; no action is required.

FQXSPMA2012I: An Over-Temperature Condition has been removed on the [PhysicalMemoryElementName] on Subsystem [MemoryElementName].

This message is for the use case when an implementation has detected an Over-Temperature Condition for Memory that has been removed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0147

User Response Procedure

Information only; no action is required.

FQXSPMA2013I: The System [ComputerSystemElementName] has detected a POST Error deassertion.

This message is for the use case when an implementation has detected that Post Error has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Memory **SNMP Trap ID: 41**

CIM Prefix: PLAT CIM ID: 0185

User Response Procedure

Information only; no action is required.

FQXSPNM4000I: Management Controller [arg1] Network Initialization Complete.

This message is for the use case where a Management Controller network has completed initialization.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - IMM Network Event **SNMP Trap ID: 37**

CIM Prefix: IMM CIM ID: 0001

User Response Procedure

Information only; no action is required.

FQXSPNM4001I: Ethernet Data Rate modified from [arg1] to [arg2] by user [arg3].

This message is for the use case where a user modifies the Ethernet Port data rate.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0003

User Response Procedure

Information only; no action is required.

FQXSPNM4002I: Ethernet Duplex setting modified from [arg1] to [arg2] by user [arg3].

This message is for the use case where a user modifies the Ethernet Port duplex setting.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0004

User Response Procedure

Information only; no action is required.

FQXSPNM4003I: Ethernet MTU setting modified from [arg1] to [arg2] by user [arg3].

This message is for the use case where a user modifies the Ethernet Port MTU setting.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0005

User Response Procedure

Information only; no action is required.

FQXSPNM4004I: Ethernet locally administered MAC address modified from [arg1] to [arg2] by user [arg3].

This message is for the use case where a user modifies the Ethernet Port MAC address setting.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0006

User Response Procedure

Information only; no action is required.

FQXSPNM4005I: Ethernet interface [arg1] by user [arg2].

This message is for the use case where a user enables or disables the Ethernet interface.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0007

User Response Procedure

Information only; no action is required.

FQXSPNM4006I: Hostname set to [arg1] by user [arg2].

This message is for the use case where user modifies the Hostname of a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category IMM Network Event **SNMP Trap ID: 37**

CIM Prefix: IMM CIM ID: 0008

User Response Procedure

Information only; no action is required.

FQXSPNM4007I: IP address of network interface modified from [arg1] to [arg2] by user [arg3].

This message is for the use case where user modifies the IP address of a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category IMM Network Event **SNMP Trap ID: 37**

CIM Prefix: IMM CIM ID: 0009

User Response Procedure

Information only; no action is required.

FQXSPNM4008I: IP subnet mask of network interface modified from [arg1] to [arg2] by user [arg3].

This message is for the use case where a user modifies the IP subnet mask of a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category IMM Network Event **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0010

User Response Procedure

Information only; no action is required.

FQXSPNM4009I: IP address of default gateway modified from [arg1] to [arg2] by user [arg3].

This message is for the use case where a user modifies the default gateway IP address of a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category IMM Network Event **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0011

User Response Procedure

Information only; no action is required.

FQXSPNM4010I: DHCP[[arg1]] failure, no IP address assigned.

This message is for the use case where a DHCP server fails to assign an IP address to a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0013

User Response Procedure

Complete the following steps until the problem is solved:

1. Make sure that the BMC Controller network cable is connected.
2. Make sure that there is a DHCP server on the network that can assign an IP address to the BMC

FQXSPNM4011I: ENET[[arg1]] DHCP-HSTN=[arg2], DN=[arg3], IP@=[arg4], SN=[arg5], GW@=[arg6], DNS1@=[arg7].

This message is for the use case where a Management Controller IP address and configuration has been assigned by the DHCP server.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0022

User Response Procedure

Information only; no action is required.

FQXSPNM4012I: ENET[[arg1]] IP-Cfg:HstName=[arg2], IP@=[arg3] ,NetMsk=[arg4], GW@=[arg5].

This message is for the use case where a Management Controller IP address and configuration has been assigned statically using user data.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0023

User Response Procedure

Information only; no action is required.

FQXSPNM4013I: LAN: Ethernet[[arg1]] interface is no longer active.

This message is for the use case where a Management Controller Ethernet interface is no longer active.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0024

User Response Procedure

Information only; no action is required.

FQXSPNM4014I: LAN: Ethernet[[arg1]] interface is now active.

This message is for the use case where a Management Controller Ethernet interface is now active.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0025

User Response Procedure

Information only; no action is required.

FQXSPNM4015I: DHCP setting changed to [arg1] by user [arg2].

This message is for the use case where a user changes the DHCP setting.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0026

User Response Procedure

Information only; no action is required.

FQXSPNM4016I: Domain name set to [arg1].

Domain name set by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0043

User Response Procedure

Information only; no action is required.

FQXSPNM4017I: Domain Source changed to [arg1] by user [arg2].

Domain source changed by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0044

User Response Procedure

Information only; no action is required.

FQXSPNM4018I: DDNS setting changed to [arg1] by user [arg2].

DDNS setting changed by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0045

User Response Procedure

Information only; no action is required.

FQXSPNM4019I: DDNS registration successful. The domain name is [arg1].

DDNS registration and values.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0046

User Response Procedure

Information only; no action is required.

FQXSPNM4020I: IPv6 enabled by user [arg1] .

IPv6 protocol is enabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0047

User Response Procedure

Information only; no action is required.

FQXSPNM4021I: IPv6 disabled by user [arg1] .

IPv6 protocol is disabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0048

User Response Procedure

Information only; no action is required.

FQXSPNM4022I: IPv6 static IP configuration enabled by user [arg1].

IPv6 static address assignment method is enabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0049

User Response Procedure

Information only; no action is required.

FQXSPNM4023I: IPv6 DHCP enabled by user [arg1].

IPv6 DHCP assignment method is enabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0050

User Response Procedure

Information only; no action is required.

FQXSPNM4024I: IPv6 stateless auto-configuration enabled by user [arg1].

IPv6 stateless auto-assignment method is enabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0051

User Response Procedure

FQXSPNM4025I: IPv6 static IP configuration disabled by user [arg1].

IPv6 static assignment method is disabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0052

User Response Procedure

Information only; no action is required.

FQXSPNM4026I: IPv6 DHCP disabled by user [arg1].

IPv6 DHCP assignment method is disabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0053

User Response Procedure

Information only; no action is required.

FQXSPNM4027I: IPv6 stateless auto-configuration disabled by user [arg1].

IPv6 stateless auto-assignment method is disabled by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0054

User Response Procedure

Information only; no action is required.

FQXSPNM4028I: ENET[[arg1]] IPv6-LinkLocal:HstName=[arg2], IP@=[arg3] ,Pref=[arg4] .

IPv6 Link Local address is active.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0055

User Response Procedure

Information only; no action is required.

FQXSPNM4029I: ENET[[arg1]] IPv6-Static:HstName=[arg2], IP@=[arg3] ,Pref=[arg4], GW@=[arg5] .

IPv6 Static address is active.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0056

User Response Procedure

Information only; no action is required.

FQXSPNM4030I: ENET[[arg1]] DHCPv6-HSTN=[arg2], DN=[arg3], IP@=[arg4], Pref=[arg5], DNS1@= [arg5].

IPv6 DHCP-assigned address is active.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0057

User Response Procedure

Information only; no action is required.

FQXSPNM4031I: IPv6 static address of network interface modified from [arg1] to [arg2] by user [arg3].

A user modifies the IPv6 static address of a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0058

User Response Procedure

Information only; no action is required.

FQXSPNM4032I: DHCPv6 failure, no IP address assigned.

A DHCP6 server fails to assign an IP address to a Management Controller.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0059

User Response Procedure

Please ensure DHCP server is working.

FQXSPNM4033I: Telnet port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the Telnet port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0061

User Response Procedure

Information only; no action is required.

FQXSPNM4034I: SSH port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the SSH port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0062

User Response Procedure

Information only; no action is required.

FQXSPNM4035I: Web-HTTP port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the Web HTTP port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0063

User Response Procedure

Information only; no action is required.

FQXSPNM4036I: Web-HTTPS port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the Web HTTPS port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0064

User Response Procedure

Information only; no action is required.

FQXSPNM4037I: CIM/XML HTTP port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the CIM\XML HTTP port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0065

User Response Procedure

Information only; no action is required.

FQXSPNM4038I: CIM/XML HTTPS port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the CIM/XML HTTPS port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0066

User Response Procedure

Information only; no action is required.

FQXSPNM4039I: SNMP Agent port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the SNMP Agent port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0067

User Response Procedure

Information only; no action is required.

FQXSPNM4040I: SNMP Traps port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the SNMP Traps port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0068

User Response Procedure

Information only; no action is required.

FQXSPNM4041I: Syslog port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the Syslog receiver port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0069

User Response Procedure

Information only; no action is required.

FQXSPNM4042I: Remote Presence port number changed from [arg1] to [arg2] by user [arg3].

A user has modified the Remote Presence port number.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0070

User Response Procedure

Information only; no action is required.

FQXSPNM4043I: SMTP Server set by user [arg1] to [arg2]:[arg3].

A user configured the SMTP server.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0086

User Response Procedure

Information only; no action is required.

FQXSPNM4044I: Telnet [arg1] by user [arg2].

A user enables or disables Telnet services.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0087

User Response Procedure

Information only; no action is required.

FQXSPNM4045I: DNS servers set by user [arg1]: UseAdditionalServers=[arg2], PreferredDNStype= [arg3], IPv4Server1=[arg4], IPv4Server2=[arg5], IPv4Server3=[arg6], IPv6Server1=[arg7], IPv6Server2=[arg8], IPv6Server3=[arg9].

A user configures the DNS servers.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0088

User Response Procedure

Information only; no action is required.

FQXSPNM4046I: LAN over USB [arg1] by user [arg2].

A user configured USB-LAN.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0089

User Response Procedure

Information only; no action is required.

FQXSPNM4047I: LAN over USB Port Forwarding set by user [arg1]: ExternalPort=[arg2], USB-LAN port=[arg3].

A user configured USB-LAN port forwarding.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0090

User Response Procedure

Information only; no action is required.

FQXSPNM4048I: PXE boot requested by user [arg1].

User requested PXE boot.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0129

User Response Procedure

Information only; no action is required.

FQXSPNM4049I: User [arg1] has initiated a TKLM Server Connection Test to check connectivity to server [arg2].

User initiated a TKLM Server Connection test.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0159

User Response Procedure

Information only; no action is required.

FQXSPNM4050I: User [arg1] has initiated an SMTP Server Connection Test.

User initiated an SMTP Server Connection test.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0160

User Response Procedure

Information only; no action is required.

FQXSPNM4051I: User [arg1] has set the SMTP Server reverse-path to [arg2].

User set SMTP Server reverse-path address.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0163

User Response Procedure

Information only; no action is required.

FQXSPNM4052I: DHCP-specified hostname is set to [arg1] by user [arg2].

DHCP-specified hostname is set by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0216

User Response Procedure

Information only; no action is required.

FQXSPOS4000I: OS Watchdog response [arg1] by [arg2] .

This message is for the use case where an OS Watchdog has been enabled or disabled by a user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0012

User Response Procedure

Information only; no action is required.

FQXSPOS4001I: Watchdog [arg1] Screen Capture Occurred.

This message is for the use case where an operating system error has occurred and the screen was captured.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0028

User Response Procedure

If there was no operating system error that caused the screen capture, complete the following steps until the problem is resolved:

1. Reconfigure the Watchdog timer to a higher value.
2. Make sure that the IMM Ethernet-over-USB interface is enabled.
3. Reinstall the RNDIS or cdc_ether device driver for the operating system.
4. Disable the Watchdog.
5. If there was an operating system error that caused the screen capture, check the integrity of the installed operating system.

FQXSPOS4002I: Watchdog [arg1] Failed to Capture Screen.

This message is for the use case where an operating system error has occurred and the screen capture failed.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0029

User Response Procedure

Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before updating the code.

Complete the following steps until the problem is solved:

1. Reconfigure the Watchdog timer to a higher value.
2. Make sure that the BMC Controller Ethernet over USB interface is enabled.
3. Reinstall the RNDIS or cdc_ether device driver for the operating system.
4. Disable the Watchdog.
5. Check the integrity of the installed BMC Controller firmware.

FQXSPOS4003I: Platform Watchdog Timer expired for [arg1].

An implementation has detected an OS Loader Watchdog Timer Expired.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Loader Timeout **SNMP Trap ID: 26**

CIM Prefix: IMM CIM ID: 0060

User Response Procedure

Complete the following steps until the problem is solved:

1. Reconfigure the Watchdog timer to a higher value.
2. Make sure that the BMC Controller Ethernet-over-USB interface isenabled.
3. Reinstall the RNDIS or cdc_ether device driver for the operating system.
4. Disable the Watchdog.
5. Check the integrity of the installed operating system.

FQXSPOS4004I: Operating System status has changed to [arg1].

Operating System status change.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0191

User Response Procedure

Information only; no action is required.

FQXSPPP4000I: Attempting to [arg1] server [arg2] by user [arg3].

This message is for the use case where a user is using the Management Controller to perform a power function on the system.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0015

User Response Procedure

Information only; no action is required.

FQXSPPP4001I: Server Power Off Delay set to [arg1] by user [arg2].

A user configured the Server Power Off Delay.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0081

User Response Procedure

Information only; no action is required.

FQXSPPP4002I: Server [arg1] scheduled for [arg2] at [arg3] by user [arg4].

A user configured a Server Power action at a specific time.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0082

User Response Procedure

Information only; no action is required.

FQXSPPP4003I: Server [arg1] scheduled for every [arg2] at [arg3] by user [arg4].

A user configured a recurring Server Power Action.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0083

User Response Procedure

Information only; no action is required.

FQXSPPP4004I: Server [arg1] [arg2] cleared by user [arg3].

A user cleared a Server Power Action.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0084

User Response Procedure

Information only; no action is required.

FQXSPPP4005I: The power cap value changed from [arg1] watts to [arg2] watts by user [arg3].

Power Cap values changed by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0113

User Response Procedure

Information only; no action is required.

FQXSPPP4006I: The minimum power cap value changed from [arg1] watts to [arg2] watts.

Minimum Power Cap value changed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0114

User Response Procedure

Information only; no action is required.

FQXSPPP4007I: The maximum power cap value changed from [arg1] watts to [arg2] watts.

Maximum Power Cap value changed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0115

User Response Procedure

Information only; no action is required.

FQXSPPP4008I: The soft minimum power cap value changed from [arg1] watts to [arg2] watts.

Soft Minimum Power Cap value changed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0115

User Response Procedure

Information only; no action is required.

FQXSPPP4009I: The measured power value exceeded the power cap value.

Power exceeded cap.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: IMM CIM ID: 0117

User Response Procedure

Information only; no action is required.

FQXSPPP4010I: The new minimum power cap value exceeded the power cap value.

Minimum Power Cap exceeds Power Cap.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: IMM CIM ID: 0118

User Response Procedure

Information only; no action is required.

FQXSPPP4011I: Power capping was activated by user [arg1].

Power capping activated by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0119

User Response Procedure

Information only; no action is required.

FQXSPPP4012I: Power capping was deactivated by user [arg1].

Power capping deactivated by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0120

User Response Procedure

Information only; no action is required.

FQXSPPP4013I: Static Power Savings mode has been turned on by user [arg1].

Static Power Savings mode turned on by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0121

User Response Procedure

Information only; no action is required.

FQXSPPP4014I: Static Power Savings mode has been turned off by user [arg1].

Static Power Savings mode turned off by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0122

User Response Procedure

Information only; no action is required.

FQXSPPP4015I: Dynamic Power Savings mode has been turned on by user [arg1].

Dynamic Power Savings mode turned on by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0123

User Response Procedure

Information only; no action is required.

FQXSPPP4016I: Dynamic Power Savings mode has been turned off by user [arg1].

Dynamic Power Savings mode turned off by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0124

User Response Procedure

Information only; no action is required.

FQXSPPP4017I: Power cap and external throttling occurred.

Power cap and external throttling occurred.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0125

User Response Procedure

Information only; no action is required.

FQXSPPP4018I: External throttling occurred.

External throttling occurred.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0126

User Response Procedure

Information only; no action is required.

FQXSPPP4019I: Power cap throttling occurred.

Power cap throttling occurred.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0127

User Response Procedure

Information only; no action is required.

FQXSPPP4020I: The measured power value has returned below the power cap value.

Power exceeded cap recovered.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: IMM CIM ID: 0130

User Response Procedure

Information only; no action is required.

FQXSPPP4021I: The new minimum power cap value has returned below the power cap value.

