IBM

Advanced Management Module

Messages Guide

IBM

Advanced Management Module

Messages Guide

Contents

Chapter 1. Introduction

This documentation provides additional information about event notifications from the advanced management module or messages in the advanced management module event log and the steps that you can take to resolve issues on a BladeCenter chassis.

Most events are informational and do not impact availability. Some events can impact BladeCenter system availability, and these events require action to address and resolve. In addition, events related to a hardware issue can be automatically called home to IBM® through the IBM BladeCenter Service Advisor, which is built into the advanced management module, if enabled. This built-in automated call-home capability ensures that IBM is immediately notified of a hardware failure, even in the middle of the night, and a replacement part is sent to resolve the issue.

Note: The advanced management module is the latest version of the original BladeCenter management module. The newer versions of the advanced management module reports the Event ID in the event log and provides service data collection. In addition, Service Advisor is not supported on the management module. This document does not directly apply to the management module; however, many of the events and the recommended user actions for those events are similar.

Some events might appear to be caused by a hardware issue but are not called home. For those events, additional problem determination is required to determine the source of the issue before it can be resolved. In many cases, issues that might at first appear to be due to hardware problems might actually the result of usage errors, code issues, or configuration. When you install new components in a BladeCenter chassis, consider updating the firmware of that component to the latest available levels to reduce issues that might be related to firmware.

Firmware for the BladeCenter chassis and its components is available at the Software and downloads Web site at: http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-63017 &brandind=5000020.

Information about component compatibility and interoperability within a BladeCenter chassis can be found at the ServerProven Web site at: http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html

Using this information

If you receive an event through the event log or through notifications, such as e-mail or SNMP, you can look up the event ID in Chapter 2, "Messages," on page 25 to determine the actions that should be taken, if any action is required.

The advanced management module

The advanced management module provides system-management functions and keyboard/video/mouse (KVM) switching for all of the blade servers in a BladeCenter chassis that support KVM. It supports the external keyboard, mouse, and video connections, for use by a local console, and a 10/100 Mbps Ethernet remote management connection.

Each BladeCenter chassis comes with at least one advanced management module. Most BladeCenter chassis support the installation of a second, redundant advanced management module. Only one advanced management module can control the BladeCenter system at a time. It is identified as the *primary*. The advanced management module that is not active is identified as the *standby*. The primary advanced management module can be detected visually by the Active LED on the management indicator panel or through the advanced management module Web interface.

Note: Do not install an advanced management module and a management module in the same BladeCenter chassis.

The firmware level on the standby advanced management module is automatically updated from the primary advanced management module. Verify they are the same firmware level from within the advanced management module Web interface before attempting to manually switch over to the standby. If the active advanced management module should fail, the standby advanced management module will automatically take over management functions of the chassis. If the standby advanced management module should fail, the primary advanced management module will record the failure and disable automatic failover.

The standby advanced management module can be put on the network using advanced failover settings, but it only provides enough function to ping and take over for the active advanced management module using the web interface if there is an error.

The advanced management module does not provide notification of a failover. However, it does provide notification when the primary and standby advanced management modules are established, such as when a failover occurs. For example, these events can be seen in the event log:
- 0x06000201 Management Module in bay 1 is primary.
- 0x06000202 Management Module in bay 2 is primary.
- 0x06000301 Management Module in bay 1 is standby.
- 0x06000302 Management Module in bay 2 is standby.

Status and problems on the standby advanced management module are available on the active advanced management module. Notifications and status are only available from the active advanced management module.

In addition to the advanced management module event log, use the information from I/O module logs and operating system logs on the blade servers to help isolate issues. These logs are not available through the advanced management module.

The BC T and BC HT advanced management module

The advanced management module that is installed in the BladeCenter T and BladeCenter HT chassis differ from the advanced management module that is installed in the other BladeCenter chassis in that it has firmware specifically designed to support these ruggedized, NEBS-3/ETSI-compliant chassis.

The BladeCenter T chassis has a unique profile that makes it ideal for rugged and telecommunications industry uses. The BladeCenter T advanced management module provides a different physical form than the advanced management module, but the firmware functionality is nearly identical.

The BladeCenter T advanced management module is sometimes referred to as the *Chassis Management Module 2* (CMM2) and is made in a different form factor than the other advanced management modules.

Each event generated by the advanced management module has a severity assigned to it. The same severities are assigned to events in the BladeCenter T and the BladeCenter HT chassis, but they are slightly different for other chassis.

The BladeCenter T and BladeCenter HT chassis provide an alarm panel (sometimes referred to as *alarm manager*) on the front of the media tray,. This is also visible from the advanced management module Web interface and command-line interface (CLI). The BladeCenter T and BladeCenter HT advanced management module support additional severities of Major and Minor, which are shown in the alarm panel and in SNMP traps

The following table shows event severities for each of the BladeCenter chassis:

Table 1. Event severities for each of the BladeCenter chassis

BladeCenter T chassis	BladeCenter HT chassis	All other BladeCenter chassis	Displayed in the event log (all chassis)
Critical	Critical	Critical	Error
Major	Major	Critical	Error
Minor	Minor	Warning or System	Warning
Informational	Informational	Informational	Informational

Terminology

The following terminology is used in this documentation.

alarm   Alarms are a signal for attention, often used interchangeably with alerts. In addition, alerts can also mean an indication from an LED, such as from the alarm panel on the BladeCenter T chassis.

alert   Alerts provide notification of an event on the advanced management module. These notifications can be in the form of Director events, e-mail, or Simple Network Management Protocol (SNMP) traps.

command-line interface
The IBM BladeCenter advanced management-module command-line interface (CLI) provides direct access to BladeCenter management functions as an alternative to using the Web-based interface. Use the command-line interface to issue commands to control the power and configuration of the management module and other components that are in a BladeCenter chassis.

event   Events are internal entities that have an event number and a structured format that may allow notification.

group   In an event description, denotes one or more components. For example, there may be a memory group, which consists of one or more memory DIMMs.

IPMI   Intelligent Platform Management Interface (IPMI) is a specification that defines the interfaces used by system administrators to manage a system. IPMI is used to provide information between the service processor on the blade server and the advanced management module.

management module
A management module is a hot-swap module that you use to configure and manage all installed BladeCenter components. There are three types of management modules:
- Management module. This is the management module that was provided when BladeCenter products were first introduced.
- Advanced management module. The advanced management module replaced the management module. It is available for the BladeCenter E, BladeCenter H, and BladeCenter S chassis.
- Chassis management module. The original management module for the BladeCenter T chassis is called the chassis management module. The chassis management module 2 is the advanced management module version for the BladeCenter T chassis.

service processor
Generic term for baseboard management controllers (BMC), Integrated System Management Processors (ISMP), and Advanced System Management (ASM) processors. These hardware-based management processors monitor system platform events such as fan failures and temperature or voltage increases, and logs their occurrence. They are also used for hardware control, such as powering the node on and off.

SNMP trap

A Simple Network Management Protocol (SNMP) trap is a message which is initiated by a network element (advanced management module or agent) and sent to the network management system (SNMP user).

VPD   Vital product data (VPD) is stored on each component in a BladeCenter chassis and is available through the advanced management module. VPD includes information about the component, such as product specifications, firmware versions, part numbers and serial numbers.

Abbreviations

The following abbreviations are used in this documentation.

- AC. Alternating Current (electricity)
- A/D. Analog-to-Digital
- AMM. Advanced Management Module
- BEM. Blade Expansion Module
- BIOS. Basic Input/Output System
- BIST. Built-In Self Test
- BSE. Blade Storage Expansion
- BSMP. Blade Service Management Processor (generic term for service processor BMC or FSP)
- CA. Certificate Authority (encryption)
- CIN. Chassis Internal Network
- CPU. Central Processing Unit
- CRC. Cyclic Redundancy Check
- DASD. Direct Access Storage Device
- DC. Direct Current (electricity)
- DHCP. Dynamic Host Configuration Protocol
- DIMM. Dual In-line Memory Module
- DNS. Domain Name Server/Service
- FRU. Field Replaceable Unit
- FTP. File Transfer Protocol
- FW. Firmware
- HTTP. Hypertext Transfer Protocol (web)
- I/O. Input/Output
- IOM. I/O Module
- IP. Internet Protocol
- IPMB. Intelligent Platform Management Bus (server system bus)
- KVM. Keyboard Video Mouse
- LDAP. Lightweight Directory Access Protocol (active directory)
- LAN. Local Area Network
- LED. Light-Emitting Diode
- MAC. Machine Address Code
- MIB. Management Information Base
- MM. Management Module
- MT. Media Tray
- MTU. Maximum Transmission Unit
- NAT. Network Address Translation
- NEBS. Network Equipment Building System/Standards (telecommunications)

- NMI. Non-Maskable Interrupt
- NTP. Network Time Protocol
- OID. Object Identifier
- OS. Operating System
- PCI. Peripheral Component Interconnect (bus)
- PFA. Predictive Failure Analysis
- POST. Power-On Self Test
- PXE. Preboot eXecution Environment (network boot)
- RAID. Redundant Array of Inexpensive Disks
- RAM. Random-Access Memory
- SDR. Sensor Data Record
- SEL. System Event Log
- SLP. Service Location Protocol
- SMASH. Systems Management Architecture for Server Hardware
- SM BIOS. System Management Basic Input/Output System
- SMTP. Simple Mail Transfer Protocol (e-mail)
- SNMP. Simple Network Management Protocol
- SSH. Secure Shell
- SSL. Secure Sockets Layer (web security protocol)
- TCP. Transmission Control Protocol
- TFTP. Trivial File Transfer Protocol
- VPD. Vital Product Data
- XML. eXtensible Markup Language

IBM BladeCenter Service Advisor

IBM BladeCenter Service Advisor provides a method to notify authorized service and support representatives on selected issues.

When a serviceable event that has been designated as a call home event is detected, a message is written in the event log and any configured alerts will be sent. The information gathered by Service Advisor is the same information that is available if you save service data from the advanced management module Web interface.