Minimum Power Cap exceeds Power Cap recovered.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: IMM CIM ID: 0131

User Response Procedure

Information only; no action is required.

FQXSPPP4022I: The server was restarted for an unknown reason.

The server was restarted for an unknown reason.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0166

User Response Procedure

Information only; no action is required.

FQXSPPP4023I: The server is restarted by chassis control command.

Server is restarted by chassis control command.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0167

User Response Procedure

Information only; no action is required.

FQXSPPP4024I: The server was reset via pushbutton.

Server was reset via pushbutton.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0168

User Response Procedure

Information only; no action is required.

FQXSPPP4025I: The server was powered-up via power pushbutton.

Server was powered-up via power pushbutton.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0169

User Response Procedure

Information only; no action is required.

FQXSPPP4026I: The server was restarted when the Watchdog expired.

Server was restarted when the Watchdog expired.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0170

User Response Procedure

Information only; no action is required.

FQXSPPP4027I: The server was restarted for OEM reason.

Server was restarted for OEM reason.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0171

User Response Procedure

Information only; no action is required.

FQXSPPP4028I: The server was automatically powered on because the power restore policy is set to always restore.

Server was automatically powered on because the power restore policy is set to “always restore.”

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0172

User Response Procedure

Information only; no action is required.

FQXSPPP4029I: The server was automatically powered on because the power restore policy is set to restore previous power state.

Server was automatically powered on because the power restore policy is set to restore previous power state.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0173

User Response Procedure

Information only; no action is required.

FQXSPPP4030I: The server was reset via Platform Event Filter.

Server was reset via Platform Event Filter.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0174

User Response Procedure

Information only; no action is required.

FQXSPPP4031I: The server was power-cycled via Platform Event Filter.

Server was power-cycled via Platform Event Filter.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0175

User Response Procedure

Information only; no action is required.

FQXSPPP4032I: The server was soft reset.

Server was soft reset.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0176

User Response Procedure

Information only; no action is required.

FQXSPPP4033I: The server was powered up via Real Time Clock (scheduled power on).

Server was powered up via Real Time Clock (scheduled power on).

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0177

User Response Procedure

Information only; no action is required.

FQXSPPP4034I: The server was powered off for an unknown reason.

Server was powered off for an unknown reason.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0177

User Response Procedure

Information only; no action is required.

FQXSPPP4035I: The server was powered off by chassis control command.

Server was powered off by chassis control command.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0179

User Response Procedure

Information only; no action is required.

FQXSPPP4036I: The server was powered off via pushbutton.

Server was powered off via pushbutton.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0180

User Response Procedure

Information only; no action is required.

FQXSPPP4037I: The server was powered off when the Watchdog expired.

Server was powered off when the Watchdog expired.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0181

User Response Procedure

Information only; no action is required.

FQXSPPP4038I: The server stayed powered off because the power restore policy is set to always restore.

Server stayed powered off because the power restore policy is set to “always restore.”

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0182

User Response Procedure

Information only; no action is required.

FQXSPPP4039I: The server stayed powered off because the power restore policy is set to restore previous power state.

Server stayed powered off because the power restore policy is set to restore previous power state.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0183

User Response Procedure

Information only; no action is required.

FQXSPPP4040I: The server was powered off via Platform Event Filter.

Server was powered off via Platform Event Filter.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0184

User Response Procedure

Information only; no action is required.

FQXSPPP4041I: The server was powered off via Real Time Clock (scheduled power off).

Server was powered off via Real Time Clock (scheduled power off).

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0185

User Response Procedure

Information only; no action is required.

FQXSPPP4042I: Management Controller [arg1] reset was initiated due to Power-On Reset.

Management Controller reset was initiated due to Power-On Reset.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0186

User Response Procedure

Information only; no action is required.

FQXSPPP4043I: Management Controller [arg1] reset was initiated by PRESET.

Management Controller reset was initiated by PRESET.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0187

User Response Procedure

Information only; no action is required.

FQXSPPP4044I: Management Controller [arg1] reset was initiated by CMM.

Management Controller reset was initiated by CMM.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0187

User Response Procedure

Information only; no action is required.

FQXSPPP4045I: Management Controller [arg1] reset was initiated by BMC CONTROLLER firmware.

Management Controller reset was initiated by BMC Controller firmware.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0188

User Response Procedure

Information only; no action is required.

FQXSPPP4046I: Remote power permission is [arg1].

Remote power permission status change.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0200

User Response Procedure

Information only; no action is required.

FQXSPPP4047I: Management Controller [arg1] reset was initiated by user [arg2].

This message is for the use case where a Management Controller reset is initiated by a user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0021

User Response Procedure

Information only; no action is required.

FQXSPPP4048I: Attempting to AC power cycle server [arg1] by user [arg2].

AC power cycle server.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0227

User Response Procedure

Information only; no action is required.

FQXSPPR0000I: [ManagedElementName] detected as present.

This message is for the use case when an implementation has detected a Managed Element is now present.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0390

User Response Procedure

Information only; no action is required.

FQXSPPR2001I: [ManagedElementName] detected as absent.

This message is for the use case when an implementation has detected a Managed Element is absent.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0392

User Response Procedure

Information only; no action is required.

FQXSPPU0001N: An Over-Temperature Condition has been detected on [ProcessorElementName].

This message is for the use case when an implementation has detected an Over-Temperature Condition detected for processor.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0036

User Response Procedure

Complete the following steps until the problem is solved:

1. Check the System Event Log (SEL) of the System Management Module (SMM) and BMC Controller for any fan or cooling-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within operating specifications.
4. Make sure that the microprocessor 1 heatsink is securely installed.
5. Make sure that the microprocessor 1 heatsink is installed correctly and the thermal material is correctly applied.
6. (Trained technician only) Replace microprocessor 1.

FQXSPPU0002G: The Processor [ProcessorElementName] is operating in a Degraded State.

This message is for the use case when an implementation has detected a Processor is running in the Degraded state.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - CPU **SNMP Trap ID: 42**

CIM Prefix: PLAT CIM ID: 0038

User Response Procedure

Complete the following steps until the problem is solved:

1. Check the System Event Log (SEL) of the System Management Module (SMM) and BMC Controller for any fan- or cooling-related issues or power-related issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.

FQXSPPU2001I: An Over-Temperature Condition has been removed on [ProcessorElementName].

This message is for the use case when an implementation has detected a Over-Temperature Condition has been removed for Processor.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 0**

CIM Prefix: PLAT CIM ID: 0037

User Response Procedure

Information only; no action is required.

FQXSPPU2002I: The Processor [ProcessorElementName] is no longer operating in a Degraded State.

This message is for the use case when an implementation has detected a Processor is no longer running in the Degraded state.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Temperature **SNMP Trap ID: 42**

CIM Prefix: PLAT CIM ID: 0039

User Response Procedure

Information only; no action is required.

FQXSPPW0001I: [PowerSupplyElementName] has been added to container [PhysicalPackageElementName].

This message is for the use case when an implementation has detected a Power Supply has been added.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0084

User Response Procedure

Information only; no action is required.

FQXSPPW0002L: [PowerSupplyElementName] has Failed.

This message is for the use case when an implementation has detected a Power Supply has failed.

Severity Error

Serviceable Yes

Automatically Notify Support Yes

Alert Category Critical - Power **SNMP Trap ID: 4**

CIM Prefix: PLAT CIM ID: 0086

User Response Procedure

Please check the System Event Log (SEL) in the System Management Module (SMM) to identify the power supply unit (PSU) failure.

FQXSPPW0003G: Failure predicted on [PowerSupplyElementName].

This message is for the use case when an implementation has detected a Power Supply failure is predicted.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: PLAT CIM ID: 0088

User Response Procedure

Please check the System Event Log (SEL) in the System Management Module (SMM) web interface to identify the predicted failure.

FQXSPPW0005I: [PowerSupplyElementName] is operating in an Input State that is out of range.

This message is for the use case when an implementation has detected a Power Supply that has input out of range.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0098

User Response Procedure

Informational only; no action required.

FQXSPPW0006I: [PowerSupplyElementName] has lost input.

This message is for the use case when an implementation has detected a Power Supply that has input that has been lost.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0100

User Response Procedure

Make sure power cables are connected correctly.

FQXSPPW0007L: [PowerSupplyElementName] has a Configuration Mismatch.

This message is for the use case when an implementation has detected a Power Supply with a configuration error.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Power **SNMP Trap ID: 4**

CIM Prefix: PLAT CIM ID: 0104

User Response Procedure

Check the System Event Log (SEL) in the System Management Module (SMM).

FQXSPPW0008I: [PowerSupplyElementName] has been turned off.

This message is for the use case when an implementation has detected a Power Unit that has been Disabled.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Power Off **SNMP Trap ID: 23**

CIM Prefix: PLAT CIM ID: 0106

User Response Procedure

Informational only; no action required.

FQXSPPW0009I: [PowerSupplyElementName] has been Power Cycled.

This message is for the use case when an implementation has detected a Power Unit that has been power cycled.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0108

User Response Procedure

Informational only; no action required.

FQXSPPW0031J: Numeric sensor [NumericSensorElementName] going low (lower non-critical) has asserted.

This message is for the use case when an implementation has detected a Lower Non-critical sensor going low has asserted.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - Voltage **SNMP Trap ID: 13**

CIM Prefix: PLAT CIM ID: 0476

User Response Procedure

CMOS battery is recommended to replace with new one.

FQXSPPW0035M: Numeric sensor [NumericSensorElementName] going low (lower critical) has asserted.

This message is for the use case when an implementation has detected a Lower Critical sensor going low has asserted.

Severity Error

Serviceable Yes

Automatically Notify Support Yes

Alert Category Critical - Voltage **SNMP Trap ID: 1**

CIM Prefix: PLAT CIM ID: 0480

User Response Procedure

Use one of the following procedures:

1. If the specified sensor is Planar 3.3V or Planar 5V (trained technician only), replace the system board.
2. If the specified sensor is Planar 12V, check the System Management Module or BMC Controller event log for power-supply-related issues, and resolve those issues.
3. (Trained technician only) If the problem remains, replace the system board.

FQXSPPW0047M: Numeric sensor [NumericSensorElementName] going high (upper critical) has asserted.

This message is for the use case when an implementation has detected a Upper Critical sensor going high has asserted.

Severity Error

Serviceable Yes

Automatically Notify Support Yes

Alert Category Critical - Voltage **SNMP Trap ID: 1**

CIM Prefix: PLAT CIM ID: 0494

User Response Procedure

Use one of the following procedures:

1. (Trained technician only) If the specified sensor is Planar 3.3V or Planar 5V, replace the system board.
2. If the specified sensor is Planar 12V, check the System Management Module or BMC Controller event log for power-supply-related issues, and resolve those issues.
3. (Trained technician only) If the problem remains, replace the system board.

FQXSPPW0057J: Sensor [SensorElementName] has transitioned from normal to non-critical state.

This message is for the use case when an implementation has detected a Sensor transitioned to non-critical from normal.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: PLAT CIM ID: 0520

User Response Procedure

Please check the System Event Log (SEL) in the System Management Module (SMM) web interface.

FQXSPPW0061M: Sensor [SensorElementName] has transitioned to critical from a less severe state.

This message is for the use case when an implementation has detected a Sensor transitioned to critical from less severe.

Severity Warning

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 4**

CIM Prefix: PLAT CIM ID: 0522

User Response Procedure

Complete the following steps:

1. Ensure the Power Supply Unit (PSU) meets the system specification in wattage, efficiency level, and supported list.
2. Check the System Event Log (SEL) in the System Management Module (SMM) for detail information.

FQXSPPW0063M: Sensor [SensorElementName] has transitioned to critical from a less severe state.

This message is for the use case when an implementation has detected a Sensor transitioned to critical from less severe.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Voltage **SNMP Trap ID: 1**

CIM Prefix: PLAT CIM ID: 0522

User Response Procedure

Reseat the faulty node in D2 enclosure (AC cycle) through these steps:

1. Reseat the faulty node in D2 enclosure (AC cycle).
2. Check if multiple nodes within the D2 enclosure are reporting SysBrd Vol fault:
    a. If the fault is reported by single node, swap the failing node with a good node.
    b. If fault follows the node, replace the system board in the compute node (trained technician only).
    c. If the fault follows the slot within the D2 enclosure, replace the shuttle (trained technician only).
3. If multi-node failure in a chassis, AC cycle entire chassis by disconnecting the power cords and plugging them back into the system again.
    d. If the problem persists, repeat steps 2 a-c.

FQXSPPW2001I: [PowerSupplyElementName] has been removed from container [PhysicalPackageElementName].

This message is for the use case when an implementation has detected a Power Supply has been removed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0085

User Response Procedure

Information only; no action is required.

FQXSPPW2002I: [PowerSupplyElementName] has returned to OK status.

This message is for the use case when an implementation has detected a Power Supply return to normal operational status.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Power **SNMP Trap ID: 4**

CIM Prefix: PLAT CIM ID: 0087

User Response Procedure

Information only; no action is required.

FQXSPPW2003I: Failure no longer predicted on [PowerSupplyElementName].

This message is for the use case when an implementation has detected a Power Supply is no longer predicted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: PLAT CIM ID: 0089

User Response Procedure

Information only; no action is required.

FQXSPPW2005I: [PowerSupplyElementName] has returned to a Normal Input State.

This message is for the use case when an implementation has detected a Power Supply that has input that has returned to normal.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: PLAT CIM ID: 0099

User Response Procedure

Information only; no action is required.

FQXSPPW2006I: [PowerSupplyElementName] has returned to a Normal Input State.

This message is for the use case when an implementation has detected a Power Supply that has input that has returned to normal.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0099

User Response Procedure

Information only; no action is required.

FQXSPPW2007I: [PowerSupplyElementName] Configuration is OK.

This message is for the use case when an implementation has detected a Power Supply configuration is OK. has returned to normal.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Power **SNMP Trap ID: 4**

CIM Prefix: PLAT CIM ID: 0105

User Response Procedure

Information only; no action is required.

FQXSPPW2008I: [PowerSupplyElementName] has been turned on.

This message is for the use case when an implementation has detected a Power Unit that has been enabled.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Power On **SNMP Trap ID: 24**

CIM Prefix: PLAT CIM ID: 0107

User Response Procedure

Information only; no action is required.

FQXSPPW2031I: Numeric sensor [NumericSensorElementName] going low (lower non-critical) has deasserted.

This message is for the use case when an implementation has detected a Lower Non-critical sensor going low has deasserted.

Severity Error

Serviceable Yes

Automatically Notify Support Yes

Alert Category Warning - Voltage **SNMP Trap ID: 13**

CIM Prefix: PLAT CIM ID: 0477

User Response Procedure

Information only; no action is required.

FQXSPPW2035I: Numeric sensor [NumericSensorElementName] going low (lower critical) has deasserted.

This message is for the use case when an implementation has detected a Lower Non-critical sensor going low has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Voltage **SNMP Trap ID: 1**

CIM Prefix: PLAT CIM ID: 0481

User Response Procedure

Information only; no action is required.

FQXSPPW2047I: Numeric sensor [NumericSensorElementName] going high (upper critical) has deasserted.

This message is for the use case when an implementation has detected a Upper Critical sensor going high has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Voltage **SNMP Trap ID: 1**

CIM Prefix: PLAT CIM ID: 0495

User Response Procedure

Information only; no action is required.

FQXSPPW2057I: Sensor [SensorElementName] has deasserted the transition from normal to non-critical state.

This message is for the use case when an implementation has detected that a sensor has deasserted a transition to non-critical from normal.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Power **SNMP Trap ID: 164**

CIM Prefix: PLAT CIM ID: 0521

User Response Procedure

Information only; no action is required.

FQXSPPW2061I: Sensor [SensorElementName] has transitioned to a less severe state from critical.

This message is for the use case when an implementation has detected a Sensor transition to less severe from critical.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Power **SNMP Trap ID: 4**

CIM Prefix: PLAT CIM ID: 0523

User Response Procedure

Information only; no action is required.

FQXSPPW2063I: Sensor [SensorElementName] has transitioned to a less severe state from critical.

This message is for the use case when an implementation has detected a Sensor transition to less severe from critical.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Voltage **SNMP Trap ID: 1**

CIM Prefix: PLAT CIM ID: 0523

User Response Procedure

Information only; no action is required.

FQXSPSD0003I: Hot Spare enabled for [ComputerSystemElementName].

This message is for the use case when an implementation has detected a Hot Spare has been enabled.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0170

User Response Procedure

Information only; no action is required.

FQXSPSD0005L: Array [ComputerSystemElementName] is in critical condition.

This message is for the use case when an implementation has detected that an Array is Critical.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Hard Disk Drive **SNMP Trap ID: 5**

CIM Prefix: PLAT CIM ID: 0174

User Response Procedure

Replace the hard disk drive that is indicated by a lit status LED.

FQXSPSD0006L: Array [ComputerSystemElementName] has failed.

This message is for the use case when an implementation has detected that an Array Failed.

Severity Error

Serviceable Yes

Automatically Notify Support Yes

Alert Category Critical - Hard Disk Drive **SNMP Trap ID: 5**

CIM Prefix: PLAT CIM ID: 0176

User Response Procedure

Complete the following steps:

1. Replace any hard disk drive that is indicated by a lit status LED.
2. Re-create the array.
3. Restore the data from a backup.

FQXSPSD0007I: Rebuild in progress for Array in system [ComputerSystemElementName].

This message is for the use case when an implementation has detected that an Array Rebuild is in progress.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 0178**

CIM Prefix: PLAT CIM ID: 0178

User Response Procedure

Information only; no action is required.

FQXSPSD2003I: Hot spare disabled for [ComputerSystemElementName].

This message is for the use case when an implementation has detected a Hot Spare has been disabled.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0171

User Response Procedure

Information only; no action is required.

FQXSPSD2005I: Critical Array [ComputerSystemElementName] has deasserted.

This message is for the use case when an implementation has detected that a Critical Array has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Hard Disk Drive **SNMP Trap ID: 5**

CIM Prefix: PLAT CIM ID: 0175

User Response Procedure

Information only; no action is required.

FQXSPSD2006I: Array in system [ComputerSystemElementName] has been restored.

This message is for the use case when an implementation has detected that a Failed Array has been restored.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Hard Disk Drive **SNMP Trap ID: 5**

CIM Prefix: PLAT CIM ID: 0177

User Response Procedure

Information only; no action is required.

FQXSPSD2007I: Rebuild completed for Array in system [ComputerSystemElementName].

This message is for the use case when an implementation has detected that an Array Rebuild has completed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0179

User Response Procedure

Information only; no action is required.

FQXSPSE4000I: Certificate Authority [arg1] has detected a [arg2] Certificate Error.

This message is for the use case when there is an error with an SSL Server, SSL Client, or SSL Trusted CA Certificate.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0002

User Response Procedure

Make sure that the certificate being imported is correct and properly generated.

FQXSPSE4001I: Remote Login Successful. Login ID: [arg1] from [arg2] at IP address [arg3].

This message is for the use case where a user successfully logs in to a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0014

User Response Procedure

Information only; no action is required.

FQXSPSE4002I: Security: Userid: [arg1] had [arg2] login failures from WEB client at IP address [arg3].

This message is for the use case where a user has failed to log in to a Management Controller from a web browser.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0016

User Response Procedure

Complete the following steps until the problem is solved:

1. Make sure that the correct login ID and password are being used.
2. Have the system administrator reset the login ID or password.

FQXSPSE4003I: Security: Login ID: [arg1] had [arg2] login failures from CLI at [arg3].

This message is for the use case where a user has failed to log in to a Management Controller from the Legacy CLI.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0017

User Response Procedure

Complete the following steps until the problem is solved:

1. Make sure that the correct login ID and password are being used.
2. Have the system administrator reset the login ID or password.

FQXSPSE4004I: Remote access attempt failed. Invalid userid or password received. Userid is [arg1] from WEB browser at IP address [arg2].

This message is for the use case where a remote user has failed to establish a remote control session from a web browser session.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0018

User Response Procedure

Make sure that the correct login ID and password are being used.

FQXSPSE4005I: Remote access attempt failed. Invalid userid or password received. Userid is [arg1] from TELNET client at IP address [arg2].

This message is for the use case where a user has failed to log in to a Management Controller from a Telnet session.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0019

User Response Procedure

Make sure that the correct login ID and password are being used.

FQXSPSE4007I: Security: Userid: [arg1] had [arg2] login failures from an SSH client at IP address [arg3].

This message is for the use case where a user has failed to log in to a Management Controller from SSH.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0041

User Response Procedure

Complete the following steps until the problem is solved:

1. Make sure that the correct login ID and password are being used.
2. Have the system administrator reset the login ID or password.

FQXSPSE4008I: SNMPv1 [arg1] set by user [arg2]: Name=[arg3], AccessType=[arg4], Address=[arg5], .

A user changed the SNMP community string.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0075

User Response Procedure

Information only; no action is required.

FQXSPSE4009I: LDAP Server configuration set by user [arg1]: SelectionMethod=[arg2], DomainName=[arg3], Server1=[arg4], Server2=[arg5], Server3=[arg6], Server4=[arg7].

A user changed the LDAP server configuration.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0076

User Response Procedure

Information only; no action is required.

FQXSPSE4010I: LDAP set by user [arg1]: RootDN=[arg2], UIDSearchAttribute=[arg3], BindingMethod=[arg4], EnhancedRBS=[arg5], TargetName=[arg6], GroupFilter=[arg7], GroupAttribute=[arg8], LoginAttribute=[arg9].

A user configured an LDAP Miscellaneous setting.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0077

User Response Procedure

Information only; no action is required.

FQXSPSE4011I: Secure Web services (HTTPS) [arg1] by user [arg2].

A user enables or disables Secure Web services.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0091

User Response Procedure

Information only; no action is required.

FQXSPSE4012I: Secure CIM/XML(HTTPS) [arg1] by user [arg2].

A user enables or disables Secure CIM/XML Web services.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0092

User Response Procedure

Information only; no action is required.

FQXSPSE4013I: Secure LDAP [arg1] by user [arg2].

A user enables or disables Secure LDAP Web services.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0093

User Response Procedure

Information only; no action is required.

FQXSPSE4014I: SSH [arg1] by user [arg2].

A user enables or disables SSH services.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0094

User Response Procedure

Information only; no action is required.

FQXSPSE4015I: Global Login General Settings set by user [arg1]: AuthenticationMethod=[arg2], LockoutPeriod=[arg3], SessionTimeout=[arg4].

A user changes the Global Login General Settings.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0098

User Response Procedure

Information only; no action is required.

FQXSPSE4016I: Global Login Account Security set by user [arg1]: PasswordRequired=[arg2], PasswordExpirationPeriod=[arg3], MinimumPasswordReuseCycle=[arg4], MinimumPasswordLength=[arg5], MinimumPasswordChangeInterval=[arg6], MaxmumLoginFailures=[arg7], LockoutAfterMaxFailures=[arg8].

A user changes the Global Login General Settings to Legacy.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0098

User Response Procedure

Information only; no action is required.

FQXSPSE4017I: User [arg1] created.

A user account was created.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0100

User Response Procedure

Information only; no action is required.

FQXSPSE4018I: User [arg1] removed.

A user account was deleted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0101

User Response Procedure

Information only; no action is required.

FQXSPSE4019I: User [arg1] password modified.

A user account was changed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0102

User Response Procedure

Information only; no action is required.

FQXSPSE4020I: User [arg1] role set to [arg2].

A user account was assigned.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0103

User Response Procedure

Information only; no action is required.

FQXSPSE4021I: User [arg1] custom privileges set: [arg2][arg3][arg4][arg5][arg6][arg7][arg8].

User account privileges were assigned.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0104

User Response Procedure

Information only; no action is required.

FQXSPSE4022I: User [arg1] for SNMPv3 set: AuthenticationProtocol=[arg2], PrivacyProtocol=[arg3], AccessType=[arg4], HostforTraps=[arg5].

User account SNMPv3 settings changed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0105

User Response Procedure

Information only; no action is required.

FQXSPSE4023I: SSH Client key added for user [arg1].

User locally defined an SSH Client key.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0106

User Response Procedure

Information only; no action is required.

FQXSPSE4024I: SSH Client key imported for user [arg1] from [arg2].

User imported an SSH Client key.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0107

User Response Procedure

Information only; no action is required.

FQXSPSE4025I: SSH Client key removed from user [arg1].

User removed an SSH Client key.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0108

User Response Procedure

Information only; no action is required.

FQXSPSE4026I: Security: Userid: [arg1] had [arg2] login failures from a CIM client at IP address [arg3].

This message is for the use case where a user has failed to log in to a Management Controller from CIM.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0140

User Response Procedure

Information only; no action is required.

FQXSPSE4027I: Remote access attempt failed. Invalid userid or password received. Userid is [arg1] from a CIM client at IP address [arg2].

This message is for the use case where a remote user has failed to establish a remote control session from CIM.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0141

User Response Procedure

Information only; no action is required.

FQXSPSE4028I: Security: Userid: [arg1] had [arg2] login failures from IPMI client at IP address [arg3].

This message is for the use case where a remote user has failed to establish a remote control session from IPMI.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0153

User Response Procedure

Information only; no action is required.

FQXSPSE4029I: Security: Userid: [arg1] had [arg2] login failures from SNMP client at IP address [arg3].

This message is for the use case where a remote user has failed to access a Management Controller from SNMP.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0154

User Response Procedure

Information only; no action is required.

FQXSPSE4030I: Security: Userid: [arg1] had [arg2] login failures from IPMI serial client.

This message is for the use case where a user has failed to log into a Management Controller from IPMI serial client.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0155

User Response Procedure

Information only; no action is required.

FQXSPSE4031I: Remote Login Successful. Login ID: [arg1] from [arg2] serial interface.

This message is for the use case where a user successfully logs into a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0156

User Response Procedure

Information only; no action is required.

FQXSPSE4032I: Login ID: [arg1] from [arg2] at IP address [arg3] has logged off.

This message is for the use case where a user has logged off a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0157

User Response Procedure

Information only; no action is required.

FQXSPSE4033I: Login ID: [arg1] from [arg2] at IP address [arg3] has been logged off.

This message is for the use case where a user has logged off a Management Controller.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0158

User Response Procedure

Information only; no action is required.

FQXSPSE4034I: User [arg1] has removed a certificate.

User removed certificate.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0164

User Response Procedure

Information only; no action is required.

FQXSPSE4035I: A certificate has been revoked.

A certificate has been revoked.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0165

User Response Procedure

Information only; no action is required.

FQXSPSE4036I: The [arg1] certificate is expired and has been removed.

Expired certificate has been removed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0190

User Response Procedure

Information only; no action is required.

FQXSPSE4037I: Crypto mode modified from [arg1] to [arg2] by user [arg3].

Crypto mode is modified.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0218

User Response Procedure

Information only; no action is required.

FQXSPSE4038I: Minimum TLS level modified from [arg1] to [arg2] by user [arg3].

Minimum TLS level is modified.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0219

User Response Procedure

Information only; no action is required.

FQXSPSE4039I: Temporary user account [arg1] is created by inband tool.

Temporary user account created.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0228

User Response Procedure

One user account is created.

FQXSPSE4040I: Temporary user account [arg1] expires.

Temporary user account expires.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0229

User Response Procedure

The user account created is expired.

FQXSPSS4000I: Management Controller Test Alert Generated by [arg1].

This message is for the use case where a user has generated a Test Alert.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System – Remote Login **SNMP Trap ID: 30**

CIM Prefix: IMM CIM ID: 0040

User Response Procedure

Information only; no action is required.

FQXSPSS4001I: Server General Settings set by user [arg1]: Name=[arg2], Contact=[arg3], Location=[arg4], Room=[arg5], RackID=[arg6], Rack U-position=[arg7].

A user configured the Location setting.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0080

User Response Procedure

Information only; no action is required.

FQXSPSS4002I: License key for [arg1] added by user [arg2].

A user installs the License Key.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0096

User Response Procedure

Information only; no action is required.

FQXSPSS4003I: License key for [arg1] removed by user [arg2].

A user removes a License Key.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0097

User Response Procedure

Information only; no action is required.

FQXSPSS4004I: Test Call Home Generated by user [arg1].

Test Call Home generated by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0134

User Response Procedure

Information only; no action is required.

FQXSPSS4005I: Manual Call Home by user [arg1]: [arg2].

Manual Call Home by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0135

User Response Procedure

Information only; no action is required.

FQXSPSS4006I: Call Home to [arg1] failed to complete: [arg2].

Call Home failed to complete.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0195

User Response Procedure

Information only; no action is required.

FQXSPSS4007I: The BMC functionality tier is changed from [arg1] to [arg2].

Tier Change.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0222

User Response Procedure

Information only; no action is required.

FQXSPSS4008I: The [arg1] setting has been changed to [arg2] by user [arg3].

The setting has been changed by user.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0225

User Response Procedure

Information only; no action is required.

FQXSPSS4009I: System enters LXPM maintenance mode.

The system enters BMC Provisioning Manager maintenance mode.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0226

User Response Procedure

Information only; no action is required.

FQXSPTR4000I: Management Controller [arg1] clock has been set from NTP server [arg2].

This message is for the use case where a Management Controller clock has been set from the Network Time Protocol (NTP) server.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0033

User Response Procedure

Information only; no action is required.

FQXSPTR4001I: Date and Time set by user [arg1]: Date=[arg2], Time-[arg3], DST Auto-adjust=[arg4], Timezone=[arg5].

A user configured the Date and Time settings.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0079

User Response Procedure

Information only; no action is required.

FQXSPTR4002I: Synchronize time setting by user [arg1]: Mode=Sync with NTP Server, NTPServerHost1=[arg2]:[arg3],NTPServerHost2=[arg4]:[arg5],NTPServerHost3=[arg6]:[arg7], NTPServerHost4=[arg8]:[arg9],NTPUpdateFrequency=[arg10].

A user configured the Date and Time synchronize settings.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0085

User Response Procedure

Information only; no action is required.

FQXSPTR4003I: Synchronize time setting by user [arg1]: Mode=Sync with server clock.

A user configured the Date and Time synchronize settings.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category None **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0224

User Response Procedure

Information only; no action is required.

FQXSPUN0009G: Sensor [SensorElementName] has asserted.

This message is for the use case when an implementation has detected a Sensor has asserted.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0508

User Response Procedure

Reboot the system. If the problem still exists, press F1 or use BMC Provisioning Manager to do an BMC Controller Firmware update.

FQXSPUN0017I: Sensor [SensorElementName] has transitioned to normal state.

This message is for the use case when an implementation has detected a Sensor transition to the normal state.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Other **SNMP Trap ID: 60**

CIM Prefix: PLAT CIM ID: 0518

User Response Procedure

Information only; no action is required.

FQXSPUN0018J: Sensor [SensorElementName] has transitioned from normal to non-critical state.

This message is for the use case when an implementation has detected a Sensor transitioned to non-critical from normal.

Severity Informational

Serviceable Yes

Automatically Notify Support No

Alert Category Warning - Other **SNMP Trap ID: 60**

CIM Prefix: PLAT CIM ID: 0520

User Response Procedure

Please check the System Event Log (SEL) of the BMC Controller to investigate the identified device for enhancement.

FQXSPUN0019M: Sensor [SensorElementName] has transitioned to critical from a less severe state.

This message is for the use case when an implementation has detected a Sensor transitioned to critical from less severe.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0522

User Response Procedure

Complete the following steps:

1. Please check the BMC Web Console to see the identified error.
2. Check the System Event Log (SEL) to fix the error.
3. If the problem still exists, please contact Service.

FQXSPUN0020N: Sensor [SensorElementName] has transitioned to non-recoverable from a less severe state.

This message is for the use case when an implementation has detected a Sensor transitioned to non-recoverable from less severe.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0524

User Response Procedure

Complete the following steps:

1. Please flash uEFI image to the latest level.
2. If the problem still exist, please remove and re-install the CMOS battery for 30 seconds to clear CMOS contents.
3. If the problem still exists, please contact Service.

FQXSPUN0023N: Sensor [SensorElementName] has transitioned to non-recoverable.

This message is for the use case when an implementation has detected a Sensor transitioned to non-recoverable.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0530

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If the error continues, replace the system board assembly (see the Intel® Server System R2600SR Setup and Service Guide).

FQXSPUN0026G: Device [LogicalDeviceElementName] has been added.

This message is for the use case when an implementation has detected a Sensor transitioned to non-recoverable.

Severity Warning

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0536

User Response Procedure

Information only; no action is required.

FQXSPUN0026I: Device [LogicalDeviceElementName] has been added.

This message is for the use case when an implementation has detected a Device was inserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0536

User Response Procedure

Information only; no action is required.

FQXSPUN2010I: Sensor [SensorElementName] has asserted.

This message is for the use case when an implementation has detected a Sensor has asserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0508

User Response Procedure

Reflash uEFI image. If error does not persist, no additional recovery action is required.

FQXSPUN2012I: Sensor [SensorElementName] has deasserted.