After gathering the information, Service Advisor automatically initiates a call to IBM. Upon receipt of the information, IBM returns a service request ID, which is placed in the call home activity log.

On the Event Log page of the advanced management module Web interface, you can choose to select the Display Call Home Flag checkbox. If you select the checkbox, events are marked with a C for call home events and an N for events that are not called home. In addition, you can filter the event log based on this setting.

Troubleshooting BladeCenter issues

Developing a general understanding of power and thermal (temperature) issues can help to quickly diagnose problems.

Troubleshooting power issues

Properly configured BladeCenter chassis provide power redundancy by supplying power to each chassis component from two or more power modules. BladeCenter chassis are connected to either AC current or DC current.

Note: (DC Current) Only trained service personnel, other than IBM service technicians, are authorized to make the connections to and disconnections from the -48 volt DC power source. IBM service technicians are not certified or authorized to install or remove the -48 volt power cable. The customer is responsible for ensuring that only trained service personnel install or remove the -48 volt power cable.

All AC current chassis except the BCS require 220 Volt AC input. The BCS chassis has auto sensing power modules which can be connected to either 110 Volt or 220 Volt AC power. Do not mix input voltages on a BCS chassis.

Each AC power module has an AC (in) and DC (out) power LED. The AC (in) power LED will be illuminated when the power module is properly connected to a power source. If the AC (in) power LED is not illuminated, inspect the complete path from the actual power source to the power module. Verify functionality of all components including the circuit breakers, wall or floor power outlets, Power Distribution Units (PDU), and power cables. Power cable specifications depend on the chassis type/model and vary in the number and style of connectors.

Note: Every power cord must be connected to a power source.

Configurations may include redundant power sources to a single chassis. AC power modules convert the AC input current to DC output current. The DC (out) power LED will be illuminated when the power module is distributing DC power to the chassis midplane. If it is not illuminated:

1. Remove AC power cable from the power source.
2. Remove and visually inspect the connections on the power module and the chassis.
3. Reseat the power module and reconnect the power cable at the source.

Further troubleshooting should be performed by IBM service technicians.

Some power modules also have a Fault LED. Verify the power input configuration before replacing a power module with an illuminated Fault LED.

Note: Before removing AC power from a power module or removing a power module from the chassis, verify that the capacity of the remaining power modules are sufficient to meet the minimum power requirements for all installed components

View power status and requirements in the advanced management module. Basic problem determination should include swapping suspect bad power cables/sources/power modules with known good units for verification whenever possible. The advanced management module polls the power modules over multiple I^{2}C busses. Details such as power module status, available power and all relevant hardware and firmware VPD can be viewed from the advanced management module.

The advanced management module has configurable power management policy settings. Power policy options vary by chassis type/model. Power policies are selected based on configuration specifics such as installed power modules, actual and estimated power consumption, the number and type of power sources, and the production roles of the blades servers. Power management policies primarily control how blade servers react to changes in available power, i.e. situations such as the loss of a power module or power source.

Note: The most restrictive power policy combined with certain chassis configurations may limit the number of blade servers allowed to power on. For more information about power management policies, see the Help section within the advanced management module or the *IBM BladeCenter Advanced Management Module User's Guide*.

Troubleshooting blade server processors throttling

Most current blade servers support the ability to reduce the power consumption of their processors when needed (throttling). The advanced management module does not throttle blade servers. The advanced management module can provide a policy setting to blade server service processors to reduce power consumption, reduce heat output, or reduce acoustic noise.

A fan or blower failure can cause processors to throttle to prevent overheating. Loss of a power module or power source may cause the processors to throttle due to reduced overall available power. There is a selectable "Acoustic Mode" setting in the advanced management module that can throttle processors when thermal conditions exist that would otherwise increase the blower/fan speed. When Acoustic Mode is enabled, processor performance may be reduced in order to minimize blower/fan noise

Troubleshooting thermal issues

The advanced management module provides status and alerts for temperature sensors throughout the chassis. Some sensors provide an actual temperature and others provide only a notification of whether a threshold has been exceeded. The advanced management module adjusts the speed of cooling devices (blowers and fans) based on the environmental conditions and threshold indications.

The main ambient temperature sensor is located in the media tray. Therefore, removing the media tray will cause the blowers/fans to run at a maximum speed. If the advanced management module cannot read the temperature sensor, it will operate as if the temperature is at the peak operational value and all components in the chassis require maximum cooling.

Other temperature sensors are located near the CPU modules in the blade servers. The CPU temperature sensors are compared against a warning and a critical temperature limit. If the CPU temperature exceeds the warning limit specified for that blade, a temperature warning event will be posted and the chassis blowers will increase in speed to correct the temperature condition. If the CPU temperature exceeds the critical limit, then the blade will be shut off. The CPU temperature sensors can be checked by clicking on the status indicator next to each blade server listed on the System Status page through the advanced management module Web interface.

Temperature warning events are recorded in the event log. They are available through e-mail notifications, SNMP traps, and IBM Director alerts, if enabled.

The following conditions can cause thermal errors:
- The ambient temperature in the environment is hot, which could be due to problems with air conditioning.
- The intake vents in the front of the chassis are obstructed.
- The air filter on the chassis needs cleaning.
- A heat sink on a blade server CPU is loose or needs thermal grease correctly applied.
- A fan module or blower module has failed or has been removed
- Bays on the chassis are empty, which prevents normal front-to-back air flow. A filler or component should always be installed in each bay in a chassis.
- A thermal sensor is faulty.

Thermal conditions tend to develop gradually (with the exception of heat sink problems). You can view and compare the temperatures and temperature sensors for various components in the BladeCenter

chassis. The advanced management module thermal sensor, located at the rear of a chassis, is expected to report slightly higher temperatures than the ambient sensor located in front of the chassis in the media tray.

A thermal sensor could be faulty if the advanced management module posts a thermal warning or maintains the blower/fan speeds at maximum RPMs immediately after power is applied to the chassis or after a specific blade server is powered up. It is normal for the chassis blowers to increase their speed immediately after power is applied to the chassis or the advanced management module is reset. However the blowers speed should be reduced within two minutes if ambient temperature conditions are good and if all temperature sensors are working as expected.

A blade with a faulty heat sink connection to a CPU might show a temperature increase within seconds after powering up the blade server. One way to determine if the temperature increase is due to a faulty heat sink, a faulty temperature sensor, chassis air flow, or an ambient air temperature problem is to monitor the blade server CPU temperature through the advanced management module Web interface while powering up the blade server.

If the blade server has two CPU modules installed, the temperature for both modules should rise at about the same rate under the same stress. If the temperature reading for one CPU module rises much faster than the other module, the heat sink for that CPU module might not be installed correctly. If both CPU module temperatures rise at about the same rate to warning or critical limits, there might be a problem with chassis air flow or ambient temperature.

Troubleshooting SAS RAID controller module issues

The BladeCenter S chassis is the first BladeCenter chassis to provide integrated hard drives within the chassis that can be shared by all blade servers within the chassis.

You must install the following to take advantage of this capability:
- Two SAS RAID controller modules must be installed, one in I/O module bay 3 and one in I/O module bay 4. The SAS RAID controller module provides integrated SAS switch and RAID controller capability.
- A SAS expansion card option must be installed in each blade server that will access the integrated shared storage.
- SAS hard disk drives must be installed in the storage modules. SATA hard disk drives are not supported.
- Both battery backup units must be installed in the bays in the media tray.

For additional information about the SAS RAID controller module, see the *SAS RAID Controller Module Installation and User's Guide*.

Problem Determination capabilities are built into the SAS RAID controller and connected back through the advanced management module to provide a more unified system structure. SAS RAID controller module alerts are mapped to the advanced management module events. If appropriate, these alerts can also generate a call home.

For rapid problem determination and resolution, the SAS RAID controller module maintains its own set of alerts in an active alert list based on the events and configuration in the RAID controller.

Typically, alerts that require user intervention will turn on the Information LED on the SAS RAID controller module. The active alert list, the alert history log, and the user's guide provide necessary information for problem analysis and resolution. In addition, the SAS RAID controller module provides its own independent alerting, such as e-mail notification.

If you see an event related to the SAS RAID controller module through the advanced management module, you can log in to the SAS RAID controller module interface (or use Storage Configuration Manager) to obtain more information.

Diagnostic tools

There are several tools available to help you diagnose and solve hardware related issues.

Service Data tool

Use the advanced management module service data tool to collect information for analysis by IBM service personnel. To access the service data tool from the advanced management module Web interface, click **Service Tools** > **AMM Service Data**.

Light path diagnostic LEDs

Light path diagnostic LEDs are a system of LEDs on the BladeCenter chassis and components within the chassis that can be used to identify system errors. If the front or rear system error LED on a BladeCenter chassis is lit, one or more error LEDs on a component also might be lit.

LEDs on the chassis may be viewed remotely from the advanced management module Web interface. The advanced management module also provides the ability to view the LEDs internal to the blade server.

Note: The System LED panel is displayed in a different locations on different chassis types, but the function of each of the LEDs is similar.

The following System LEDs are displayed:

Power-on
> This green LED is lit when there is power coming to the chassis midplane.

Location
> This blue LED is lit (solid or flashing) to indicate the location of the chassis.

Over-temperature
> This amber LED is lit (solid) to indicate that the system temperature has exceeded a threshold level, or that one or more components within the chassis have exceeded an over-temperature threshold.

Information
> This amber LED is lit (solid) to indicate that noncritical event has occurred. The information LED for one or more components in the chassis, such as an I/O module, will also be lit.

System error
> This amber LED is lit (solid) to indicate that a critical system error has occurred. This LED is lit for the following conditions:
> * When messages with a severity of error or critical are generated
> * When the fault LED on a component within the chassis is lit

For example, on a BladeCenter S chassis, the following system LEDs are displayed on the media tray:
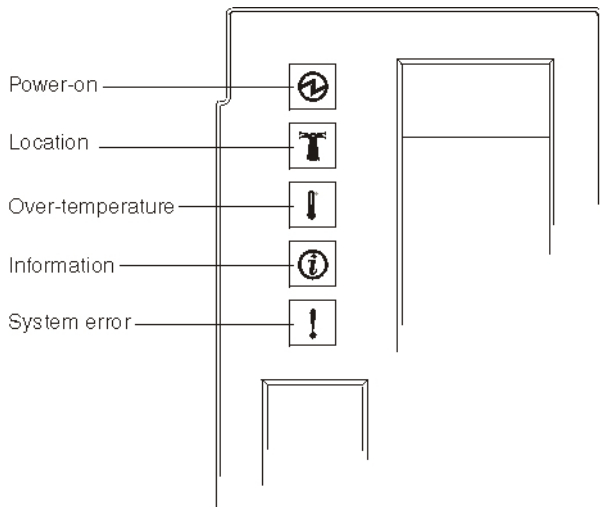
View the system LEDs remotely through the advanced management module Web interface. The main LED page shows the external LEDs on the chassis panels and the front panel. The internal blade LEDs are also available through a blade hyperlink from the LED page. This enables you to see the status of the internal LEDs on the blade server without having to turn off the blade server, remove it from the chassis, and activate the light path indications.

The chassis LEDs indicate the status of the components in the chassis. For example, if the error, information, temperature, or location LED is lit for a blade server, the same LED will be lit on the system LED panel for the chassis. The information and location LEDs can also be turned off remotely, but you might need to turn off the LED on the blade for the request to be accepted.

Light path diagnostic LEDs - BladeCenter T and BladeCenter HT chassis

The system LEDs are displayed on the media tray.
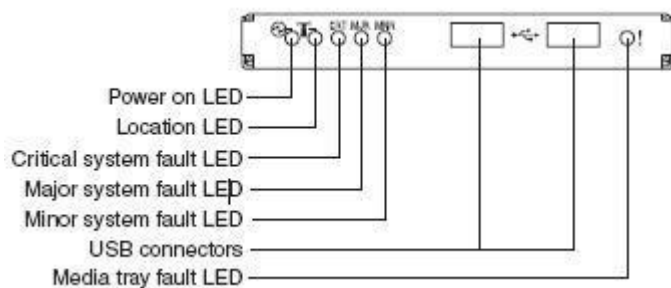
The following system LEDs are displayed:

Power-on
> When this green LED is lit, power is present in the BladeCenter HT unit. When this LED is off, the power subsystem, the power module, or the LED has failed.

Attention
> If the power-on LED is off, it does not mean that electrical current is not present in the BladeCenter HT unit. The LED might be defective. To remove all electrical current from the BladeCenter HT chassis, you must disconnect all power cords from all power input connectors.

Location
> When this blue LED is lit or flashing, it has been turned on by the system administrator to aid in visually locating the BladeCenter HT unit. If a blade server requires attention, the location LED on the blade server usually will also be lit. After the BladeCenter HT unit has been located, the system administrator turns off the location LED.

Critical system fault
> When this LED is lit, the BladeCenter HT chassis has a critical system fault. A critical system fault is an error or event that is detected by the system with a significant impact to the system. In this case, the system cannot continue to operate or is operating in a non-redundant power configuration or a non-redundant cooling configuration.
>
> **Note:** The color of this LED can be set to amber or red through the management module.

Major system fault
> When this LED is lit, the BladeCenter HT unit has a major system fault. The system can continue to operate but might lose some function and performance.
>
> **Note:** The color of this LED can be set to amber or red through the management module.

Minor system fault
> When this amber LED is lit, the BladeCenter HT unit has a minor system fault. The system can continue to operate, usually without noticeable loss of functionality or performance.

Media tray fault
> When this amber LED is lit, there is a fault on the media tray. The system can continue to operate, usually without the use of the components on the media tray.

LEDs for remote chassis

To quickly find LED status on other chassis on the same subnet, you can view the remote chassis, if Service Location Protocol (SLP) is enabled. From the advanced management module Web interface, click **Monitors** > **Remote Chassis**.

You can view the advanced management modules and the management modules, including firmware versions, in the same datacenter (up to 500). In addition, you can link to other advanced management module from this page as well.

Note: The management module does not support viewing the status, but later versions did provide health (status) and firmware versions.

Advanced management module event messages

There are several ways to view events that are generated by the advanced management module.

The system status summary

You can access a list of outstanding events that require immediate attention, and the overall status of each of the blade servers and other components in the BladeCenter chassis.

To access the system status summary page from the advanced management module Web interface, click **Monitors** > **System Status**. The following figure shows an example of the System Status Summary page.

Figure 1. System Status Summary page

If you are using a BladeCenter HT or a BladeCenter T chassis, the system status page also displays active alarm conditions that are grouped by alarm type (critical, major, or minor). Critical, major, and minor alarms light the LED associated with their alarm level on the BladeCenter T unit. Acknowledging an alarm moves it from the critical, major, or minor active list to the acknowledged list and turns off its LED. Clearing an alarm removes it from all alarm lists and turns off its LED. Acknowledging or clearing an alarm only turns off its LED when there are no other alarms of the same level that are active to keep the LED turned on.

The following figure shows the System Status Summary page for the BladeCenter T and BladeCenter HT chassis.

Figure 2. System Status Summary page - BladeCenter T and BladeCenter HT chassis

The event log

Access the event log through the advanced management module Web interface or through the advanced management module command-line interface (CLI), SNMP, and SMASH.

The most recent events are displayed first in the event log. The following shows an example of the way events are displayed in the event log through the Web interface:

Index	Sev	Source	Date/Time	Serv	Event ID	Text
1	I	Audit	08/13/08, 11:21:25	U	0x0000007a	Remote login successful for user 'toms' from Web at IP 9.44.113.85
2	I	SERVPROC	08/13/08, 11:21:11	U	0x00016001	Management module network initialization complete
3	I	SERVPROC	08/13/08, 11:21:04	U	0x06000201	Management Module in bay 1 is primary.

The advanced management module has a monitor log function, which can be enabled or disabled from the Event Log page of the advanced management module Web interface. If enabled, the monitor log function alerts users when the event log is 75 percent full and again when the log is completely full. In older versions of the advance management module firmware, these events might also cause the Informational LED to be lit.

To turn off the log full status, clear the log from the Event Log page of the advanced management module Web interface. Scroll to the bottom of the event log to clear log entries.

Note: When the event log is full, new events continue to be added, the oldest events in the log are deleted.

E-mail notification

The advanced management module can be configured to send e-mail to users when an alert occurs. You can also select the severity and types of alerts that are generated.

The following figure shows an example of the e-mail generated if a user is configured to receive critical alerts for chassis cooling devices.

Subject: Non-Critical Alert from test_board
Alert Text: Event log full

Type of Alert: Non-Critical
Severity: 2
Application ID: ServProc
Application Alert Type: 07
Event ID:0x0000006b
Log Source:SERVPROC
Date(m/d/y): 08/11/08
Time(h:m:s): 12:56:00

Contact: No Contact Configured
Location: No Location Configured

BladeCenter MM Name: test_board
BladeCenter Serial Number:
BladeCenter UUID: 07A3284990D2893F40224195720A145
BladeCenter Machine Type/Module:
Call Home Flag: N
AMM IP Address: 9.123.253.66

Figure 3. E-mail notification

For more information about configuring e-mail alerts from the advanced management module Web interface, see the *Advanced Management Module User's Guide*. For more information about configuring e-mail alerts from the advanced management module command-line interface (CLI), see the *Advanced Management Module Command-Line Interface Reference Guide*.

SNMP traps

Simple Network Management Protocol (SNMP) is a set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

An SNMP trap is a message which is initiated by a network element (the advanced management module) and sent to the network management system (SNMP user). You can configure SNMP agents and traps, and you can determine where those traps are sent.

Note: If you plan to configure Simple Network Management Protocol (SNMP) traps on the management module, you might need to install and compile the management information base (MIB) on your SNMP manager. The MIB supports SNMP traps. The MIB is included in the management-module firmware update package from the IBM BladeCenter software and device drivers Web site athttp://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-63017&brandind=5000020.

The following example shows an example of an SNMP alert.

Note: In SNMP alerts, the event identifier is displayed as a decimal (spTrapEvtname). You will need to convert that decimal number into a hexadecimal number to map it to the event identifier for the event displayed in Chapter 2, "Messages," on page 25.

```
Binding #1: spTrapDateTime *** (octets) Date(m/d/y)=08/11/08, Time(h:m:s)=12:56:00
Binding #2: spTrapAppId *** (octets) BladeCenter Advanced Management Module
Binding #3: spTrapSpTxtId *** (octets) test_board
Binding #4: spTrapSysUuid *** (octets) 07A3284990D2893F40224195720A145
Binding #5: spTrapSysSern *** (octets) (zero-length)
Binding #6: spTrapAppType *** (int32) 7
Binding #7: spTrapPriority *** (int32) 2
Binding #8: spTrapMsgText *** (octets) Event log full
Binding #9: spTrapHostContact *** (octets) No Contact Configured
Binding #10: spTrapHostLocation *** (octets) No Location Configured
Binding #11: spTrapBladeName *** (octets) (zero-length)
Binding #12: spTrapBladeSern *** (octets) (zero-length)
Binding #13: spTrapBladeUuid *** (octets) (zero-length)
Binding #14: spTrapEvtName *** (gauge32) 107
Binding #15: spTrapSourceId *** (octets) SERVPROC
Binding #16: spTrapCallHomeFlag *** (gauge32) 0
Binding #17: spTrapSysIPAddress *** (octets) 9.123.253.66
Binding #18: spTrapSysMachineModel *** (octets) (zero-length)
Binding #19: spTrapBladeMachineModel *** (octets) (zero-length)
```

Figure 4. Example of an SNMP alert

For more information about configuring SNMP from the advanced management module Web interface, see the *Advanced Management Module User's Guide*. For more information about configuring SNMP from the advanced management module command-line interface (CLI), see the *Advanced Management Module Command-Line Interface Reference Guide*.