This message is for the use case when an implementation has detected a Sensor has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0509

User Response Procedure

Information only; no action is required.

FQXSPUN2018I: Sensor [SensorElementName] has deasserted the transition from normal to non-critical state.

This message is for the use case when an implementation has detected a Sensor has deasserted a transition to non-critical from normal.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Warning - Other **SNMP Trap ID: 60**

CIM Prefix: PLAT CIM ID: 0521

User Response Procedure

Information only; no action is required.

FQXSPUN2019I: Sensor [SensorElementName] has transitioned to a less severe state from critical.

This message is for the use case when an implementation has detected a Sensor transition to less severe from critical.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0523

User Response Procedure

Information only; no action is required.

FQXSPUN2020I: Sensor [SensorElementName] has deasserted the transition to non-recoverable from a less severe state.

This message is for the use case when an implementation has detected a Sensor transition to non-recoverable from less severe has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0525

User Response Procedure

Information only; no action is required.

FQXSPUN2023I: Sensor [SensorElementName] has deasserted the transition to non-recoverable.

This message is for the use case when an implementation has detected a Sensor transition to non-recoverable has deasserted.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0531

User Response Procedure

Information only; no action is required.

FQXSPUN2030I: Device [LogicalDeviceElementName] has been removed from unit [PhysicalPackageElementName].

This message is for the use case when an implementation has detected a Device was removed.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0537

User Response Procedure

Information only; no action is required.

FQXSPUP0007L: Invalid or Unsupported firmware or software was detected on system [ComputerSystemElementName].

This message is for the use case when an implementation has detected an Invalid/Unsupported Firmware/ Software Version.

Severity Error

Serviceable Yes

Automatically Notify Support No

Alert Category Critical - Other **SNMP Trap ID: 50**

CIM Prefix: PLAT CIM ID: 0446

User Response Procedure

Reflash or update BMC Controller firmware.

FQXSPUP4000I: Please ensure that the Management Controller [arg1] is flashed with the correct firmware. The Management Controller is unable to match its firmware to the server.

This message is for the use case where Management Controller firmware version does not match the server.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0031

User Response Procedure

Update the BMC Controller firmware to a version that the server supports.

Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before updating the code.

FQXSPUP4001I: Flash of [arg1] from [arg2] succeeded for user [arg3] .

This message is for the use case where a user has successfully flashed the firmware component (MC Main Application, MC Boot ROM, BIOS, Diagnostics, System Power Backplane, Remote Expansion Enclosure Power Backplane, and Integrated System Management).

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: IMM CIM ID: 0035

User Response Procedure

Informational only; no action is required.

FQXSPUP4002I: Flash of [arg1] from [arg2] failed for user [arg3].

This message is for the use case where a user has not flashed the firmware component from the interface and IP address due to a failure.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0036

User Response Procedure

Informational only; no action is required.

FQXSPUP4003I: [arg1] firmware mismatch internal to system [arg2]. Please attempt to flash the [arg3] firmware.

This message is for the use case where a specific type of firmware mismatch has been detected.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0042

User Response Procedure

Reflash the BMC Controller firmware to the latest version.

FQXSPUP4004I: BMC CONTROLLER firmware mismatch between nodes [arg1] and [arg2]. Please attempt to flash the BMC CONTROLLER firmware to the same level on all nodes.

A mismatch of BMC Controller firmware has been detected between nodes.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0132

User Response Procedure

Attempt to flash the BMC Controller firmware to the same level on all nodes.

FQXSPUP4005I: FPGA firmware mismatch between nodes [arg1] and [arg2]. Please attempt to flash the FPGA firmware to the same level on all nodes.

A mismatch of FPGA firmware has been detected between nodes.

Severity Error

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID: 22**

CIM Prefix: IMM CIM ID: 0133

User Response Procedure

Attempt to flash the FPGA firmware to the same level on all nodes.

FQXSPWD0000I: Watchdog Timer expired for [WatchdogElementName].

This message is for the use case when an implementation has detected a Watchdog Timer expired.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0368

User Response Procedure

Informational only; no action is required.

FQXSPWD0001I: Reboot of system [ComputerSystemElementName] initiated by Watchdog [WatchdogElementName].

This message is for the use case when a Reboot by a Watchdog occurred and been detected.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0370

User Response Procedure

Informational only; no action is required.

FQXSPWD0002I: Powering off system [ComputerSystemElementName] initiated by Watchdog [WatchdogElementName].

This message is for the use case when a Poweroff by a Watchdog has occurred and been detected.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0372

User Response Procedure

Informational only; no action is required.

FQXSPWD0003I: Power cycle of system [ComputerSystemElementName] initiated by Watchdog [WatchdogElementName].

This message is for the use case when a Power Cycle by Watchdog has occurred and been detected.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0374

User Response Procedure

Informational only; no action is required.

FQXSPWD0004I: Watchdog Timer interrupt occurred for [WatchdogElementName].

This message is for the use case when a Watchdog Timer interrupt has occurred and been detected.

Severity Informational

Serviceable No

Automatically Notify Support No

Alert Category System - Other **SNMP Trap ID:**

CIM Prefix: PLAT CIM ID: 0376

User Response Procedure

Informational only; no action is required.

4. Unified Extensible Firmware Interface (UEFI) Events

Unified Extensible Firmware Interface (UEFI) error messages can be generated when the server starts up in Power-on Self-Test (POST) or while it is running. These UEFI error messages are logged in the BMC event log residing in the server.

4.1 Event Descriptors

Each event has an assigned code. For each event code, the following fields are displayed:

Event Identifier

An identifier that uniquely identifies an event.

Event Description

The logged message string that appears for an event. When the event string is displayed in the event log, information such as a specific component is displayed. In this documentation, that additional information appears as variables, such as [arg1] or [arg2].

Explanation

Phrase which provides additional information to detail why the event occurred.

Severity

An indication of the level of concern for the condition. The severity is abbreviated in the event log to the first character. The following severities can be displayed:

- **Informational**. The event was recorded for audit purposes, usually a user action or a change of state that is normal behavior.
- **Warning**. The event is not as severe as an error, but, if possible, the condition should be corrected before it becomes an error. It might also be a condition that requires additional monitoring or maintenance.
- **Error**. The event is a failure or critical condition that impairs service or an expected function.

User Response

Indication of the actions to perform to solve the event. Perform the steps listed in this section in the order shown until the problem is solved. Contact Support if, after all steps are performed, the problem is not resolved.

4.2 Unified Extensible Firmware Interface (UEFI) Event List

This section lists all messages that can be sent from the UEFI.

FQXPMEM0001M: Unable to locate LXPM firmware image.

Unable to locate BMC Provisioning Manager firmware image.

Severity Error

User Response Procedure

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).

Note: When performing an AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

2. If an error recurs, contact Support.

FQXPMEM0002I: LXPM firmware image found. Starting LXPM.

BMC Provisioning Manager firmware image found. Starting BMC Provisioning Manager.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMEM0003I: LXPM has exited. Control returned to UEFI.

BMC Provisioning Manager has exited. Control returned to UEFI.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMNM0001G: Failed to set new BMC network parameters.

Failed to set new BMC network parameters.

Severity Warning

User Response Procedure

Complete the following steps:

1. Verify that input parameters are correct.
2. If not correct, reset the BMC via the BMC Web Console.
3. Retry.
4. Use UEFI to set the parameters (optional).

FQXPMNM0002I: Set BMC network parameters to new values.

Set BMC network parameters to new values.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMOS0001K: Bootx64.efi is not found, Failed to Boot OS.

Bootx64.efi is not found; Failed to Boot OS.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC via the BMC Web Console and retry to boot the OS.
2. If OS still fails to boot, perform AC reset.
3. Retry to boot the OS.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMOS0002K: Read Deployment Manager Signature Failure from USB.

Read Deployment Manager Signature Failure from USB.

Severity Warning

User Response Procedure

Complete the following steps:

1. Ensure proper operation of the virtual USB connection.
2. Reset the BMC via the BMC Web Console and retry reading the Deployment Management Signature Failure.
3. If still unable to read the signature failure, perform AC reset.
4. Retry reading the Deployment Management Signature Failure.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMOS0003K: Failed to copy Windows boot files to target.

Failed to copy Windows boot files to target.

Severity Warning

User Response Procedure

Complete the following steps:

1. Verify the proper operation of the virtual USB connection.
2. Reset the BMC via the BMC Web Console and retry copying the Windows boot file.
3. If still unable to copy the Windows boot file, perform AC reset.
4. Retry copying the Windows boot file.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMOS0004K: BMC Communication Failed: EMMC2USB Mount Failure.

BMC Communication Failed: EMMC2USB Mount Failure.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC via the BMC Web Console and retry mounting the EMMC2USB.
2. If still unable to mount the EMMC2USB, perform AC reset.
3. Retry mounting the EMMC2USB.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMOS0005K: BMC Communication Failed: DRIVER Mount Failure.

BMC Communication Failed: DRIVER Mount Failure.

Severity Warning

User Response Procedure

Complete the following steps:

1. Verify the proper operation of the virtual USB connection.
2. Reset the BMC via the BMC Web Console and retry mounting the driver.
3. If still unable to mount the driver, perform AC reset.
4. Retry mounting the driver.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMOS0006K: BMC Communication Success!! Volume Name MISMATCHED.

BMC Communication Success!! Volume Name MISMATCHED.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC via the BMC Web Console and retry.
2. Perform AC reset.
3. Retry.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMOS0007K: Failed to read License RTF file.

Failed to read License RTF file.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC via the BMC Web Console and retry reading the License RTF file.
2. If still unable to read the License RTF License file, perform AC reset.
3. Retry reading the License RTF file.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMOS0008K: Please make sure the Ethernet cable has been plugged into your computer and your network settings are correct.

Please make sure the Ethernet cable has been plugged into the server and the network settings are correct.

Severity Warning

User Response Procedure

1. Ensure proper operation of SMB/CIFS and NFS communications.
2. Retry.

FQXPMOS0009K: Current System Boot Mode is Legacy. Only Support UEFI Mode.

Current System Boot Mode is Legacy. Only Support UEFI Mode.

Severity Warning

User Response Procedure

Change Boot mode to UEFI mode.

FQXPMOS0010I: Red Hat RHEL 7.3 (64-bit) OS installed.

Red Hat RHEL 7.3 (64-bit) OS installed .

Severity Informational

User Response Procedure

N/A

FQXPMOS0011I: Red Hat RHEL 6.9 (64-bit) OS installed.

Red Hat RHEL 6.9 (64-bit) OS installed .

Severity Informational

User Response Procedure

N/A

FQXPMOS0012I: SLES 12 for AMD64 and Intel64 Service Pack 2 OS installed.

SLES 12 for AMD64 and Intel64 Service Pack 2 OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0013I: SLES 11 for AMD64 and Intel64 Service Pack 4 OS installed.

SLES 11 for AMD64 and Intel64 Service Pack 4 OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0014I: Windows Server 2012 R2 SERVERWINFOUNDATION OS installed.

Windows Server 2012 R2 SERVERWINFOUNDATION OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0015I: Windows Server 2012 R2 SERVERSTANDARD OS installed.

Windows Server 2012 R2 SERVERSTANDARD OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0016I: Windows Server 2012 R2 SERVERDATACENTER OS installed.

Windows Server 2012 R2 SERVERDATACENTER OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0017I: Windows Server 2012 R2 SERVERSOLUTION OS installed.

Windows Server 2012 R2 SERVERSOLUTION OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0018I: Windows Server 2012 R2 SERVERSTORAGESTANDARD OS installed.

Windows Server 2012 R2 SERVERSTORAGESOLUTION OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0019I: Hyper-V Server 2012 R2 SERVERHYPERCORE OS installed.

Hyper-V Server 2012 R2 SERVERHYPERCORE OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0020I: Hyper-V Server 2016 SERVERHYPERCORE OS installed.

Hyper-V Server 2016 SERVERHYPERCORE OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0021I: Windows Server 2016 SERVERSOLUTION OS installed.

Windows Server 2016 R2 SERVERSOLUTION OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0022I: Windows Server 2016 SERVERSTANDARD OS installed.

Windows Server 2016 SERVERSTANDARD OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0023I: Windows Server 2016 SERVERDATACENTER OS installed.

Windows Server 2016 SERVERDATACENTER OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0024I: Windows Server 2016 SERVERSTORAGESTANDARD OS installed.

Windows Server 2016 SERVERSTORAGESTANDARD OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0025I: Windows Server 2016 SERVERSTORAGEWORKGROUP OS installed.

Windows Server 2016 SERVERSTORAGEWORKGROUP OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0026I: Vmware ESXi 6.5 U1 OS installed.

Vmware ESXi 6.5 U1 OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMOS0027I: Vmware ESXi 6.0 U3 OS installed.

Vmware ESXi 6.0 U3 OS installed.

Severity Informational

User Response Procedure

N/A

FQXPMSD0001M: HDD Test was interrupted by the host with a hardware or software reset.

HDD Test was interrupted by the host with a hardware or software reset.

Severity Error

User Response Procedure

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If the error recurs, contact Support.

FQXPMSD0002M: A fatal error or unknown test error occurred while the device was executing its self-test.

A fatal error or unknown test error occurred while the device was executing its self-test.

Severity Error

User Response Procedure

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If the error recurs, contact Support.

FQXPMSD0003M: Self-test completed having a test element that failed and the test element that failed is not known.

Self-test completed having a test element that failed and the test element that failed is not known.

Severity Error

User Response Procedure

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If the error recurs, contact Support.

FQXPMSD0004M: Self-test completed having the electrical element of the test failed.

Self-test completed having the electrical element of the test failed.

Severity Error

User Response Procedure

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If the error recurs, contact Support.

FQXPMSD0005M: Self-test completed having the servo (and/or seek) test element of the test failed.

Self-test completed having the servo (and/or seek) test element of the test failed.

Severity Error

User Response Procedure

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If the error recurs, contact Support.

FQXPMSD0006M: Self-test completed having the read element of the test failed.

Self-test completed having the read element of the test failed.

Severity Error

User Response Procedure

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If the error recurs, contact Support.

FQXPMSD0007M: Hard Drive(s) not found.

Hard Drive(s) not found.

Severity Error

User Response Procedure

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If the error recurs, contact Support.

FQXPMSR0001K: Found unsupported RAID adapter.

Found unsupported RAID adapter.

Severity Warning

User Response Procedure

RAID adapters are not supported in the Intel® Server System R2600SR. Remove the unsupported RAID adapter.

FQXPMSR0012I: Change disk drives' state successfully.

Change disk drives' state successfully.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMSR0021L: Failed to create new virtual disk.

Failed to create new virtual disk.

Severity Warning

User Response Procedure

RAID adapters are not supported in the Intel® Server System R2600SR. Remove the unsupported RAID adapter.

FQXPMSR0022I: Create new virtual disk successfully.

Create new virtual disk successfully.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMSR0032I: Remove existing virtual disk successfully.

Remove existing virtual disk successfully.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMUP0001K: The system configuration does not meet the prerequisite.

The system configuration does not meet the prerequisite.

Severity Warning

User Response Procedure

1. Follow prompts to update the firmware and retry.
2. If error recurs, contact Support.

FQXPMUP0002K: The selected packages are not compatible.

The selected packages are not compatible.

Severity Warning

User Response Procedure

1. Follow prompts to update each individual firmware package.
2. If error recurs, contact Support.

FQXPMUP0003K: Unable to obtain the minimum level of UEFI.

Unable to obtain the minimum level of UEFI.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error occurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0004K: Unable to obtain the installed version of UEFI.

Unable to obtain the installed version of UEFI.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error occurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0005K: Unable to obtain the installed version of BMC.

Unable to obtain the installed version of the BMC.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error occurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0006K: Unable to obtain the installed version of LXPM.

Unable to obtain the installed version of the BMC Provisioning Manager.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error occurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0007K: Unable to obtain the installed version of Linux driver.

Unable to obtain the installed version of Linux driver.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error occurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0008K: Unable to obtain the installed version of Windows driver.

Unable to obtain the installed version of Windows driver.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error occurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0101I: Start to update LXPM.

Start to update the BMC Provisioning Manager.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMUP0102I: Start to update Windows driver.

Start to update Windows driver.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMUP0103I: Start to update Linux driver.

Start to update Linux driver.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMUP0104I: Start to update UEFI.

Start to update UEFI.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMUP0105I: Start to update BMC.

Start to update BMC.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMUP0106I: Successful to update the firmware.

Successful to update the firmware.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMUP0201M: BMC communication failed: EMMC2USB mount failure. Failed to update the firmware.

BMC communication failed: EMMC2USB mount failure. Failed to update the firmware.