Syslog

The syslog protocol provides a method for the advanced management module to send event log messages in a standard, RFC 3164-compliant format via the network to up to two syslog collectors. This is useful since the advanced management module event log has a limited capacity and wraps once it is full, overwriting the oldest entries. By configuring syslog collectors, you will prevent the loss of any event history.

The advanced management module syslog service is disabled by default. You can enable it and configure the syslog collectors by specifying their IP addresses/host names, and port numbers (the default port number is 514). The advanced management module also provides the ability to filter the transmitted log messages by minimum severity level for all targets.

For more information about configuring syslog from the advanced management module Web interface, see the *Advanced Management Module User's Guide*. For more information about configuring syslog from the advanced management module command-line interface (CLI), see the *Advanced Management Module Command-Line Interface Reference Guide*.

IBM Director

If you are using IBM Director for systems management, you can configure the advanced management module to send events to IBM Director.

IBM Director is IBM's systems management product. Through the remote connection on the advanced management module, you can use IBM Director on a management console to configure your chassis, modify the configuration, and set up more advanced features.

If you are using IBM Director for systems management, it will automatically discover the BladeCenter chassis and receive events from the advanced management module.

For more information about IBM Director, go to the IBM Director Web site at: http://www.ibm.com/
systems/management/director/

Service bulletins

IBM continually updates the support Web site with tips and techniques that you can use to resolve many
issues that you may be having with your BladeCenter system.

To find the latest service bulletins that are available for the advanced management module, go to the
BladeCenter support search Web site athttp://www.ibm.com/systems/support/supportsite.wss/
dosearch?q=advanced+managment+module+retain&search.x=1&search=Search&brandind=5000020
&taskind=0%7CAll+tasks&familyind=0%7CAll+Product+Families&typeind=&osind=&oldfamily=0. In the
Search field, enter the following terms: advanced, management, module, and retain.

In addition, service bulletins have been generated for many of the events that are described in Chapter 2,
"Messages," on page 25. If you perform the recommended actions, but you are still having trouble,
consider searching the BladeCenter support site for service bulletins that might be related to your issue.

IBM Dynamic System Analysis (DSA)

IBM Dynamic System Analysis (DSA) collects and analyzes system information to aid in diagnosing
system problems related to blade servers. DSA collects information about a blade server, such as system
configuration, installed applications, device drivers, and hardware inventory.

Additionally, DSA creates a merged log that allows users to easily identify cause-and-effect relationships
from different log sources in the system.

For more information about DSA, go to the DSA Web site at: http://www.ibm.com/systems/support/
supportsite.wss/docdisplay?brandind=5000008&lndocid=SERV-DSA

Run Dynamic System Analysis (DSA) to collect information about the hardware, firmware, software, and
operating system. Have this information available when you contact IBM or an approved warranty
service provider. For instructions for running the DSA program, see http://publib.boulder.ibm.com/
infocenter/toolsctr/v1r0/topic/dsa/dsa_t_collecting_inventory_data.html or complete the following steps:

1. Go to http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp.
2. In the navigation pane, click **IBM System x and BladeCenter Tools Center**.
3. Click **Diagnostics** > **Dynamic System Analysis** > **Collecting system information**.

If you have to download the latest version of DSA, go to DSA Web site or complete the following steps.

Note: Changes are made periodically to the IBM Web site. The actual procedure might vary slightly from
what is described in this document.

1. Go to http://www.ibm.com/systems/support/.
2. Under **Product support**, click **BladeCenter**.
3. Under **Popular links**, click **Software and device drivers**.
4. Under **Related downloads**, click **Dynamic System Analysis (DSA)**.

For information about DSA command-line options, see http://publib.boulder.ibm.com/infocenter/
toolsctr/v1r0/topic/dsa/dsa_r_commands.html or complete the following steps:

1. Go to http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp.
2. In the navigation pane, click **IBM System x and BladeCenter Tools Center**.
3. Click **Diagnostics** > **Dynamic System Analysis** > **Reference** > **Commands**.

Fields displayed for a message

In this documentation, the following fields are displayed for each message:

Event identifier

A hexadecimal identifier that uniquely identifies an event or class of events. In this documentation, the event identifiers are prefixed with 0x and followed by eight characters. In Chapter 2, the events are ordered by event identifier.

Event identifiers can be seen in the event log and in notifications (e-mails and SNMP alerts).

Note: In SNMP alerts, the event identifier is displayed as a decimal number. You will need to convert that integer into a hexadecimal number to map it to the event displayed in Chapter 2, "Messages," on page 25.

Event description

The logged message string that appears for an event.

In many cases, the logged message string that appears in this document is slightly different from the event string that appears in the event log.

When the event string is displayed in the event log, information such as the user ID, or the specific blade server bay number, is displayed. In this document, that additional information appears as follows:

- %d – this is replaced by a number (typically for bay number for a blade server or an I/O module)
- %s – this is replaced by a string (typically a user ID)
- %% - this is replaced by the percent sign (%)

For example, consider the event 0x06000201:

`0x06000201 Management Module in bay %d is primary.`

In the event log, the %d is replaced with the management module bay number:

`0x06000201 Management Module in bay 1 is primary.`

The logged message string might have additional information added to the beginning or end of the message. Consider the event 0x806F0229:

`0x806F0229 absent`

In the event log, the logged message string is replaced with additional information:

`0x806F0229 Battery 1 (Battery Status) absent.`

Related messages

If present, this section lists event identifiers and descriptions for events that are related to this event. The events listed in this section all have the same explanation and user response, but are for a different component number, such as a blade server bay number.

Explanation

Provides additional information to assist the user in understanding the reason why the event occurred.

Severity

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

Table 2. Severity levels

Severity	Description
Informational	An informational message is something that was recorded for audit purposes, usually a user action or a change of states that are normal behavior.

Table 2. Severity levels (continued)

Severity	Description
Warning	A warning is not as severe as an error, but if possible, the condition should be corrected before it becomes an error. It may also be a condition that requires additional monitoring or maintenance.
Error	An error typically indicates a failure or critical condition that impairs service or an expected function. **Note:** In the Alert Category field, events with a severity of Error are shown as a severity of Critical.

Alert Category

Similar events are grouped together in categories. Information in the alert category field is displayed in the following format:

component (*severity*) – *trap_category*

where:

component

Events are grouped into the following component categories:

Note: These categories are based on the enhanced alert categories.
- Blades
- Chassis/System Management
- Cooling Devices
- I/O Modules
- Inventory
- Network change
- Power Modules
- Power On/Off

In addition, the following categories are available:
- Event log. Events related to the event log. For example, if the field Monitor log state events is enabled on the Event log page of the advanced management module Web interface, events related to the log being 75% full and the log being 100% full are listed for this category.
- User activity. Audit related events, such as when a user logs in to the advanced management module Web interface.

severity

Events are also grouped into the following severity levels:
- Informational
- Warning
- Critical

Note: The severity Critical for the Alert Category field is the same as the severity Error in the Severity field.

Even though these severities are not used on the BladeCenter T and BladeCenter HT for alerts, they are used for those chassis to create alert categories.

trap_category

The trap category found in the SNMP alert management information base (MIB).

SNMP users will be notified of the alerts in the event categories via an SNMP trap. The traps are defined in mmalert.mib, which is distributed with the advanced management module firmware. The following table shows the MIB Object and the Object Identifier (OID) for the selected alert category:

Enhanced Alert Categories	MIB Object	OID
Critical/Error		
Chassis/System Management (Critical)	mmTrapChassisC	.1.3.6.1.4.1.2.6.158.3.0.130
Cooling Devices (Critical)	mmTrapFanC	.1.3.6.1.4.1.2.6.158.3.0.133
Power Modules (Critical)	mmTrapPsC	.1.3.6.1.4.1.2.6.158.3.0.4
Blades (Critical)	mmTrapBladeC	.1.3.6.1.4.1.2.6.158.3.0.128
I/O Modules (Critical)	mmTrapIOC	.1.3.6.1.4.1.2.6.158.3.0.129
Storage Modules (Critical)	mmTrapStorageC	.1.3.6.1.4.1.2.6.158.3.0.131
NonCritical/Warning		
Chassis/System Management (Warning)	mmTrapChassisN	.1.3.6.1.4.1.2.6.158.3.0.162
Cooling Devices (Warning)	mmTrapFanN	.1.3.6.1.4.1.2.6.158.3.0.165
Power Modules (Warning)	mmTrapPowerN	.1.3.6.1.4.1.2.6.158.3.0.164
Blades (Warning)	mmTrapBladeN	.1.3.6.1.4.1.2.6.158.3.0.160
I/O Modules (Warning)	mmTrapION	.1.3.6.1.4.1.2.6.158.3.0.161
Storage Modules (Warning)	mmTrapStorageN	.1.3.6.1.4.1.2.6.158.3.0.163
Event Log (Warning)	mmTrapLogFullN	.1.3.6.1.4.1.2.6.158.3.0.7
System/Informational		
Chassis/System Management (Informational)	mmTrapChassisS	.1.3.6.1.4.1.2.6.158.3.0.178
Cooling Devices (Informational)	mmTrapFanS	.1.3.6.1.4.1.2.6.158.3.0.181
Power Modules (Informational)	mmTrapPowerS	.1.3.6.1.4.1.2.6.158.3.0.180
Blades (Informational)	mmTrapBladeS	.1.3.6.1.4.1.2.6.158.3.0.176
I/O Modules (Informational)	mmTrapIOS	.1.3.6.1.4.1.2.6.158.3.0.177
Storage Modules (Informational)	mmTrapStorageS	.1.3.6.1.4.1.2.6.158.3.0.179
Event Log (Informational)	mmTrapSysLogS	.1.3.6.1.4.1.2.6.158.3.0.35
Power On/Off (Informational)	mmTrapPwrDOS	.1.3.6.1.4.1.2.6.158.3.0.182
Inventory change (Informational)	mmTrapSysInvS	.1.3.6.1.4.1.2.6.158.3.0.34
Network change (Informational))	mmTrapNwChangeS	.1.3.6.1.4.1.2.6.158.3.0.37
User activity (Informational)	mmTrapRemoteLoginS	.1.3.6.1.4.1.2.6.158.3.0.30
Test Message	mmTrapAppS	.1.3.6.1.4.1.2.6.158.3.0.22

Along with the support for the new categories, the existing (legacy) categories are still available. New SNMP users should use the enhanced categories.