Severity Error

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI to perform the update.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0202M: Transfer the update package error. Failed to update the firmware.

Transfer the update package error. Failed to update the firmware.

Severity Error

User Response Procedure

Complete the following steps:

1. Ensure the update package is not damaged and retry updating the firmware.
2. Ensure proper connection to USB/network drive and retry updating the firmware.
3. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
4. Use the BMC or OneCLI to perform the update .If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0203M: BMC communication failed: EMMC2USB unmount failure. Failed to update the firmware.

BMC communication failed: EMMC2USB unmount failure. Failed to update the firmware.

Severity Error

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI to perform the update.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0204M: BMC communication failed: Execute the update CMD failure. Failed to update the firmware.

BMC communication failed: Execute the update CMD failure. Failed to update the firmware.

Severity Error

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI to perform the update.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0205M: BMC communication failed: Get the update status failure. Failed to update the firmware.

BMC communication failed: Get the update status failure. Failed to update the firmware.

Severity Error

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI to perform the update.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0206M: The level of the update package is too old. Failed to update the firmware.

The level of the update package is too old. Failed to update the firmware.

Severity Error

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI to perform the update.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0207M: The update package is invalid. Failed to update the firmware.

The update package is invalid. Failed to update the firmware.

Severity Error

User Response Procedure

Complete the following steps:

1. Ensure the update package is not damaged and retry updating the firmware.
2. Ensure proper connection to USB/network drive and retry updating the firmware.
3. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
4. Use the BMC or OneCLI to perform the update.
5. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMUP0208M: Failed to execute reboot BMC command.

Failed to execute reboot BMC command.

Severity Error

User Response Procedure

Complete the following steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI to perform the update.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back. After AC power is restored, power on the host system.

FQXPMVD0001H: Failed to get VPD data.

Failed to get VPD data.

Severity Warning

User Response Procedure

Complete the following steps:

1. Press "Back" button and press "Update VPD" button again.
2. If step 1 is unsuccessful, perform AC reset.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back on. After AC power is restored, power on the host system.

FQXPMVD0002H: Failed to update the VPD data.

Failed to update the VPD data.

Severity Warning

User Response Procedure

Complete the following steps:

1. Press "Update" button on VPD update page.
2. If step 1 is unsuccessful, perform AC reset.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back. After AC power is restored, power on the host system.

FQXPMVD0003I: Update VPD data successfully.

Update VPD data successfully.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXPMVD0011K: Failed to get the TPM/TCM policy status.

Failed to get TPM/TCM policy status.

Severity Warning

User Response Procedure

Complete the following steps:

1. Press "Update" button on VPD update page.
2. If step 1 is unsuccessful, perform AC reset.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back. After AC power is restored, power on the host system.

FQXPMVD0012K: Failed to set the TPM/TCM policy.

Failed to set the TPM/TCM policy.

Severity Warning

User Response Procedure

Complete the following steps:

1. Press "Apply" button on VPD update page.
2. If step 1 is unsuccessful, reboot the system.
3. If error recurs, contact Support.

Note: When performing an AC reset, power off the AC. Wait several seconds before powering the AC back. After AC power is restored, power on the host system.

FQXSFDD0001G: DRIVER HEALTH PROTOCOL: Missing Configuration. Requires Change Settings From F1.

DRIVER HEALTH PROTOCOL: Missing Configuration. Requires Change Settings From F1.

Severity Warning

User Response Procedure

Complete the following steps:

1. Go to F1 Setup > System Settings > Settings > Driver Health Status List and find the driver/controller reporting “Configuration Required” status.
2. Search for the Driver menu from System Settings and change the driver settings appropriately.
3. Save settings and restart system.

FQXSFDD0002M: DRIVER HEALTH PROTOCOL: Reports 'Failed' Status Controller.

DRIVER HEALTH PROTOCOL: Reports 'Failed' Status Controller.

Severity Error

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If problem persists, reflash the adapter firmware.

FQXSFDD0003I: DRIVER HEALTH PROTOCOL: Reports 'Reboot' Required Controller.

DRIVER HEALTH PROTOCOL: Reports 'Reboot' Required Controller.

Severity Informational

User Response Procedure

Complete the following steps:

1. No action required - system will reboot automatically at the end of POST.
2. If message persists, reflash the adapter firmware.

FQXSFDD0004M: DRIVER HEALTH PROTOCOL: Reports 'System Shutdown' Required Controller.

DRIVER HEALTH PROTOCOL: Reports 'System Shutdown' Required Controller.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If problem persists, reflash the adapter firmware.

FQXSFDD0005M: DRIVER HEALTH PROTOCOL: Disconnect Controller Failed. Requires 'Reboot'.

DRIVER HEALTH PROTOCOL: Disconnect Controller Failed. Requires 'Reboot'.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If problem persists, reflash the adapter firmware.

FQXSFDD0006M: DRIVER HEALTH PROTOCOL: Reports Invalid Health Status Driver.

DRIVER HEALTH PROTOCOL: Reports Invalid Health Status Driver.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If problem persists, reflash the adapter firmware.

FQXSFDD0007G: Security Key Lifecycle Manager (SKLM) IPMI Error.

Security Key Lifecycle Manager (SKLM) IPMI Error.

Severity Warning

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
2. Reboot system. If problem persists, escalate to the next level of support.

FQXSFIO0005M: An intra-board UPI failure has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

An intra-board UPI failure has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
2. Inspect processor socket for foreign debris or damage. If debris is found, remove debris.
3. If error recurs or socket damage is found, replace the system board.

FQXSFIO0006M: An inter-board UPI failure has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

An inter-board UPI failure has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
2. Inspect processor socket for foreign debris or damage. If debris is found, remove debris.
3. If error recurs or socket damage is found, replace the system board.

FQXSFIO0007M: An error has been detected by the IIO on Bus [arg1]. The value of Global Fatal Error Status register is [arg2]. The value of Global Non-Fatal Error Status register is [arg3]. Please check error logs for additional downstream device error data, the physical slot number is [arg4].

An error has been detected by the IIO on Bus [arg1]. The value of Global Fatal Error Status register is [arg2]. The value of Global Non-Fatal Error Status register is [arg3]. Please check error logs for additional downstream device error data; the physical slot number is [arg4].

Severity Error

User Response Procedure

Complete the following steps:

1. Check log for a separate error for an associated PCIe* device and service that error.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
3. Replace the system board.

FQXSFIO0008M: An intra-board UPI dynamic link width reduction has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

An intra-board UPI dynamic link width reduction has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

Severity Error

User Response Procedure

Complete the following steps:

1. Reboot system.
2. If problem persists, escalate it to the next level of support.

FQXSFIO0009M: An inter-board UPI dynamic link width reduction has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

An inter-board UPI dynamic link width reduction has been detected on the link between processor [arg1] port [arg2] and processor [arg3] port [arg4].

Severity Error

User Response Procedure

Complete the following steps:

1. Reboot system.
2. If problem persists, escalate it to the next level of support.

FQXSFIO0010M: An Uncorrectable PCIe Error has Occurred at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].

An Uncorrectable PCIe* Error has Occurred at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].

Severity Error

User Response Procedure

Complete the following steps if the compute node and/or any attached cables were recently installed, moved, serviced or upgraded:

1. Reseat the adapter and any attached cables.
2. Reload device driver.
3. If the device is not recognized, reconfiguring slot to Gen1 or Gen2 may be required.

Note: Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports -> PCIe Gen1/Gen2/Gen3 Speed Selection or the OneCLI utility.

Then do these steps:

4. Check the Intel Support Site (http://www.intel.com/support) for a firmware or device driver update that applies to this error.
5. Load the new device driver and install any required firmware updates.
6. Do one of the following:
    a. If the problem persists, remove that adapter.
    b. If system reboots successfully without an adapter, replace the adapter with one that is updated.

FQXSFIO0011M: A PCIe parity error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].

A PCIe* parity error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware or device driver update that applies to this error.
2. Load new device driver and any required firmware updates.
3. If this node and/or any attached cables were recently installed, moved, serviced, or upgraded:
    a. Reseat the adapter and any attached cables.
    b. Reload the device driver.
    c. If a device is not recognized, reconfiguring the slot to Gen1 or Gen2 may be required (see the following Note instruction).

Note: Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports -> PCIe Gen1/Gen2/Gen3 Speed Selection or the OneCLI utility.

---

    d. If a PCIe* error has also been reported on a second slot within the same node, perform steps a, b, and c above for that adapter before proceeding.
    e. If the problem persists, then remove the adapter card for this slot.
4. Do one of the following:
    a. If system reboots successfully without the adapter, replace that card.
    b. If the system fails to reboot successfully and a second slot within the same node has also logged a PCIe* error, re-insert the adapter from the previous step and remove the second adapter.
    c. If system reboots successfully without the second adapter, replace that card.
5. If a problem persists, do the following:
    a. Replace the compute node with the PCIe* slot in question.
    b. Replace the compute book associated with the PCIe* slot/slots.
6. Replace the processor.

FQXSFIO0012M: A PCIe system error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].

A PCIe* system error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware or device driver update that applies to this error.
2. Load new device driver and any required firmware updates.
3. If this node and/or any attached cables were recently installed, moved, serviced, or upgraded:
    a. Reseat the adapter and any attached cables.
    b. Reload the device driver.
    c. If a device is not recognized, reconfiguring the slot to Gen1 or Gen2 may be required (see the Note following this instruction).

Note: Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports -> PCIe Gen1/Gen2/Gen3 Speed Selection or the OneCLI utility.

---

    d. If a PCIe* error has also been reported on a second slot within the same node, perform steps a, b, and c above for that adapter before proceeding.
    e. If the problem persists, then remove the adapter card for this slot.
4. Do one of the following:
    a. If system reboots successfully without the adapter, replace that card.
    b. If the system fails to reboot successfully and a second slot within the same node has also logged a PCIe* error, re-insert the adapter from the previous step and remove the second adapter.
    c. If system reboots successfully without the second adapter, replace that card.
5. If a problem persists, do the following:
    a. Replace the compute node with the PCIe* slot in question.
    b. Replace the compute book associated with the PCIe* slot/slots.
6. Replace the processor.

FQXSFIO0013I: The device found at Bus [arg1] Device [arg2] Function [arg3] could not be configured due to resource constraints. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].

The device found at Bus [arg1] Device [arg2] Function [arg3] could not be configured due to resource constraints. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].

Severity User

User Response Procedure

Complete the following steps:

1. If this PCIe* device and/or any attached cables were recently installed, moved, serviced, or upgraded, reseat adapter and any attached cables.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.

Note: It may be necessary to disable unused option ROMs from UEFI F1 setup, OneCLI utility, or using adapter manufacturer utilities so that adapter firmware can be updated.

---

3. Move the adapter to a different slot. If a slot is not available or error recurs, replace the adapter.
4. If the adapter was moved to a different slot and the error did not recur, verify that this is not a system limitation. Then replace the system board. Also, if this is not the initial installation and the error persists after adapter replacement, replace the system board.

FQXSFIO0014J: A bad option ROM checksum was detected for the device found at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].

A bad option ROM checksum was detected for the device found at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].

Severity User

User Response Procedure

Complete the following steps:

1. If this PCIe* device and/or any attached cables were recently installed, moved, serviced, or upgraded, reseat adapter and any attached cables.
2. Move adapter to a different system slot, if available.
3. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.

Note: It may be necessary to configure slot to Gen1 or to use special utility software so that adapter firmware can be upgraded. Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports -> PCIe Gen1/Gen2/Gen3 Speed Selection or the OneCLI utility.

---

4. Replace adapter.

FQXSFIO0015I: IFM: System reset performed to reset adapters.

IFM: System reset performed to reset adapters.

Severity Informational

User Response Procedure

No user required for this event. This is for informational purposes only.

FQXSFIO0016M: IFM: Reset loop avoided - Multiple resets not allowed.

IFM: Reset loop avoided - Multiple resets not allowed.

Severity Warning

User Response Procedure

Complete the following steps:

1. Update all firmware (including adapter firmware) to the latest levels.
2. If problem persists escalate to the next level of support.

FQXSFIO0017M: IFM: Error communicating with the BMC - IFM may not be deployed correctly.

IFM: Error communicating with the BMC - IFM may not be deployed correctly.

Severity Error

User Response Procedure

Complete the following steps:

1. Update all firmware (including adapter firmware) to the latest levels.
2. If problem persists escalate to the next level of support.

FQXSFIO0018I: IFM: Configuration too large for compatibility mode.

IFM: Configuration too large for compatibility mode.

Severity Informational

User Response Procedure

No user response is required for this event. For informational purposes only.

FQXSFIO0019J: PCIe Resource Conflict [arg1].

PCIe* Resource Conflict [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. If this PCIe* device and/or any attached cables were recently installed, moved, serviced, or upgraded, reseat the adapter and any attached cables.
2. Move the adapter to a different system slot, if available.
3. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.

Note: It may be necessary to configure slot to Gen1 or to use special utility software so that adapter firmware can be upgraded. Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports -> PCIe Gen1/Gen2/Gen3 Speed Selection or the OneCLI utility.

---

4. Replace the PCIe*device.

FQXSFIO0020J: PCIe Isolation has occurred in PCIe slot [arg1]. The adapter may not operate correctly.

PCIe* Isolation has occurred in PCIe* slot [arg1]. The adapter may not operate correctly.

Severity Error

User Response Procedure

Complete the following steps:

1. Check the log for a separate error related to an associated PCIe* device and resolve that error.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.
3. If the problem persists, replace the adapter.
4. If this is not the initial installation and the error persists after adapter replacement, replace the system board.

FQXSFIO0021J: PCIe LER has occurred in PCIe slot [arg1]. The adapter may not operate correctly.

PCIe* LER has occurred in PCIe* slot [arg1]. The adapter may not operate correctly.

Severity Error

User Response Procedure

Complete the following steps:

1. Check the log for a separate error related to an associated PCIe* device and resolve that error.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.
3. If the problem persists, move the adapter to a different slot. If a slot is not available or error recurs, replace the adapter.
4. If the adapter was moved to a different slot and the error did not recur, verify that this is not a system limitation. Then replace the system board.
5. If this is not the initial installation and the error persists after adapter replacement, replace the system board.

FQXSFIO0022J: PCIe Link Width has degraded from [arg2] to [arg3] in PCIe slot [arg1]

PCIe* Link Width has degraded from [arg2] to [arg3] in PCIe slot [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the log for a separate error related to an associated PCIe* device and resolve that error.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.
3. If the problem persists, move the adapter to a different slot. If a slot is not available or error recurs, replace the adapter.
4. If the adapter was moved to a different slot and the error did not recur, verify that this is not a system limitation. Then replace the system board.
5. If this is not the initial installation and the error persists after adapter replacement, replace the system board.

FQXSFIO0023J: PCIe Link Speed has degraded from [arg2] to [arg3] in PCIe slot [arg1].

PCIe* Link Speed has degraded from [arg2] to [arg3] in PCIe* slot [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the log for a separate error related to an associated PCIe* device and resolve that error.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.
3. If the problem persists, move the adapter to a different slot. If a slot is not available or error recurs, replace the adapter.
4. If this is not the initial installation and the error persists after adapter replacement, replace the system board.

FQXSFMA0001M: DIMM [arg1] has been disabled due to an error detected during POST.

DIMM [arg1] has been disabled due to an error detected during POST.

Severity Error

User Response Procedure

Complete the following steps:

1. If the DIMM was disabled because of a memory fault, follow the procedure for that event.
2. If no memory fault is recorded in the logs and no DIMM connector error LEDs are lit, re-enable the DIMM through the Setup utility or the OneCLI utility.
3. If problem persists, power cycle the compute node from the management console.
4. Reset BMC to default settings.
5. Reset UEFI to default settings.
6. Update BMC and UEFI firmware.
7. Replace the system board.

Note: Additional information about V10/V20/V30 DIMM fault indicators:
V10: All DIMMs in the system are qualified, including the failing DIMM.
V20: The failing DIMM is unqualified.
V30: The failing DIMM is qualified but the system contains non-failing unqualified DIMMs.

FQXSFMA0002I: The uncorrectable memory error state has been cleared.

The uncorrectable memory error state has been cleared.

Severity Error

User Response Procedure

Information only; no action is required.

FQXSFMA0002M: An uncorrectable memory error has been detected on DIMM [arg1].

An uncorrectable memory error has been detected on DIMM [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. If the compute node has recently been installed, moved, serviced, or upgraded, verify that the DIMM is properly seated; visually verify that there is no foreign material in any DIMM connector on that memory channel. If either of these conditions is found, correct and retry boot with the same DIMM.
    a. If no problem is observed on the DIMM connectors or the problem persists, replace the DIMM identified on the event log entry.
    b. If the problem recurs on the same DIMM connector, replace the other DIMMs on the same memory channel.

Note: The event log may contain a recent FQXSFMA0011I event denoting a detected change in DIMM population that could be related to this problem.

    c. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.
    d. If the problem recurs on the same DIMM connector, inspect connector for damage. If found, replace the system board.
2. Replace the affected processor.
3. Replace the system board.

Note: Additional information about V10/V20/V30 DIMM fault indicators:
V10: All DIMMs in the system are qualified, including the failing DIMM.
V20: The failing DIMM is unqualified.
V30: The failing DIMM is qualified, but the system contains non-failing unqualified DIMMs.

FQXSFMA0003K: A memory mismatch has been detected. Please verify that the memory configuration is valid [arg1].

A memory mismatch has been detected. Please verify that the memory configuration is valid [arg1].

Severity Error

User Response Procedure

Complete the following steps:

Note: If an uncorrectable memory error or failed memory test cannot be traced, check the log and service that event first. DIMMs disabled by other errors or actions may be causing this event.

---

1. Verify that the DIMMs are installed in the correct population sequence.
2. Disable memory mirroring and sparing.
3. Update UEFI firmware.
4. Replace the DIMM.
5. Replace the processor.

FQXSFMA0004N: No system memory has been detected [arg1].

No system memory has been detected [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. If any memory errors are logged other than this one, take actions indicated for those codes first.
2. If no other memory diagnostic codes appear in the logs, verify that all DIMM connectors are enabled using the Setup utility or the OneCLI utility.
3. If the problem remains, shut down and remove node from chassis and physically verify that one or more DIMMs are installed and that all DIMMs are installed in the correct population sequence.
4. If DIMMs are present and properly installed, check for any lit DIMM-connector LEDs, and, if found, reseat those DIMMs.
5. If DIMMs are not installed, install approved DIMMS in the correct population sequence.
6. Reinstall the node in chassis, power on the node.
7. Check logs for memory diagnostic codes.
8. If the problem remains, replace the processor and repeat steps 6 and 7
9. If the problem remains, replace the system board and repeat steps 6 and 7.

FQXSFMA0005N: Memory is present within the system but could not be configured. Please verify that the memory configuration is valid [arg1].

Memory is present within the system but could not be configured. Please verify that the memory configuration is valid [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. Ensure one or more DIMMs is installed in the server.
2. Resolve existing memory errors if they are present.
3. If no memory fault is recorded in the logs and no DIMM connector error LEDs are lit, verify that all DIMM connectors are enabled using the Setup utility or the OneCLI utility.
4. If DIMM connector error lights are lit, reseat all DIMMs ensuring that DIMMs are installed in the correct population sequence, according to the service information for this product.
5. Clear CMOS memory.

Note: All firmware settings will revert to the defaults when reseated.

6. Reflash UEFI firmware.
7. Replace the processor.
8. Replace the system board.

FQXSFMA0006I: [arg1] DIMM [arg2] has been detected, the DIMM serial number is [arg3].

[arg1] DIMM [arg2] has been detected, the DIMM serial number is [arg3].

Severity Error

User Response Procedure

Complete the following steps:

1. If this information event is logged in the BMC System Event Log (SEL), the server does not have qualified memory installed. Please verify that the installed memory if on the list of supported DIMMs.
2. The identified memory installed may not be covered under warranty.

Note: Without qualified memory, speeds supported above industry standards will not be enabled.

3. Please contact the local sales representative or authorized business partner to order qualified memory to replace the unqualified DIMM(s).
4. After qualified memory is installed and the server is powered up, verify that this informational event has not been logged again.

FQXSFMA0007I: [arg1] DIMM number [arg2] has been replaced [arg3].

[arg1] DIMM number [arg2] has been replaced [arg3].

Severity Informational

User Response Procedure

Complete the following steps:

1. If this information event is logged in the BMC System Event Log (SEL), the server does not have qualified memory installed.

Note: Without qualified memory, speeds supported above industry standards will not be enabled.

---

2. Please contact the local sales representative or authorized business partner to order qualified memory to replace the unqualified DIMM(s).
3. After qualified memory is installed and the server is powered up, verify this informational event is not logged again.

FQXSFMA0008M: DIMM [arg1] has failed the POST memory test [arg2].

DIMM [arg1] has failed the POST memory test [arg2].

Severity Error

User Response Procedure

Complete the following steps:

1. Be sure to AC-cycle the system to re-enable affected DIMM connector or re-enable manually using F1 setup.
2. If the compute node has been recently installed, serviced, moved, or upgraded, check to ensure that DIMMs are firmly seated and that no foreign material can be seen in the DIMM connector. If either condition is observed, correct and retry with the same DIMM.

Note: The event log may contain a recent FQXSFMA0011IA4 event denoting a detected change in DIMM population that could be related to this problem.

---

   a. If the problem persists, replace the DIMM identified by the event log entry. If this is a flash DIMM, make sure it is still under warranty before replacing it.
   b. If the problem re-occurs on the same DIMM connector, swap the other DIMMs on the same memory channel across channels one at a time to a different memory channel or processor. (
   c. If the problem follows a moved DIMM to a different memory channel, replace that DIMM.
   d. If the problem stays with the original DIMM connector, re-inspect the DIMM connector for foreign material and remove it if found.
   e. If the connector is damaged, replace the system board.
   f. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this memory error.
3. Remove the affected processor and inspect processor socket pins for damaged or misaligned pins.
   a. If damage is found or if this is an upgraded processor, replace the system board.
   b. If there is only one processor (or the problem follows the affected processor), replace the affected processor.
   c. If there are multiple processors, swap processors to move the affected processor to another processor socket and retry.
4. If the problem still exists, replace the system board.

FQXSFMA0009K: Invalid memory configuration for Mirror Mode. Please correct memory configuration [arg1].

Invalid memory configuration for Mirror Mode. Please correct memory configuration [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. If a DIMM connector error LED is lit, resolve the failure.
2. Make sure that the DIMM connectors are correctly populated for mirroring mode, according to the service information for this product.

FQXSFMA0010K: Invalid memory configuration for Sparing Mode. Please correct memory configuration [arg1].

Invalid memory configuration for Sparing Mode. Please correct memory configuration [arg1].

Severity Error

User Response Procedure

Make sure that the DIMM connectors are correctly populated for sparing mode according to the service information for this product.

FQXSFMA0011I: Memory population change detected [arg1].

Memory population change detected [arg1].

Severity Informational

User Response Procedure

Complete the following steps:

1. If DIMMs have been added to or removed from the system and no additional errors were detected, then please ignore this message.
2. Check the System Event Log (SEL) for uncorrected DIMM failures and replace those DIMMs.

FQXSFMA0012L: The [arg1] PFA Threshold limit has been exceeded on DIMM [arg2] at address [arg3]. The value of MC Status is [arg4] and the value of MC Misc is [arg5][arg6].

The [arg1] PFA Threshold limit has been exceeded on DIMM [arg2] at address [arg3]. The value of MC Status is [arg4] and the value of MC Misc is [arg5][arg6].

Severity Error

User Response Procedure

Complete the following steps:

1. If the compute node has recently been installed, moved, serviced, or upgraded, verify that the DIMM is properly seated and visually confirm that there is no foreign material in any DIMM connector on that memory channel. If either of these conditions is found, correct and reinstall the compute node with the same DIMM.

Note: The event log may contain a recent FQXSFMA0011I event denoting detected change in DIMM population that could be related to this problem.

---

2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this memory error.
3. The release notes will list the known problems the update addresses.
4. If the previous steps do not resolve the problem, at the next maintenance opportunity, replace the affected DIMM (as indicated by the failure log entry).
    a. If PFA re-occurs on the same DIMM connector, swap the other DIMMs on the same memory channel one at a time to a different memory channel or processor.
    b. If PFA follows a moved DIMM to any DIMM connector on the different memory channel, replace the moved DIMM.
    c. If problem continues to re-occur on the same DIMM connector, inspect DIMM connector for foreign material and remove, if found.
    d. If the DIMM connector is damaged, replace system board.
5. Remove the affected processor and inspect the processor socket pins for damaged or misaligned pins. If damage is found or the processor is an upgrade part, replace the system board.
6. Replace the affected processor.
7. Replace the system board.

FQXSFMA0013I: Mirror Fail-over complete. DIMM [arg1] has failed over to the mirrored copy [arg2].

Mirror Fail-over complete. DIMM [arg1] has failed over to the mirrored copy [arg2].

Severity Informational

User Response Procedure

Check the System Event Log (SEL) for uncorrected DIMM failures and replace those DIMMs.

FQXSFMA0014I: Memory spare copy initiated [arg1].

Memory spare copy initiated [arg1].

Severity Informational

User Response Procedure

No user required for this event. For informational purposes only.

FQXSFMA0015I: Memory spare copy has completed successfully [arg1].

Memory spare copy has completed successfully [arg1].

Severity Informational

User Response Procedure

Complete the following steps:

Check the system log for related DIMM failures and replace those DIMMs.

FQXSFMA0016M: Memory spare copy failed [arg1].

Memory spare copy failed [arg1].

Severity Error

User Response Procedure

Check the system log for related DIMM failures and replace those DIMMs.

FQXSFMA0017I: DIMM Re-enabled [arg1].

DIMM Re-enabled [arg1].

Severity Informational

User Response Procedure

Check system log for related DIMM failures.

FQXSFMA0018I: DIMM Service Action Detected, Slot Re-Enabled [arg1].

DIMM Service Action Detected, Slot Re-Enabled [arg1].

Severity Informational

User Response Procedure

Check the system log for related DIMM failures.

FQXSFMA0019I: System Memory Resized [arg1].

System Memory Resized [arg1].

Severity Informational

User Response Procedure

Check system log for related DIMM failures and replace those DIMMs.

FQXSFMA0022N: All DIMMs have been disabled and the system will be unable to boot until this is corrected.

All DIMMs have been disabled and the system will be unable to boot until this is corrected.

Severity Error

User Response Procedure

Check system log for related DIMM failures and replace those DIMMs.

FQXSFMA0023M: Error has occurred in NVDIMM flash. NVDIMM backup/restore may not operate correctly [arg1].

Error has occurred in NVDIMM flash. NVDIMM backup/restore may not operate correctly [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. If the compute node has recently been installed, moved, serviced, or upgraded, verify that the DIMM is properly seated and visually confirm that there is no foreign material in any DIMM connector on that memory channel.
2. If no problem is observed on the DIMM connectors or the problem persists, check the Intel Support Site (http://www.intel.com/support) for a firmware update applicable to this memory error.
3. If the problem persists, replace the DIMM identified by the event log entry.
4. If problem recurs on the same DIMM connector, inspect connector for damage. If found, replace the system board.

FQXSFMA0024M: Error has occurred in NVDIMM Supercap. NVDIMM backup/restore may not operate correctly [arg1].

Error has occurred in NVDIMM Supercap. NVDIMM backup/restore may not operate correctly [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. If the compute node has recently been installed, moved, serviced, or upgraded, verify that the DIMM is properly seated and visually confirm that there is no foreign material in any DIMM connector on that memory channel.
2. If no problem is observed on the DIMM connectors or the problem persists, check the Intel Support Site (http://www.intel.com/support) for an applicable firmware or adapter update.
3. If the problem persists, replace the DIMM identified by LightPath and/or event log entry.
4. If problem recurs on the same DIMM connector, inspect connector for damage. If found, replace the system board.

FQXSFMA0025M: NVDIMM Supercap has been disconnected. NVDIMM will lose its backup ability until this is corrected [arg1].

NVDIMM Supercap has been disconnected. NVDIMM will lose its backup ability until this is corrected [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. If the compute node has recently been installed, moved, serviced, or upgraded, verify that the DIMM is properly seated and visually confirm that there is no foreign material in any DIMM connector on that memory channel.
2. If no problem is observed on the DIMM connectors or the problem persists, check the Intel Support Site (http://www.intel.com/support) for an applicable firmware or adapter update.
3. If the problem persists, replace the DIMM identified by LightPath and/or event log entry.
4. If problem recurs on the same DIMM connector, inspect connector for damage. If found, replace the system board.

FQXSFMA0026M: DIMM [arg1] Self-healing attempt [arg2] [arg3].

DIMM [arg1] Self-healing attempt [arg2] [arg3].

Severity Error

User Response Procedure

Complete the following steps:

1. If the compute node has recently been installed, moved, serviced, or upgraded, verify that the DIMM is properly seated and visually confirm that there is no foreign material in any DIMM connector on that memory channel. If either of these conditions is found, correct and retry with the same DIMM.

Note: The event log may contain a recent FQXSFMA0011I event denoting detected change in DIMM population that could be related to this problem.

---

2. Check the Intel Support Site (http://www.intel.com/support) for a firmware or adapter update that applies to this error.
3. If the previous steps do not resolve the problem, at the next maintenance opportunity, replace the affected DIMM (as indicated by failure log entry).
    a. If PFA re-occurs on the same DIMM connector, swap the other DIMMs on the same memory channel one at a time to a different memory channel or processor.
    b. If PFA follows a moved DIMM to any DIMM connector on the different memory channel, replace the moved DIMM.
    c. If problem re-occurs on the same DIMM connector, inspect the DIMM connector for damage. If found, replace the system board.
4. Remove the affected processor and inspect the processor socket pins for damaged or misaligned pins. If damage is found or the processor is an upgrade part, replace the system board.
5. Replace the affected processor.
6. Replace the system board.

FQXSFMA0027K: Invalid memory configuration (Unsupported DIMM Population) detected. Please verify memory configuration is valid.

Invalid memory configuration (Unsupported DIMM Population) detected. Please verify that the memory configuration is valid.

Severity Error

User Response Procedure

Complete the following steps:

1. This event could follow an uncorrectable memory error or failed memory test. Check the log and resolve that event first. DIMMs disabled by other errors or actions could cause this event.

FQXSFMA0028K: Memory Capacity exceeds CPU limit [arg1].

Memory Capacity exceeds CPU limit [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. Remove AC power from the system.
2. Modify memory configuration to ensure memory capacity does not exceed processor SKU limit.

FQXSFPU0001N: An unsupported processor has been detected.

An unsupported processor has been detected.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify the processor is a valid FRU/option that is listed as a server-proven device for this system. If a non-supported processor is identified, remove that processor or replace with a supported processor.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor and install the update, if applicable.

FQXSFPU0002N: An invalid processor type has been detected.

An invalid processor has been detected.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify the processor is a valid FRU/option that is listed as a server-proven device for this system. If a non-supported processor is identified, remove that processor or replace with a supported processor.
2. Check the Intel Support Site (http://www.intel.com/support for a firmware update required for this processor and install that update, if applicable.

FQXSFPU0003K: A processor mismatch has been detected between one or more processors in the system.

A processor mismatch has been detected between one or more processors in the system.

Severity Error

User Response Procedure

Complete the following steps:

1. This message could occur with messages about other processor configuration problems. If so, resolve those messages first.
2. If the problem persists, ensure that matching processors are installed (i.e., matching option part numbers, etc).
3. Verify that the processors are installed in the correct sockets according to the service information for this product. If not, correct that problem.
4. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
5. Replace mismatching processor. Inspect processor socket and replace the compute node if socket is damaged.

FQXSFPU0004K: A discrepancy has been detected in the number of cores reported by one or more processors within the system.

A discrepancy has been detected in the number of cores reported by one or more processors within the system.

Severity Error

User Response Procedure

Complete the following steps:

1. If this is a newly installed option, ensure that matching processors are installed in the correct processor sockets.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the processor. Inspect the processor socket and replace the system board first if the socket is damaged.

FQXSFPU0005K: A mismatch between the maximum allowed UPI link speed has been detected for one or more processors.

A mismatch between the maximum allowed UPI link speed has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. If this is a newly installed option, ensure that matching processors are installed in the correct processor sockets.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the processor. Inspect the processor socket and replace the system board first if the socket is damaged.

FQXSFPU0006K: A power segment mismatch has been detected for one or more processors.

A power segment mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Processors installed do not have the same power requirements.
2. Ensure that all processors have matching power requirements (such as 65, 95, or 130 Watts).
3. Replace the processor. Inspect the processor socket and replace the system board first if the socket is damaged.

FQXSFPU0007K: Processors have mismatched Internal DDR Frequency.

Processors have mismatched Internal DDR Frequency.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching DIMMs are installed in the correct population sequence. Correct any configuration issues found.
2. Replace the associated processor. Inspect the processor socket and replace the system board first if the socket is damaged.

FQXSFPU0008K: A core speed mismatch has been detected for one or more processors.