Every SNMP trap has the same set of variables for each trap. These parameters might be extended in the future by adding additional objects to the bottom (end) of the existing data.

For more information about specifying monitored alerts, see the *Advanced Management Module User's Guide*.

Log source

Use the log source as an aid in determining which component has reported an event. The log source field shows one of the following sources:

- Audit. A user action log.
- Blade_*number*. The blade server indicated by the bay number.
- Cool_*number*. A fan or blower, depending on chassis type, indicted by bay number.
- IOMod_*number*. An I/O module indicated by the bay number.
- Stor_*number*. A storage module indicated by the bay number.
- Power_*number* . A power module indicated by the bay number.
- SERVPROC. The service processor for the advanced management module.

Automatically notify service

If this field is set to "Yes," and you have enabled Service Advisor, your authorized service and support provider will be automatically notified if the event is generated. If IBM is the service provider, IBM will contact you. In addition, AutoFTP will send the service data related to this event to the specified FTP server, if AutoFTP is configured.

Note: Service Advisor must be configured to run for the call-home function to work.

While waiting for IBM to call, you can perform the recommended actions for the event.

Recoverable

If this field is a "Yes," it indicates that the advanced management module can generate a message that shows the condition has recovered. This does not mean that the event is a recovery of the condition.

If the message is a recovery message, the advanced management module will typically prefix the message with the word "Recovery". An example of a recoverable message is an over-temperature threshold event. A component alerts the advanced management module for an over-temperature condition and then recovers when the condition no longer exists.

If this field is a "No" then there is no possible recovery reported by the advanced management module. These are typically informational message such as a user has logged in, or a component was installed.

For standard blade server messages that are informational and can be recovered, a customize message will be displayed. For example, consider the following message:

```
0x806F000F  E  FW/BIOS, firmware progress (ABR Sensor) error
```

The recovery event will be displayed if the blade server recovers from the event

```
0x806F000F I Recovery FW/BIOS, firmware progress (ABR Sensor) error
```

Example

For some events, the event identifier and event description provide an exact message that is displayed. In other cases, the event description listed in Chapter 2, "Messages," on page 25 is a partial description; the actual description provides additional information. In those cases, an example of an actual event is provided in this section.

Chassis LED

The front panel of a chassis provides LED indicators for faults, temperatures, information and location (Blue). Some events will cause an LED to illuminate. Other events, such as events from a blade server, are indicated through the chassis as well as through Light Path on the blade server. For example, if a blade server indicates an error LED is lit, the chassis error LED should also be lit. Where appropriate, this field displays the chassis LEDs that are lit for an event.

For more information about LEDs and light path, see "Light path diagnostic LEDs" on page 9.

Alarm Panel LED (BC T and BC HT)

The alarm panel on the BladeCenter T and BladeCenter HT chassis can indicate a Critical, Major, Minor or informational LED. Where appropriate, this field displays the Alarm Panel LEDs that are lit for an event.

For more information about LEDs and light path, see "Light path diagnostic LEDs - BladeCenter T and BladeCenter HT chassis" on page 10.

User response

Indicates what actions should be performed by the user to resolve the event. If, after performing all of the actions described in the User Response, the user cannot resolve the problem, the user should contact IBM. See "Getting help and technical assistance" on page 22 for more information.

Perform the steps listed in this section in the order shown until the problem is resolved.

Note: In addition to the steps shown in this section, another resource that you can use is the *Problem Determination and Service Guide* for the specified blade server type. It might have more specific steps that can be used to resolve this event.

IPMI blade server event messages

The interface between the advanced management module and the service processor on the blade server is an industry standard called Intelligent Platform Management Interface (IPMI). IPMI defines a standard set of events that can be sent from the service processor to the advanced management module for monitoring the status of the blade server.

The event log strings associated with Event IDs with the high order bit set are dynamically built from standard IPMI events received from the service processors on blade servers. The events received from the blade server are in numerical format and the advanced management module translates the message into text based on the IPMI standard. The AMM event log string for a service processor IPMI event also includes the service processor defined 16-byte Sensor Data Record ID string in parenthesis that describes the sensor record associated with the event.

IPMI-based events add additional information to the message string when the event is displayed:
* Entity ID. The specific component, such as a bus or a panel.
* Instance. The unique occurrence of a component. The instance is typically a numbered occurrence of an entity.
* Sensor Type (for threshold and generic discrete only). An indication of what can be measured by the sensor, such as temperature or memory.

The Event ID for an IPMI-based event can be broken up into 4 bytes:
* Byte 1 (left most byte) 0x80 – means it is an advanced management module standard IPMI event
* Byte 2 is the event/readying type code.
* Byte 3 is the sensor-specific offset
* Byte 4 is for threshold and generic discrete

For example, consider the event 0x806F010F:
* 0x80. This is a generic event
* 6f. The event is sensor specific
* 01. The sensor-specific offset, which in this case means not running or stopped. The offset is dependent on the sensor type.
* 0F. The sensor type, which in this case is firmware progress

The resulting error message is:

```
0x806F010F E (Blade Name) System board, firmware progress (Pri FW Status)
          option ROM hang
```

Special messages

There are several event IDs that have special meaning in the event log.

They are not recorded in Chapter 2, "Messages," on page 25 because these event IDs in the event log are not notification messages; they will not generate e-mail notifications or SNMP traps.

- 0x10000001. Messages with this event ID in the event log were written to the event log in a previous version of advanced management module code. Older versions of the event log did not store the event ID, so a number was provided for consistency in viewing the log.
- 0x10000002 – Messages with this event ID in the event log are blade server service processor *pass-through* messages that are written directly to the event log. These messages are not documented here because they are generated by the specific blade server. They are detected by the following prefixes in the messages:
  - POSTBIOS:
  - SMI Hdlr
  - DIAGS:
  - SMS:
  - SYS F/W:

  For example:

  ```
  (deck03-GPVT) SYS F/W: Firmware. See procedure FSPSP04 then FSPSP06
  (5000EED8 B181D30B 030100F0 53ADAF10 C14420FF 400000FF 00000006 000D1E02 00000001 00000000)
  ```
- 0x10000003. Messages with this event ID in the event log indicate that a non-volatile RAM (NVRAM) reset occurred, normally during AMM initialization, which causes the system log to be cleared. This message is logged for additional information

Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

Use this information to obtain additional information about IBM and IBM products, determine what to do if you experience a problem with your BladeCenter product or optional device, and determine whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe you require IBM to perform warranty service on your IBM product, the IBM Service Technicians will be able to assist you more efficiently if you prepare before you call.

- Have you checked for updated BIOS, firmware, or operating system device drivers for your system? The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware of the product (unless covered by an additional maintenance contract). Your IBM Service Technician will request that you upgrade your software/firmware if your issue has a documented solution within a software upgrade.

  You can obtain the latest downloads for your system from the IBM BladeCenter support site at http://www.ibm.com/systems/support/supportsite.wss/selectproduct?taskind=2&brandind=5000020 &taskind=2.

- Have you added new hardware or installed new software in your environment? The IBM BladeCenter Server Proven site at http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html shows you what hardware and software is supported by BladeCenter systems.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.
- Go to the IBM support site at http://www.ibm.com/support to check for information to help you solve the problem.
- Gather the following information to provide to IBM Service. This data will assist IBM in quickly providing a solution to your issue, and ensure you receive the appropriate level service for which you may have contracted.

    Note: For information about using IBM Dynamic System Analysis (DSA) to collect information, see "IBM Dynamic System Analysis (DSA)" on page 16
    - Hardware and Software Maintenance agreement contract numbers, if appropriate
    - Machine Type number (IBM 4 digit machine identifier)
    - Machine model number
    - Machine serial number
    - Current$^®$ system BIOS and firmware levels
    - Other pertinent information such as error messages and logs
- Submit an Electronic Service Request.
    1. Go to http://www.ibm.com/support.
    2. Under Support & downloads, click **Open service request**.
    3. Follow the prompts.

    Submitting an Electronic Service Request will start the process of determining a solution to your issue by getting all the pertinent information in the hands of IBM Service quickly and efficiently. IBM Service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services.

To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/planetwide/ and click **Find a Business Partner** on the right side of the page. For IBM support telephone numbers, see http://www.ibm.com/planetwide/. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with BladeCenter products.

For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, see http://www.ibm.com/services/ or see http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Additional resources

There are several resources available to help you in using the advanced management module and resolving issues with your BladeCenter system.

Related documentation

Use the following documentation to learn more about the advanced management module.

- *IBM BladeCenter Advanced Management Module Installation Guide*
- *IBM BladeCenter Advanced Management Module User's Guide*
- *IBM BladeCenter Advanced Management Module Command Line Interface Reference Guide*

You can find these documents at the following Web site http://publib.boulder.ibm.com/infocenter/systems/topic/com.ibm.bladecenter.advmgtmod.doc//adv_man_mod_printable_doc.html

Documentation for BladeCenter components is available at the following Web site: http://publib.boulder.ibm.com/infocenter/systems/topic/com.ibm.bladecenter.common.nav.doc/bladecenter_converged_welcome_page.html

IBM websites

Use these websites to obtain additional information about your BladeCenter system and resolving issues

- IBM Support website: http://www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020
- Search BladeCenter website: http://www.ibm.com/systems/support/supportsite.wss/dosearch?q=8886+retain&notsearch=Y&taskind=0%7CAll+tasks&familyind=0%7CAll+Product+Families&oldfamily=0&brandind=5000020&search.x=0&onSelectSubmit=N
- IBM BladeCenter Software and Downloads website: http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-63017&brandind=5000020
- IBM ServerProven website: http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html
- IBM Journal of Research and Development - IBM BladeCenter: http://www.research.ibm.com/journal/rd49-6.html
- IBM Redbooks® website:http://www.redbooks.ibm.com/

Chapter 2. Messages

The messages in this section are ordered by event ID in hexadecimal. If you receive an event through the event log or through notifications, such as e-mail or SNMP, you can look up the event ID to determine the actions that should be taken, if any action is required.