A core speed mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the processor. Inspect the processor socket and replace the system board first if the socket is damaged.

FQXSFPU0009K: An external clock frequency mismatch has been detected for one or more processors.

An external clock frequency mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that the processor is a valid option that is listed as a Server-Proven device for this system. If not, remove the processor and install one listed on the Server-Proven website.
2. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
3. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
4. Replace the processor. Inspect the processor socket and replace the system board first if the socket is damaged.

FQXSFPU0010K: A cache size mismatch has been detected for one or more processors.

A cache size mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the system board.

FQXSFPU0011K: A cache type mismatch has been detected for one or more processors.

A cache type mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the system board.

FQXSFPU0012K: A cache associativity mismatch has been detected for one or more processors.

A cache type associativity mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the system board.

FQXSFPU0013K: A processor model mismatch has been detected for one or more processors.

A processor model mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the system board.

FQXSFPU0014N: A processor family mismatch has been detected for one or more processors.

A processor family mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the system board.

FQXSFPU0015K: A processor stepping mismatch has been detected for one or more processors.

A processor stepping mismatch has been detected for one or more processors.

Severity Error

User Response Procedure

Complete the following steps:

1. Verify that matching processors are installed in the correct processor sockets. Correct any mismatch issues found.
2. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
3. Replace the system board.

FQXSFPU0016N: A processor within the system has failed the BIST.

A processor within the system has failed the BIST.

Severity Error

User Response Procedure

Complete the following steps:

1. If the processor or firmware was just updated, check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this processor error.
2. If this is a single processor system or the problem follows the affected processor, replace the processor.
3. If there are multiple processors, swap processors to move the affected processor to another processor socket and retry.
4. Inspect the processor socket on each processor removed. Replace the system board first if the processor socket is damaged or misaligned pins are found.
5. Replace the system board.

FQXSFPU0017G: A processor microcode update failed.

A processor microcode update failed.

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware update which applies to this processor error.
2. Replace the processor.

FQXSFPU0018N: CATERR(IERR) has asserted on processor [arg1].

CATERR(IERR) has asserted on processor [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a UEFI firmware update that applies to this processor error.
2. Reboot system. If problem persists, escalate to the next level of support.

FQXSFPU0019N: An uncorrectable error has been detected on processor [arg1].

An uncorrectable error has been detected on processor [arg1].

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a UEFI firmware update that applies to this processor error.
2. Reboot system. If problem persists, contact Support.

FQXSFPU0020I: The UEFI firmware image capsule signature is invalid.

The UEFI firmware image capsule signature is invalid.

Severity Informational

User Response Procedure

Complete the following steps:

1. Reboot system.
2. Reflash UEFI image.
3. If error does not persist, no additional recovery action is required.
4. If error persists, or boot is unsuccessful, replace the system board.

FQXSFPU0021G: Hardware physical presence is in asserted state.

Hardware physical presence is in asserted state.

Severity Warning

User Response Procedure

Complete the following steps:

1. Complete administrative tasks requiring the TPM Physical Presence Switch to be "ON."
2. Restore the physical presence switch to the "OFF" position and reboot the system.
3. Replace the system board.

FQXSFPU0021I: The TPM physical presence state has been cleared.

The TPM physical presence state has been cleared.

Severity Informational

User Response Procedure

Information only: no action is required.

FQXSFPU0022G: The TPM configuration is not locked.

The TPM configuration is not locked.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If problem persists, contact Support.

FQXSFPU0023G: Secure Boot Image Verification Failure Warning.

Secure Boot Image Verification Failure Warning. This applies when the user wants to boot from an unauthorized UEFI image or OS while Secure Boot is enabled and Secure Boot Mode is in User Mode.

Severity Warning

User Response Procedure

To allow system boot from this unauthorized image, first disable Secure Boot and then enroll the unauthorized UEFI image into the Authorized Signature Database. Complete the following steps:

1. Disable Secure Boot through these steps:
    a. Before asserting Physical Presence, change the Secure Boot Setting to “Disable” through F1 Setup -> System Settings -> Security -> Security Boot Configuration -> Security Boot Setting
    b. Assert Physical Presence via the Physical Presence Jumper or Remote Physical Presence through one of these two methods. Either:
        1) Move the Physical Presence Jumper to the "ON" position, or
        2) If the "Physical Presence Policy" has been set to "Enable" in F1 Setup (as described above) use the IPMI Tool to assert remote Physical Presence via "System Settings -> Security -> Physical Presence Policy" in F1 Setup.
    c. After asserting the Physical Presence, change the Secure Boot Policy to Custom Policy through Setup -> System Settings -> Security -> Security Boot Configuration-> Security Boot Policy.
    d. Enter the "Security Boot Custom Policy" menu and press the "Enroll EFI Image" button.
    e. Select the unauthorized UEFI Image from the popup box.
    f. Enroll the unauthorized UEFI Image into the Authorized Signature Database .
2. If the problem persists, contact Support.

FQXSFPU0024G: Intel BIOS ACM startup failed, make sure TPM is enabled.

Intel BIOS ACM startup failed; make sure TPM is enabled.

Severity Warning

User Response Procedure

Complete the following steps:

1. Assert Physical Presence via the Physical Presence Jumper or Remote Physical Presence. Either:
    a. Move the Physical Presence Jumper to the "ON" position, or
    b. Assert the remote Physical Presence via the IPMI tool if the "Physical Presence Policy" has been set to "Enable" in F1 Setup. The setting can be found in F1 Setup at "System Settings -> Security -> Physical Presence Policy".
2. Enable and activate the TPM. The setting can be found in F1 at "System Settings -> Security -> Trusted Platform Module -> TPM1.2".
    a. Change [TPM Device] to "Enable."
    b. Change [TPM State] to "Activate."
3. Reboot the system.
4. If problem persists, contact Support.

FQXSFPU0025I: The default system settings have been restored.

The default system settings have been restored.

Severity Informational

User Response Procedure

Complete the following steps:

Information only no action is required.

FQXSFPU0030N: A firmware fault has been detected in the UEFI image.

A firmware fault has been detected in the UEFI image.

Severity Error

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
2. Reflash UEFI image.
3. Replace the system board.

FQXSFPU0031N: The number of POST attempts has reached the value configured in F1 setup. The system has booted with default UEFI settings. User specified settings have been preserved and will be used on subsequent boots unless modified before rebooting.

The number of POST attempts has reached the value configured in the F1 setup. The system has booted with default UEFI settings. User-specified settings have been preserved and will be used on subsequent boots unless modified before rebooting.

Severity Error

User Response Procedure

Complete the following steps:

1. Original UEFI settings are still present. To continue using the original settings, select Save Settings.
2. If the reboots were not intentionally triggered, check logs for probable cause. (For example, if there is a battery fault event, follow the steps to resolve that event.)
3. Undo recent system changes (settings or devices added).
4. Verify that the system boots.
5. Reinstall options one at a time to locate the problem.
6. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
7. Update UEFI firmware if applicable.
8. Remove and re-install the CMOS battery for 30 seconds to clear CMOS contents. If it boots successfully, then restore system settings.
9. Replace the system board.

FQXSFPU0032G: A boot configuration error has been detected.

A boot configuration error has been detected.

Severity Error

User Response Procedure

Complete the following steps:

1. F1 Setup -> Save Settings
2. Retry OOB config update.

FQXSFPU0033G: Processor has been disabled.

Processor has been disabled.

Severity Warning

User Response Procedure

Complete the following steps:

1. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
2. Reboot system.
3. If problem persists, escalate to the next level of support.

FQXSFPU0034L: The TPM could not be properly initialized.

The TPM could not be properly initialized.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot system.
2. Reflash UEFI image.
3. If error does not persist, no additional recovery action is required.
4. If error persists or boot is unsuccessful, replace the system board.

FQXSFPU4033F: TPM Firmware recovery is in progress. Please DO NOT power off or reset system.

TPM Firmware recovery is in progress. Please DO NOT power off or reset system.

Severity Warning

User Response Procedure

Information only; no action is required.

FQXSFPU4034I: TPM Firmware recovery is finished, rebooting system to take effect.

TPM Firmware recovery is finished; rebooting system to take effect.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4035M: TPM Firmware recovery failed. TPM chip may be damaged.

TPM Firmware recovery failed. TPM chip may be damaged.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If the error recurs, TPM-related features will not work.
3. Contact Support if necessary.

FQXSFPU4036F: TPM Firmware recovery is starting. Please DO NOT power off or reset system.

TPM Firmware recovery is starting. Please DO NOT power off or reset system.

Severity Warning

User Response Procedure

Information only; no action is required.

FQXSFPU4037I: TPM Firmware recovery is finished.

TPM Firmware recovery is finished.

Severity Warning

User Response Procedure

Information only; no action is required.

FQXSFPU4038I: TPM Firmware recovery successful.

TPM Firmware recovery successful.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4040M: TPM self-test has failed.

TPM self-test has failed.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If the error recurs, TPM-related features will notwork.
3. Contact Support if necessary.

FQXSFPU4041I: TPM Firmware update is in progress. Please DO NOT power off or reset system.

TPM Firmware update is in progress. Please DO NOT power off or reset system.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4042I: TPM Firmware update is finished, rebooting system to take effect.

TPM Firmware update is finished; rebooting system to take effect.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4043G: TPM Firmware update aborted. System is rebooting...

TPM Firmware update aborted. System is rebooting...

Severity Warning

User Response Procedure

Information only; no action is required.

FQXSFPU4044I: The current TPM firmware version could not support TPM version toggling.

The current TPM firmware version could not support TPM version toggling.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4045G: Physical Presence is not asserted, abort TPM Firmware upgrade.

Physical Presence is not asserted; abort TPM Firmware upgrade.

Severity Warning

User Response Procedure

Information only; no action is required.

FQXSFPU4046I: TPM Firmware will be updated from TPM1.2 to TPM2.0.

TPM Firmware will be updated from TPM1.2 to TPM2.0.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4047I: TPM Firmware will be updated from TPM2.0 to TPM1.2.

TPM Firmware will be updated from TPM2.0 to TPM1.2.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4049I: TPM Firmware update successful.

TPM Firmware update successful.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4050G: Failed to update TPM Firmware.

Failed to update TPM Firmware.

Severity Warning

User Response Procedure

Information only; no action is required.

FQXSFPU4051G: Undefined TPM_TCM_POLICY found.

Undefined TPM_TCM_POLICY found.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If problem persists, contact Support.

FQXSFPU4052G: TPM_TCM_POLICY is not locked.

TPM_TCM_POLICY is not locked.

Severity Warning

User Response Procedure

Complete the following steps:

1. Reboot the system.
2. If problem persists, contact Support.

FQXSFPU4053G: System TPM_TCM_POLICY does not match the planar.

System TPM_TCM_POLICY does not match the planar.

Severity Warning

User Response Procedure

Complete the following steps:

1. Remove any newly added TPM/TCM card from the planar or re-install theoriginal TPM/TCM card that shipped with the system.
2. Reboot the system.
3. If problem persists, contact Support.

FQXSFPU4054G: TPM/TCM card logical binding has failed.

TPM/TCM card logical binding has failed.

Severity Warning

User Response Procedure

Reboot the system.

FQXSFPU4056M: TPM/TCM card is changed, need install back the original TCM/TPM card which shipped with the system.

TPM/TCM card is changed, need install back the original TCM/TPM card which shipped with the system.

Severity Error

User Response Procedure

Complete the following steps:

1. Reinstall the original TPM/TCM card that shipped with the system.
2. Reboot the system.
3. If problem persists, contact Support.

FQXSFPU4080I: Host Power-On password has been changed.

Host Power-On password has been changed.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4081I: Host Power-On password has been cleared.

Host Power-On password has been cleared.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4082I: Host Admin password has been changed.

Host Admin password has been changed.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4083I: Host Admin password has been cleared.

Host Admin password has been cleared.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4084I: Host boot order has been changed.

Host boot order has been changed.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPU4085I: Host WOL boot order has been changed.

Host WOL boot order has been changed.

Severity Informational

User Response Procedure

Information only; no action is required.

FQXSFPW0001L: CMOS has been cleared.

CMOS has been cleared.

Severity Error

User Response Procedure

Complete the following steps:

1. If the CMOS clear was user-initiated, this event can be safely ignored and no further action is required.
2. If the system was recently installed, moved, or serviced, make sure the battery is properly seated.
3. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
4. Replace CMOS battery.
5. If the problem still exists, replace the system board.

FQXSFSM0001L: Power capping is disabled.

Power capping is disabled.

Severity Warning

User Response Procedure

Complete the following steps:

Check settings and event logs.

FQXSFSM0002N: Boot Permission denied by Management Module: System Halted.

Boot Permission denied by Management Module: System Halted.

Severity Warning

User Response Procedure

Complete the following steps:

1. Check BMC log.
2. Review power policies and system configuration settings in the BMC Web Console.

FQXSFSM0003N: Timed Out waiting on boot permission from Management Module: System Halted.

Timed Out waiting on boot permission from Management Module: System Halted.

Severity Warning

User Response Procedure

Complete the following steps:

1. Check the BMC log.
2. Review power policies and system configuration settings in the BMC Web Console.

FQXSFSM0004M: An BMC communication failure has occurred.

An BMC communication failure has occurred.

Severity Warning

User Response Procedure

Complete the following steps:

1. Check the BMC network cables and configuration.
2. AC cycle the system.
3. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
4. Reflash BMC Firmware.
5. Replace the system board in the compute node.

FQXSFSM0005M: An error occurred while saving UEFI settings to the BMC.

An error occurred while saving UEFI settings to the BMC.

Severity Warning

User Response Procedure

Complete the following steps:

1. Use F1 Setup, Verify, and Save Settings to recover settings.
2. Reset BMC from SMM or BMC GUI.
3. AC cycle the system.
4. Check the Intel Support Site (http://www.intel.com/support) for a firmware update that applies to this error.
5. Reflash BMC firmware.
6. Remove and re-install CMOS battery for 30 seconds to clear CMOS contents.
7. Replace the system board.

FQXSFSM0006M: Unable to retrieve the system configuration from the BMC.

Unable to retrieve the system configuration from the BMC.

Severity Warning

User Response Procedure

Complete the following steps:

1. Use F1 Setup, Verify, and Save Settings to recover settings.
2. Reset BMC from SMM or BMC Web Console.
3. AC cycle the system.
4. Check the Intel Support Site (http://www.intel.com/support) for a firmware update applicable to this error.
5. Reflash BMC firmware.
6. Remove and re-install CMOS battery for 30 seconds to clear CMOS contents.
7. Replace the system board.

FQXSFSM0007I: The BMC System Event log (SEL) is full.

The BMC System Event log (SEL) is full.

Severity Informational

User Response Procedure

Complete the following steps:

1. Use the BMC Web Console to clear the System Event Log (SEL).
2. If the BMC Web Console is unavailable, use F1 Setup to access System Event Logs Menu and Choose Clear the BMC System Event Log and then restart the server.

FQXSFSM0008M: Boot permission timeout detected.

Boot permission timeout detected.

Severity Error

User Response Procedure

Complete the following steps:

1. Check the CMM/BMC System Event Logs (SEL) for communication errors and resolve those errors.
2. Reseat the compute node.
3. If problem persists, escalate to the next level of support.

FQXSFSR0001M: [arg1] GPT corruption detected, DiskGUID: [arg2]

[arg1] GPT corruption detected, DiskGUID: [arg2]

Severity Warning

User Response Procedure

Complete the following steps:

1. Press F1 Setup -> System Settings -> Recovery -> Disk GPT Recovery and set to "Automatic."
2. Save settings and restart the system.
3. Boot to F1 setup; system automatically tries to recover the GPT during the POST.
4. Restart the system.
5. If problem persists, re-format the LUN or disk and re-install the OS.

FQXSFSR0002I: [arg1] GPT corruption recovered, DiskGUID: [arg2]

[arg1] GPT corruption recovered, DiskGUID: [arg2]

Severity Informational

User Response Procedure

No further user action is required at this point since issue has been resolved.

FQXSFSR0003G: The number of boot attempts has been exceeded. No bootable device found.

The number of boot attempts has been exceeded. No bootable device found.

Severity Warning

User Response Procedure

Complete the following steps:

1. Remove AC power from the system.
2. Connect at least one bootable device to the system.
3. Connect AC power to the system.
4. Power on system and retry.

FQXSFTR0001L: An invalid date and time have been detected.

An invalid date and time have been detected.

Severity Warning

User Response Procedure

Complete the following steps:

1. Check the BMC System Event Log (SEL). This event should immediately precede a FQXSFPW0001L error. Resolve that event or any other battery-related errors.
2. Use F1 Setup to reset date and time.
    a. If problem returns after a system reset, replace the CMOS battery.
3. Check the Intel Support Site (http://www.intel.com/support) for a firmware update applicable to this error.
4. Replace the system board.

5. BMC Provisioning Manager Events

The following events can be generated by the BMC Provisioning Manager.

5.1 Event Descriptors

For each event code, the following fields are displayed:

Event Identifier

An identifier that uniquely identifies an event.

Event Description

The logged message string that appears for an event. When the event string is displayed in the event log, information such as a specific component is displayed. In this documentation, that additional information appears as variables, such as [arg1] or [arg2].

Explanation

Phrase which provides additional information to detail why the event occurred.

Severity

An indication of the level of concern for the condition. The severity is abbreviated in the event log to the first character. The following severities can be displayed:

- **Informational**. The event was recorded for audit purposes, usually a user action or a change of state that is normal behavior.
- **Warning**. The event is not as severe as an error, but, if possible, the condition should be corrected before it becomes an error. It might also be a condition that requires additional monitoring or maintenance.
- **Error**. The event is a failure or critical condition that impairs service or an expected function.

User Response

Indication of the actions to perform to solve the event. Perform the steps listed in this section in the order shown until the problem is solved. Contact Support if the problem is not resolved after all steps are performed.

5.2 BMC Provisioning Manager Event List

This section lists all messages that can be sent from the BMC Provisioning Manager.

FQXPMEM0001M: Unable to locate LXPM firmware image.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

2. If the error recurs, contact Support.

FQXPMEM0002I: LXPM firmware image found. Starting LXPM.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMEM0003I: LXPM has exited. Control returned to UEFI.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required. The BMC Provisioning Manager has exited.

FQXPMNM0001G: Failed to set new BMC network parameters.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

To set new BMC network parameters, do the following:

1. Verify input parameters are correct.
2. Wait one minute and retry.
3. Reset the BMC via the BMC Web Console.
4. Retry.
5. Use UEFI to set parameters (optional).

FQXPMNM0002I: Set BMC network parameters to new values.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMOS0001K: Bootx64.efi is not found, Failed to Boot OS.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

To boot the OS, do the following:

1. Reset the BMC via the BMC Web Console and retry.
2. Perform AC reset.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

3. Retry.

FQXPMOS0002K: Read Deployment Manager Signature Failure from USB.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

To boot the OS, do the following:

1. Ensure proper operation of the virtual USB connection.
2. Reset the BMC via the BMC Web Console and retry.
3. Perform AC reset.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

4. Retry.

FQXPMOS0003K: Failed to copy Windows boot files to target.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

To copy the boot files, do the following:

1. Ensure proper operation of the virtual USB connection.
2. Reset the BMC via the BMC Web Console and retry.
3. Perform AC reset.
4. Retry.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMOS0004K: BMC Communication Failed: EMMC2USB Mount Failure.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC via the BMC Web Console and retry.
2. Perform AC reset.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

3. Retry.

FQXPMOS0005K: BMC Communication Failed: DRIVER Mount Failure.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

To boot the OS, do the following:

1. Verify proper operation of the virtual USB connection.
2. Reset the BMC via the BMC Web Console and retry.
3. Perform AC reset.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

4. Retry.

FQXPMOS0006K: BMC Communication Success!! Volume Name MISMATCHED.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC via the BMC Web Console andretry.
2. Perform AC reset.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

3. Retry.

FQXPMOS0007K: Failed to read License RTF file.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC via the BMC Web Console andretry.
2. Perform AC reset.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

---

3. Retry.

FQXPMOS0008K: Please make sure the Ethernet cable has been plugged into your computer and your network settings are correct.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Ensure proper operation of SMB/CIFS and NFS communications.
2. Retry.

FQXPMOS0009K: Current System Boot Mode is Legacy. Only Support UEFI Mode.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Change Boot mode to UEFI mode.
2. Retry.

FQXPMOS0010I: Red Hat RHEL 7.3 (64-bit) OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0011I: Red Hat RHEL 6.9 (64-bit) OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0012I: SLES 12 for AMD64 and Intel64 Service Pack 2 OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0013I: SLES 11 for AMD64 and Intel64 Service Pack 4 OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0014I: Windows Server 2012 R2 SERVERWINFOUNDATION OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0015I: Windows Server 2012 R2 SERVERSTANDARD OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0016I: Windows Server 2012 R2 SERVERDATACENTER OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0017I: Windows Server 2012 R2 SERVERSOLUTION OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0018I: Windows Server 2012 R2 SERVERSTORAGESTANDARD OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0019I: Hyper-V Server 2012 R2 SERVERHYPERCORE OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0020I: Hyper-V Server 2016 SERVERHYPERCORE OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0021I: Windows Server 2016 SERVERSOLUTION OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0022I: Windows Server 2016 SERVERSTANDARD OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0023I: Windows Server 2016 SERVERDATACENTER OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0024I: Windows Server 2016 SERVERSTORAGESTANDARD OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0025I: Windows Server 2016 SERVERSTORAGEWORKGROUP OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0026I: Vmware ESXi 6.5 U1 OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMOS0027I: Vmware ESXi 6.0 U3 OS installed.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

N/A

FQXPMSD0001M: HDD Test was interrupted by the host with a hardware or software reset.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If error recurs, contact Support.

FQXPMSD0002M: A fatal error or unknown test error occurred while the device was executing its self-test.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If error recurs, contact Support.

FQXPMSD0003M: self-test completed having a test element that failed and the test element that failed is not known.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If error recurs, contact Support.

FQXPMSD0004M: Self-test completed having the electrical element of the test failed.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If error recurs, contact Support.

FQXPMSD0005M: self-test completed having the servo (and/or seek) test element of the test failed.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If error occurs, contact Support.

FQXPMSD0006M: Self-test completed having the read element of the test failed.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If error recurs, contact Support.

FQXPMSD0007M: Hard Drive(s) not found.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Verify proper connection of hard drives, backplane, and all related cables.
2. Ensure device firmware is at the latest level.
3. Retry test.
4. If error recurs, contact Support.

FQXPMSR0001K: Found unsupported RAID adapter.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

RAID is not supported in this server system. Remove the unsupported RAID adapter.

FQXPMSR0012I: Change disk drives' state successfully.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMSR0022I: Create new virtual disk successfully.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMSR0032I: Remove existing virtual disk successfully.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMUP0001K: The system configuration does not meet the prerequisite.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Follow prompts to update the firmware and retry.
2. If error recurs, contact Support.

FQXPMUP0002K: The selected packages are not compatible.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Follow prompts to update each firmware package.
2. If error recurs, contact Support.

FQXPMUP0003K: Unable to obtain the minimum level of UEFI.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0004K: Unable to obtain the installed version of UEFI.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0005K: Unable to obtain the installed version of BMC.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0006K: Unable to obtain the installed version of LXPM.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0007K: Unable to obtain the installed version of Linux driver.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0008K: Unable to obtain the installed version of Windows driver.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0101I: Start to update LXPM.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMUP0102I: Start to update Windows driver.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMUP0103I: Start to update Linux driver.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMUP0104I: Start to update UEFI.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMUP0105I: Start to update BMC.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMUP0106I: Successful to update the firmware.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMUP0201M: BMC communication failed: EMMC2USB mount failure. Failed to update the firmware.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI tools to perform the update.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0202M: Transfer the update package error. Failed to update the firmware.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Ensure the update package is not damaged and retry.
2. Ensure proper connection to USB/network drive and retry.
3. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
4. Use the BMC or OneCLI tools to perform the update.
5. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0203M: BMC communication failed: EMMC2USB unmount failure. Failed to update the firmware.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI tools to perform the update.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0204M: BMC communication failed: Execute the update cmd failure. Failed to update the firmware.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI tools to perform the update.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0205M: BMC communication failed: Get the update status failure. Failed to update the firmware.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. Use the BMC or OneCLI tools to perform the update.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0206M: The level of the update package is too old. Failed to update the firmware.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Follow prompts to select a newer version of the update package and retry.
2. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
3. Use the BMC or OneCLI tools to perform the update.
4. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0207M: The update package is invalid. Failed to update the firmware.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Ensure the update package is not damaged and retry.
2. Ensure proper connection to USB/network drive and retry.
3. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
4. Use the BMC or OneCLI tools to perform the update.
5. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMUP0208M: Failed to execute reboot BMC command.

Severity Error

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Reset the BMC and the host system via the BMC Web Console or AC reset (power off, power on AC).
2. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMVD0001H: Failed to get VPD data.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Press "Back" button and press "Update VPD" button again.
2. If step 1 is unsuccessful, perform AC reset.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMVD0002H: Failed to update the VPD data.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Press "Update" button on VPD update page.
2. If step 1 is unsuccessful, perform AC reset.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMVD0003I: Update VPD data successfully.

Severity Informational

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Information only; no action is required.

FQXPMVD0011K: Failed to get the TPM/TCM policy status.

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Press "Back" button and press "Update VPD..." button again.
2. If step 1 is unsuccessful, perform AC reset.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

FQXPMVD0012K: Failed to set the TPM/TCM policy

Severity Warning

Audit Log TRUE

Automatically Notify Support

User Response Procedure

Complete these steps:

1. Press "Apply" button on VPD update page.
2. If step 1 is unsuccessful, perform AC reset.
3. If error recurs, contact Support.

Note: When performing AC reset, after powering off AC, wait several seconds before powering on AC. After AC power is restored, power on the host system.

Appendix A. Glossary of Terms

Term	Definition
ACM	Authenticated Code Mode
AP	Application Processor
ASU	Advanced Settings Utility
ATA	Advanced Technology Attachment
BEL	Named after Alexander Graham Bell, a logarithmic unit expressing magnitude of change in level of power, voltage, current, or sound intensity. A decibel (dB), 1/10 bel (B), measures relative power.
BMC	Baseboard Management Controller
BIOS	Basic Input/Output System
BIST	Built-in Self-Test
BSP	Boot Strap Processor. (The processor selected at boot time to be the primary processor in a multi-processor system.)
CIFS	Common Internet File System
CIM	Common Information Model
CLI	Command Line Interface
CMM	Chassis Management Module
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit
DC	Direct Current (current flows in one direction)
DC-PG	Direct Current - Power Good. See also DC.
DDNS	Dynamic Domain Name Server
DDR	Double-Data Rate
DDR4	Double-Data Rate 4. See also DDR.
DER	Distinguished Encoding Rules (This method for encoding a data object includes public key infrastructure certificates and keys).
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module (This plug-in memory module has signal and power pins on both sides of the internal printed circuit board (front and back)).
DMI	Desktop Management Interface
DNS	Domain Name Server
DOM	Disk on Module
DOS	Disk Operating System
EDS	External Design Specification
EFI	Extensible Firmware Interface
EI	Enhanced Intel
EIOM	Ethernet I/O Module
EMI	Electromagnetic Interference
EPOW	Early Power-off Warning
FMA	Floating-Point Multiply Add
FP	Front Panel
FPGA	Field-Programmable Gate Arrays
FRU	Field-Replaceable Unit
FW	Firmware
GB	Gigabyte
GPT	Globally Unique Identifier (GUID) Partition Table. See also GUID.

GUI	Graphical User Interface
GUID	Globally Unique Identifier
HCI	Host Controller Interface Specification.
HDD	Hard Disk Drive
HPC	High Performance Computing
HTTPS	Hyper Text Transfer Protocol Service
IFM	Install From Media
IIO	Integrated I/O Module
IMM	Integrated Management Module
IOM	I/O Module
IP	Internet Protocol
IPL	Initial Program Load
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface. A set of computer interface specifications for an autonomous computer subsystem that provides management and monitoring capabilities independently of the host system's CPU, firmware (BIOS or UEFI) and operating system. See also IPMB.
IPIF	Intel® Platform Innovation Framework for EFI architecture
ISA	Instruction Set Architecture
ISTA	International Safe Transit Association
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
LER	Live Error Recovery
LLA	Local Link Address (i.e. IPv6 Link)
LOM	LAN On (Mother) Board
LUN	Logical Unit Number
LXPM	BMC Provisioning Manager
MAC	Media Access Control
MIB	SNMP Alert Management Information Base. See also SNMP.
MISC	Minimum Instruction Set Computer
MSDU	MAC Service Data Unit. See also MAC.
MTM	Mobile Trusted Module
MT/s	Mega Transfers per second
NB	Northbound
NDA	Non-Disclosure Agreement
NFS	Network File System
NIC	Network Interface Card
NM	Node Manager
NMI	Non-Maskable Interrupt
NTB	Non-Transparent Bridge
NTLM	NT LAN Manager. A suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. Replaces the Microsoft LAN Manager (LANMAN) product. See also LAN.
NTP	Network Time Protocol
NVDIMM	Non-Volatile Dual In-Line Memory Module. See also DIMM.
NVPD	Network Vital Product Data
NVMHCI	Non-Volatile Memory Host Controller Interface Specification. See also HCI.

NVRAM	Non-Volatile RAM. See also RAM.
OCP	Overcurrent Protection
OEM	Original Equipment Manufacturer
OFU	One-Boot Flash Update Utility
OLTT	Open Loop Thermal Throttling
OOB	Out of Band
OS	Operating System
PCB	Printed Circuit Board
PCBA	Printed Circuit Board Assembly. See also PCB.
PCH	Platform Controller Hub
PCI	Peripheral Component Interconnect (or PCI Local Bus Standard – also called "Conventional PCI").
PCIe*	Peripheral Component Interconnect Express* (an updated form of PCI offering better throughput and error management). See also PCI.
PCI-SIG*	Peripheral Component Interconnect Special Interest Group. See also PCI.
PCI-X	Peripheral Component Interconnect Extended. See also PCI.
PCT	Platform Confidence Test
PDM	Power Distribution Module.
PDU	Protocol Data Unit
PEF	Platform Event Filter
PEI	Pre-EFI Initialization. Component of Intel® Platform Innovation Framework.
PEIM	PEI Module. See also PEI.
PERR	Parity Error
PFA	Predictive Failure Analysis
PFC	Power Factor Correction
PHM	Processor Heatsink Module
PHSM	Processor Heatsink Module
PIOR	PCIe I/O Riser
POST	Power-on Self-Test (BIOS activity from the time the system is at Power On until the Operating System boot begins.)
PPM	Processor Power Module
PS/2	IBM Personal System/2
PSM	Processor Power Module
PSU	Power Supply Unit
PTU	Power Thermal Utility
PXE	Preboot Execution Environment. Specification which describes a standardized client-server environment that boots a software assembly, retrieved from a network, on PXE-enabled clients.
QPI	Intel® QuickPath Interconnect
QR	Quad Rank (Memory DIMM organization, DRAMs organized in four (4) ranks)
QSFP	Quad Small Form Factor-Pluggable. See also SFF.
RAID	Redundant Array of Independent Disks (This provides data security by spreading data over multiple disk drives. RAID 0, RAID 1, RAID 10, and RAID 5 are different patterns of data on varying numbers of disks to provide varying degrees of security and performance.)
RAM	Random Access Memory
RAS	Reliability, Availability, and Serviceability
RASM	Reliability, Availability, and Serviceability, and Manageability. See also RAS.
RC	Raw Class

RDC	Remote Desktop Connection
RHEL	Red Hat Enterprise Linux
RNDIS	Remote Network Driver Interface Specification
ROC	RAID on Chip. See also RAID.
ROM	Read-Only Memory
RPM	Revolutions Per Minute
RTF	Rich Text Format
SCA	Single Connector Attachment
SDU	Service Data Unit
SEC	Security (Component of Intel® Platform Innovation Framework for EFI architecture).
SEL	System Event Log
SFP	Small Form Factor Pluggable. See also SFF.
SFP+	The enhanced small form-factor pluggable (SFP+) is an enhanced version of the SFP that supports data rates up to 16 GBit/s. See also SFP.
SKLM	Security Key Lifecycle Manager
SKU	Stock-Keeping Unit
SLES	SUSE Linux Enterprise Server
SMM	System Management Module
SMTP	Simple Mail Transfer Protocol
SOL	Serial-over-LAN
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SUP	System Update Package
TCM	Trusted Cryptographic Module
TIM	Thermal Interface Material
TKLM	Tivoli Key Lifecycle Manager
TLS	Transport Layer Security
TPM	Trusted Platform Module
TPS	Technical Product Specification
UEFI	Unified Extensible Firmware Interface
UPI	Intel® UltraPath Interconnect
URL	Uniform Resource Locator
USB	Universal Serial Bus (standard serial expansion bus meant for connecting peripherals)
VID	Voltage Identification
VPD	Vital Product Data
WOL	Wake on LAN
XCC	BMC Controller