Note: The events listed in this documentation are related to the latest advanced management module firmware.

For more information about events 0x10000001, 0x10000002, and 0x10000003, see "Special messages" on page 22.

0x00000014   Test alert generated

Explanation: A test notification message has been generated.

Severity: Informational

Alert Category: Test Message - mmTrapAppS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Test alert generated by Web user USERID.

User response: Information only; no action is required.

0x00000067   Multiple Chassis Cooling Device failures

Explanation: Multiple fan modules have failed.

Severity: Error

Alert Category: Cooling Devices (Critical) - mmTrapFanC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Look in the event log to determine which fan modules have failed and replace those fan modules.

0x0000006B   Event log full

Explanation: The advanced management module event log is full. New entries in the event log will overwrite the oldest entries.

Severity: Warning

Alert Category: Event Log (Warning) - mmTrapLogFullN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: If you do not wish to continue monitoring events (receive log full and log 75% full messages) in the event log, you can choose to turn off the event monitoring from the advanced management module Web interface. Otherwise, perform these steps:

1. Inspect the event log and make sure that a syslog collector is enabled to save the log data.

2. Delete the event log messages.

For information about event monitoring and enabling a syslog collector, refer to the Advanced Management Module User's Guide or the Advanced Management Module Command-Line Interface Reference Guide. These documents are available on the Web.

0x0000006F   Blade voltage outside of recommended range

Explanation: The blade server voltage is outside of the recommended range

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: If another blade server has this same problem, it could be an issue with the Power Modules. Otherwise it could be a blade hardware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.

0x00000071   Event log 75 percent full

Explanation: The advanced management module event log is 75% full. When the event log is completely full, the new entries will overwrite the oldest entries.

Severity: Informational

Alert Category: Event Log (Informational) - mmTrapSysLogS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: If you do not wish to continue monitoring events (receive log full and log 75% full messages) in the event log, you can choose to turn off the event monitoring from the advanced management module Web interface. Otherwise, perform these steps:

1. Inspect the event log and make sure that a syslog collector is enabled to save the log data.

2. Delete the event log messages.

For information about event monitoring and enabling a syslog collector, refer to the Advanced Management Module User's Guide or the Advanced Management Module Command-Line Interface Reference Guide. These documents are available on the Web.

0x00000072   POST watchdog triggered

Explanation: The power on self test (POST) watchdog in the specified blade server has been triggered.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. From the advanced management module Web interface, look at the LEDs for the blade server (click Monitors and then click LEDs) and check for any errors. If an error has occurred, refer to the Hardware Maintenance Manual and Troubleshooting Guide or the Problem Determination and Service Guide for the specified blade server type to resolve the error. The Hardware Maintenance Manual and Troubleshooting Guide and Troubleshooting Guide or the Problem Determination and Service Guide are available on the Web.

2. If you added options to the blade server, reseat those options. Otherwise, reseat the blade server.

3. If the blade server is an HS20 or an HS40 blade server, listen for any beep codes that may occur when the blade server reboots. Refer to the Hardware Maintenance Manual and Troubleshooting Guide or the Problem Determination and Service Guide for more information about resolving beep codes.

4. If the blade server is a JS20 blade server, refer to the Problem Determination and Service Guide for more information about this event.

0x00000073   OS watchdog triggered

Explanation: The operating system (OS) watchdog for the specified blade server has been triggered. This may be the result of an operating system error.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Critical

User response: The actions to take are based on the type of blade server for which this event was generated:

- If the blade server type is a JS20, see the Problem Determination and Service Guide for information about resolving this error.
- If the blade server type is an HS20 or an HS40, perform these steps:
  1. Make sure that the operating system is still running and that the expected applications are still operating.
  2. Restart the blade server if it did not automatically start when this event was generated.
  3. Disable the OS watchdog and restart the blade server. You can disable the OS watchdog from BIOS. Restart the blade server and press F1 to display the BIOS menu.

0x00000077   System boot failed

Explanation: The system boot process for the specified blade server failed before the operating system was loaded.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: The actions to take are based on the type of blade server for which this event was generated:

1. From the BIOS menu on the blade server, verify that the boot parameters are configured correctly. Restart the blade server and press F1 to display the BIOS menu.

2. If you have added options to the blade server, reset those options. Otherwise, reset the blade server.

3. Listen for any beep codes that may occur when the blade server reboots. Refer to the Hardware Maintenance Manual and Troubleshooting Guide or the Problem Determination and Service Guide for more information about resolving beep codes.

0x0000007A   Remote login successful for user

Explanation: The specified user has logged in to the advanced management module successfully.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Remote login successful for user 'USERID' from FTP at IP 192.168.0.1

User response: Information only; no action is required.

0x00000081   System boot initiated

Explanation: The specified blade server has restarted.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00010022   DHCP application failed to obtain DHCP IP address.

Explanation: The advanced management module cannot obtain an IP address from the DHCP server.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Perform these steps:
1. Check that the Ethernet cable is plugged in and devices on both ends of the cable are functioning.
2. Verify that the DHCP server is up and running.

0x00014033   USB port overcurrent failure

Explanation: A USB port has failed due to an over current condition.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: Check to see if the USB ports are working (such as the keyboard, the mouse, and devices plugged into the media tray USB ports). If all devices are functioning, no action is required. If not, perform these steps:

1. Unplug the USB device that is not working. If the problem goes away, suspect a problem with the USB device.
2. Plug in the USB device again.
3. Restart the advanced management module.
4. Replace the advanced management module.

0x00014034   USB hub overcurrent failure

Explanation: A USB hub has failed due to an over current condition.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: Check to see if the USB ports are working (such as the keyboard, the mouse, and devices plugged into the media tray USB ports). If all devices are functioning, no action is required. If not, perform these steps:

1. Unplug the USB device that is not working. If the problem goes away, suspect a problem with the USB device.
2. Plug in the USB device again.
3. Restart the advanced management module.
4. Replace the advanced management module.

0x00014035   User deleted file

Explanation: The specified file name has been deleted from the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User USERID from 192.168.0.1 (Web) deleted file '1.TXT'.

User response: Information only; no action is required.

0x00014045   CIN blade Pair

Explanation: One or both chassis internal network (CIN) parameters for the blade server have been changed. These parameters include the CIN VLAN ID and the CIN IP address.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:

- CIN blade Pair 4094 192.168.0.1 added
- CIN blade Pair 4094 192.168.0.1 disabled
- CIN blade Pair 4094 192.168.0.1 enabled
- CIN blade Pair 4094 192.168.1.1 changed
- CIN blade Pair 4094 192.168.1.1 deleted

User response: Information only; no action is required.

0x00014046 Globally enabling CIN

Explanation: The chassis internal network (CIN) has been enabled for all configured blade servers.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Globally enabling CIN failed by user 'USERID' from '192.168.0.1 (Web)'
- Globally enabling CIN successful by user 'USERID' from '192.168.0.1 (Web)'

User response: Informational only. No action required.

0x00014047 Globally disabling CIN

Explanation: The chassis internal network (CIN) has been disabled. All CIN functions are disabled for all configured blade servers.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Globally disabling CIN failed by user 'USERID' from '192.168.0.1 (Web)'
- Globally disabling CIN successful by user 'USERID' from '192.168.0.1 (Web)'

User response: Informational only. No action required.

0x0001404A IPv6 support is enabled

Explanation: IPv6 support has been enabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001404B   IPv6 support is disabled

Explanation: IPv6 support has been disabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001404C   IPv6 static configuration is enabled

Explanation: IPv6 static address assignment has been enabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001404D   IPv6 static configuration is disabled

Explanation: IPv6 static address assignment has been disabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001404E   %s IPv6 static configuration is changed %s

Explanation: IPv6 static address configuration has been changed on the advanced management module by the specified user account.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Primary AMM IPv6 static configuration is changed by user 'USERID' from '10.11.20.48 (Web)' Gateway=2001::3456 Prefix length=64 IP address=2001::1234.

User response: Information only; no action is required.

0x00014053   IPv6 DHCP Address Configuration is enabled

Explanation: DHCPv6 has been enabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00014054   IPv6 DHCP Address Configuration is disabled

Explanation: DHCPv6 has been disabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00014055   %s AMM DHCPv6 application failed to obtain DHCP IP address.

Explanation: The advanced management module was not able to obtain a dynamic address assignment from DHCPv6.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Primary AMM DHCPv6 application failed to obtain DHCP IP address.

User response: Perform these steps:
1. Check that the Ethernet cable is plugged in and devices on both ends of the cable are functioning.
2. Verify that the DHCPv6 server is up and running.

0x00014056   AMM DHCPv6 config:

Explanation: The specified DHCPv6 configuration is currently enabled for the advanced management module.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00014060   IPv6 stateless address auto-configuration is enabled

Explanation: IPv6 stateless address auto-configuration has been enabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00014061   IPv6 stateless address auto-configuration is disabled

Explanation: IPv6 stateless address auto-configuration has been disabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015011   Configurations of Automated FTP problem report.

Explanation: The configuration of Automated FTP/TFTP cannot be changed because one or more configuration settings are not valid.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User USERID failed to change configurations of Automated FTP problem report.

Alarm Panel LED (BC T and BC HT): Minor

User response: Correct the configuration settings (including all passwords) and attempt to save the configuration again.

0x00015012   Configurations of Automated FTP problem report.

Explanation: The automated FTP/TFTP report for service data has been enabled, disabled, or the configuration has been changed by the specified user.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User USERID changed configurations of Automated FTP problem report.

User response: Information only; no action is required.

0x00015013   Automated problem report failed.

Explanation: The attempt to automatically FTP/TFTP service data was not successful.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Test event FTP automated problem report failed. Invalid Machine Type/Model or Serial No of Chassis.

User response: Perform these steps:
1. Ping the FTP server to make sure that it is functional.
2. Verify that the FTP server exists and is configured correctly.
3. Attempt to log in to the FTP server.
4. Determine if there is a firewall issue between the advanced management module and the FTP server.

0x00015014   Manual e-mail of service information

Explanation: An e-mail notification was generated by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Manual e-mail of service information is reported by user USERID.
- Manual e-mail of service information failed to be reported by user USERID.

User response: Information only; no action is required.

0x00015030   The AMM failed over during a call home operation. The new primary AMM will make a call home.

Explanation: During a call home operation, the advanced management module failed. This event will be called home when the failover is complete and the standby advanced management module becomes the new primary advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: No

User response: Information only; no action is required.

Note to service personnel:

Because of the nature of this error, Service Data will sometimes not be sent to IBM by the AMM. If that occurs, contact the customer and have them initiate a manual call home operation. Instruct them not to reboot, failover or flash the AMM until we confirm the data has been received. The Service Data can then be examined and the messages found can be dealt with individually per the recommendations in this document.

0x00015040 **The AMM was restarted with call home events pending. The new primary AMM will complete the operation.**

Explanation: During a call home operation, the advanced management module was reset. This specific event will be called home after the primary advanced management module becomes functional.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: No

User response: Information only; no action is required.

Note to service personnel:

Because of the nature of this error, Service Data might not be sent to IBM by the advanced management module. If that occurs, contact the customer and have them initiate a manual call home operation. Instruct them not to reboot, initiate a failover, or update the firmware on the advanced management module until you are sure that service data has been received. After service data has been received, the corrective action is to search the logs for call home messages that may have problems. These messages can be dealt with individually per the recommendations in this document.

0x00015050 **Service data collection for event**

Explanation: Service Advisor cannot collect service data for the specified event. Therefore, Service Advisor will not call home for the event.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Service data collection for event 0x00026801 failed. Event will not be reported.

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the event log for other errors related to the advanced management module and resolve them.
2. Attempt to collect the service data for this event through the advanced management module Web interface or the command-line interface. See the Advanced Management Module User's Guide or the Advanced Management Module Command-Line Interface Reference Guide for more information. These documents are available from the Web.
3. Restart the advanced management module and attempt to collect the service data again.
4. Generate a call home using Service Advisor for the event.

0x00015060 **modified the Call Home Exclusion List.**

Explanation: The call home exclusion list has been modified by the specified user.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User USERID modified the Call Home Exclusion List.

User response: Information only; no action is required.

0x00015100   Firmware update started by user

Explanation: The specified user account started a firmware update for the specified device.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Firmware update started by user 'USERID' from 192.168.0.1 (Web) for AMM.

User response: Information only; no action is required.

0x00015101   Firmware update of Advanced Management Module

Explanation: The advanced management module firmware has been updated.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of Advanced Management Module (AMM Main Application) from 192.168.0.1 (Web) succeeded for user 'USERID'. build id:BPET025 11-05-08, revision 2

User response: Information only; no action is required.

0x00015102   Firmware update of Advanced Management Module

Explanation: The firmware was not updated on the advanced management module. The previous version of firmware will be used.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of Advanced Management Module failed : User session is no longer valid

Alarm Panel LED (BC T and BC HT): Minor

User response: Attempt to update the firmware on the advanced management module again.

0x00015103   Firmware update of Blade

Explanation: The firmware for the specified blade server has been updated.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of Blade (Blade System Management Processor) from 192.168.0.1 (Web) succeeded for user 'USERID'. Build id: BCBT50A

User response: Information only; no action is required.

0x00015104   Firmware update of Blade

Explanation: The firmware for the specified blade server was not updated.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of Blade (Blade System Management Processor) failed : User session is no longer valid

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Attempt to update the firmware on the blade server again, making sure that the firmware is intended for the specified blade server.
2. Restart the service processor for the specified blade server. You can restart the service processor from the advanced management module Web interface. Then attempt to update the firmware again.

Note: Some blade servers, such as the BladeCenter HS22, require that the chassis management LAN be functional for firmware updates via TFTP to occur. There must also be a functioning switch module with a connection to the blade server. For these updates, the local storage on the advanced management module (RDoC) will need enough space to hold the firmware. If there is already a firmware image on the RDoC, it will need to be removed.

0x00015105   Firmware update of I/O Module

Explanation: The firmware for the specified I/O module has been updated.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of I/O Module (Optical Pass-thru Module) from 192.168.0.1 (Web) succeeded for user 'USERID'. Build id: BROR09AUS

User response: Information only; no action is required.

0x00015106   Firmware update of I/O Module

Explanation: The firmware for the specified I/O module was not updated.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of I/O Module (Optical Pass-thru Module) from 192.168.0.1 (Web) failed for user 'USERID' : device write failed after retry

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Attempt to update the firmware on the I/O module again.

2. Make sure that there is sufficient space for the image in the local storage area on the advanced management module. You can access the local storage area through the advanced management module Web interface (MM Control --> File Management) or through an FTP session.

0x00015401   Service processor of Blade 01 is in firmware update mode and needs to be flashed.

Related messages:
- 0x00015402 : Service processor of Blade 02 is in firmware update mode and needs to be flashed.
- 0x00015403 : Service processor of Blade 03 is in firmware update mode and needs to be flashed.
- 0x00015404 : Service processor of Blade 04 is in firmware update mode and needs to be flashed.
- 0x00015405 : Service processor of Blade 05 is in firmware update mode and needs to be flashed.
- 0x00015406 : Service processor of Blade 06 is in firmware update mode and needs to be flashed.
- 0x00015407 : Service processor of Blade 07 is in firmware update mode and needs to be flashed.
- 0x00015408 : Service processor of Blade 08 is in firmware update mode and needs to be flashed.
- 0x00015409 : Service processor of Blade 09 is in firmware update mode and needs to be flashed.
- 0x0001540A : Service processor of Blade 10 is in firmware update mode and needs to be flashed.
- 0x0001540B : Service processor of Blade 11 is in firmware update mode and needs to be flashed.
- 0x0001540C : Service processor of Blade 12 is in firmware update mode and needs to be flashed.
- 0x0001540D : Service processor of Blade 13 is in firmware update mode and needs to be flashed.
- 0x0001540E : Service processor of Blade 14 is in firmware update mode and needs to be flashed.

Explanation: The service processor on the specified blade server has detected that the firmware for the specified blade server requires updating.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Update the firmware for the service processor. You can find firmware on the IBM BladeCenter software and device drivers Web page.

0x00015500   Failed to change service processor management network interface

Explanation: The external interface of the management network for the blade server cannot be set.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Failed to change service processor management network interface 1 configuration of blade 2.

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Attempt to set the management network configuration for the blade server again.

2. Reset the service processor on the blade server.
3. Reseat the blade server.
4. Update the firmware for the service processor on the blade server. You can find firmware on the IBM BladeCenter software and device drivers Web page.

0x00015501   AMM internal USB fault.

Explanation: The advanced management module encountered an internal USB error.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Restart the advanced management module.
2. Reseat the advanced management module.
3. Replace the advanced management module.

0x00015503   AMM reset due to watchdog timeout

Explanation: The advanced management module was reset due to watchdog timeout.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Continue to monitor the event log to determine if the situation occurs again. If so, it could be related to a change in the configuration of the advanced management module or the network. Check the event log to determine what changes have been made to the advanced management module that might have caused this event.
2. Check the change history on the Web for firmware updates that might be related to watchdog timeouts or advanced management module resets. Update the firmware if applicable.

0x00015504   The operator is not permitted to change the power policy to consume more power than is available.

Explanation: The power policy cannot be changed to a setting that enables the chassis to use more power than is available from a single power supply.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015505   Wake on LAN for

Explanation: The specified user account enabled or disabled Wake on LAN for the specified blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Wake on LAN for blade 01 enabled by user 'USERID' from 192.168.0.1
- Wake on LAN for all blades disabled by user 'USERID' from 192.168.0.1

User response: Information only; no action is required.

0x00015506   Blade %s management network interface configuration updated by '%s' from '%s'.

Explanation: The specified user updated the blade server management network interface configuration.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015600   Firmware update of Standby Management Module

Explanation: When the primary advanced management module completes a firmware update or a standby advanced management module is installed, the firmware for the standby will be updated if it is different than the firmware level of the primary. The firmware update of the standby advanced management module failed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of Standby Management Module from MM 1 to MM 2 failed.

Alarm Panel LED (BC T and BC HT): Minor

User response: Restart the primary advanced management module. When the primary advanced management module is restarted, it will determine that the firmware levels are different and will attempt to update the firmware again.

If the primary advanced management module fails over to the standby (making it the primary) and the firmware levels are different, the new primary advanced management module will attempt to update the previous primary advanced management module to the active firmware level.

Note: The background update of the standby advanced management module can upgrade to newer or older firmware levels.

0x00015700   **Firmware update of Standby Management Module**

Explanation: The firmware update of the specified image from the primary advanced management module to the standby advanced management module succeeded.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Firmware update of Standby Management Module from MM 1 to MM 2 was successful.

User response: Information only; no action is required.

0x00015800   **Management bus hang detected by both management modules.**

Explanation: Both advanced management modules detected a communication problem on the I2C management bus. A device on the I2C bus might be nonresponsive.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
- Remove the specified device and wait approximately 90 seconds to see if a recovery event is sent.
- If the recovery event is sent, install the device again.
- If the problem persists, replace the specified device.
- Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x00015801   **Chassis type detection failure.**

Explanation: The chassis type detected by the advanced management module is not valid. Therefore, the advanced management module will substitute a new chassis type value and attempt to restart. Do not change the configuration until the advanced management module has restarted.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Example Message: Chassis type detection failure. The AMM will override current chassis type BC-1 with BC-H for recovery before reboot.

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: The advanced management module will override the chassis type and restart automatically to resolve the issue. While the advanced management module is restarting, do not change the hardware configuration.

Continue to monitor the event log to determine if the situation occurs again. If so, reseat the advanced management module.

0x00015802   Detected a duplicate IP address

Explanation: The advanced management module received an Address Resolution Protocol (ARP) request or reply with an IP address that is the same as that IP address used by the advanced management module.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Detected a duplicate IP address 9.123.251.76 configured at MAC@=00:15:58:7f:05:98

Alarm Panel LED (BC T and BC HT): Minor

User response: Make sure the IP addresses for all network devices on the same subnet are unique.

0x00015803   AMM can not convert host name

Explanation: The advanced management module cannot resolve the specified hostname for the specified syslog collector.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Verify that the syslog collector is configured correctly and can be reached from the advanced management module.
2. Verify that DNS is configured correctly for hostname resolution.

0x00015804   Media Tray being used by blade

Explanation: The specified blade server has requested access to the media tray, but the media tray is currently in use by another blade server. Only one blade server at a time can access the media tray.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Media Tray being used by blade 01 while blade 14 allocated the ownership

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Attempt to switch control of the media tray to the blade server again.
2. Reset the service processor of the blade server that currently controls the media tray.
3. Reseat the blade server that currently controls the media tray.

0x00015805   KVM being used by blade

Explanation: The specified blade has requested access to the KVM, but the KVM is currently being used by another blade server. Only one blade server at a time can access the KVM.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: KVM being used by blade 02 while blade 13 allocated the ownership

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Attempt to switch control of the KVM to the blade server again.
2. Reset the service processor of the blade server that currently controls the KVM.
3. Reseat the blade server that currently controls the KVM.

0x00015806   Local request for media tray failed. Local switching is disabled.

Explanation: Control of the media tray cannot be initiated locally (from the button on the blade server) because local switching has been disabled.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015807   Local request for KVM failed. Local switching is disabled.

Explanation: Control of the KVM cannot be initiated locally (from the button on the blade server) because local switching has been disabled.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015808   The active Management Module configuration data was saved to the chassis

Explanation: The specified user saved configuration information to the chassis from the primary advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015809   The configuration data was restored from the chassis to the active Management Module

Explanation: The specified user restored configuration information from the chassis to the primary advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001580A   Restoring the configuration data from the chassis to the active Management Module failed

Explanation: The specified user was unable to restore the configuration data from the chassis to the primary advanced management module.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Attempt to restore the configuration data again.
2. Attempt to restore configuration data from another configuration file.
3. Configure the advanced management module manually.

0x0001580B   data collection initiated for blade

Explanation: The specified user initiated data collection for the specified blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Service Processor data collection initiated for blade 01 by 'USERID'

User response: Information only; no action is required.

0x00015900   commands on blade Ethernet over USB interface

Explanation: The specified user account enabled or disabled the Ethernet over USB interface setting.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- User USERID enabled commands on blade Ethernet over USB interface for blade 1.
- User USERID disabled commands on blade Ethernet over USB interface for blade 1.

User response: Information only; no action is required.

0x00015901 Remote kvm switching

Explanation: The specified user account has enabled or disabled remote KVM switching.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015902 powered off blade

Explanation: The specified user powered off the specified blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' powered off blade 11

User response: Information only; no action is required.

0x00015903 powered on blade

Explanation: The specified user powered on the specified blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' powered on blade 11

User response: Information only; no action is required.

0x00015904 No power permission to the blade. Power command was not sent to blade

Explanation: A power command has not been sent to a blade due to power permission not being granted to that blade. Power permission may not be given if there adequate power is not available for a particular blade.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00015905   Power command sent to blade failed.

Explanation: The power command was not accepted by the blade server. The blade has responded with a failed status or did not reply.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Perform these steps:
1. Try the power command again.
2. If the blade server is local, press the power button (make sure that local button presses are enabled).
3. Reseat the blade server.

0x00015906   restarted blade

Explanation: The specified user restarted the specified blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' restarted blade 11

User response: Information only; no action is required.

0x00015907   restarted service processor on blade

Explanation: The specified user restarted the service processor on the specified blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' restarted service processor on blade 11

User response: Information only; no action is required.

0x00015908   restoring I/O module settings for bay

Explanation: The specified user reset the specified I/O module to the factory defaults.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' restoring I/O module settings for bay 01 to factory defaults

User response: Information only; no action is required.

0x00015909   Attempting to isolate source of management bus failure.

Explanation: The advanced management module is unable to communicate with a blade server on the management bus. Therefore, the advanced management module will attempt to isolate the source of the management bus failure.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Perform these steps:
1. Wait for communication to be recovered by the advanced management module or for the event log to display an event related to being unable to isolate the failure.
2. For each blade server in the chassis that is reporting communication errors:
   a. Reseat the blade server.
   b. Restart the blade server.
   c. Check the event log to determine if the issue has been resolved.
3. Update the service processor firmware for each blade server that is reporting communication errors.

0x0001590A   Service processor firmware update timeout.

Explanation: The advanced management module did not receive notification that the service processor firmware for the blade server was updated. The update might have been successful, but it should be verified.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Verify that the service processor firmware for the blade server has been updated to the appropriate level. You can determine the level of the firmware for the blade server through the advanced management module user interface.

0x00015A01   Power module 01 transient error.

Related messages:
- 0x00015A02 : Power module 02 transient error.
- 0x00015A03 : Power module 03 transient error.
- 0x00015A04 : Power module 04 transient error.
- 0x00015A05 : Power module 05 transient error.
- 0x00015A06 : Power module 06 transient error.

Explanation: The specified power module encountered an intermittent error.

Severity: Informational

Alert Category: Power Modules (Informational) - mmTrapPowerS

0x00016001 • 0x0001600B

Log Source: Power_##

Automatically notify service: No

Recoverable: No

Example Message:

- Power module 2 transient error. Over voltage fault
- Power module 2 transient error. Under voltage fault
- Power module 2 transient error. Over current fault
- Power module 2 transient error. 48V over voltage fault
- Power module 2 transient error. 48V under voltage fault
- Power module 2 transient error. 48V over current fault

User response: Monitor the event log to determine if this error continues to occur. If so, replace the power module.

0x00016001   Management module network initialization complete

Explanation: The network initialization for the primary advanced management module is complete.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001600A   User login failure exceeds maximum number of successive login failures. User account will be temporarily locked out.

Explanation: A user has attempted to log in and failed, and the attempt has exceeded the maximum number of login failures for this user. The user account will be temporarily locked out.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Contact a system administrator to reset the user account.

0x0001600B   All system messages deleted from event log

Explanation: The system log events or audit log events have been deleted by the specified user ID.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001600D **'Do not log new authentication events for the same user for',**

Explanation: The setting "Do not log new authentication events for the same user for" a specified duration has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Do not log new authentication events for the same user for', successfully changed to '5 seconds' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001600E **'Ignore client IP address when tracking user authentication events',**

Explanation: The setting "Ignore client IP address when tracking user authentication events" has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Ignore client IP address when tracking user authentication events', successfully changed to 'no' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001600F **SSL server certificate error**

Explanation: The Secure Shell (SSL) certificate on the specified advanced management module is not valid. Users will not be able to access the advanced management module through the Web interface.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Perform these steps:

1. Log in to the advanced management module. You will need to log in using the command-line interface (CLI) or the serial port on the advanced management module. Refer to the Advanced Management Module Command-Line Reference for more information about using the CLI.

2. Regenerate the SSL certificate using the sslcfg command (you must have supervisor authority or chassis management authority to use this command). Alternatively, you can use the sslcfg command to disable SSL if it is not required.

Refer to the Advanced Management Module User's Guide for more information about SSL.

0x00016010   SSL client certificate error

Explanation: The advanced management module has detected that the Secure Sockets Layer (SSL) client certificate is not valid. It does not match the SSL server certificate.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Generate or install a new SSL client certificate. See the Advanced Management Module User's Guide for more information about SSL certificates.

0x00016011   SSL trusted CA certificate 1 error

Explanation: Trusted certificates are imported to the advanced management module and used by the advanced management module Secure Sockets Layer (SSL) client to authenticate the LDAP Server SSL certificate. The advanced management module has detected that the specified trusted certificate is not valid

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Reinstall the trusted certificate. Refer to the Advanced Management Module User's Guide for more information on trusted certificates.

0x00016012   SSL trusted CA certificate 2 error

Explanation: Trusted certificates are imported to the advanced management module and used by the advanced management module Secure Sockets Layer (SSL) client to authenticate the LDAP Server SSL certificate. The advanced management module has detected that the specified trusted certificate is not valid

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Reinstall the trusted certificate. Refer to the Advanced Management Module User's Guide for more information on trusted certificates.

0x00016013   SSL trusted CA certificate 3 error

Explanation: Trusted certificates are imported to the advanced management module and used by the advanced management module Secure Sockets Layer (SSL) client to authenticate the LDAP Server SSL certificate. The advanced management module has detected that the specified trusted certificate is not valid

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Reinstall the trusted certificate. Refer to the Advanced Management Module User's Guide for more information on trusted certificates.

0x00016014   SSL server certificate error

Explanation: The Secure Sockets Layer (SSL) certificate on the specified advanced management module is not valid. Users will not be able to access the advanced management module through the Web interface.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Perform these steps:

1. Log in to the advanced management module. You will need to log in using the command-line interface (CLI) or the serial port on the advanced management module. Refer to the Advanced Management Module Command-Line Reference for more information about using the CLI.

2. Regenerate the SSL certificate using the sslcfg command (you must have supervisor authority or chassis management authority to use this command). Alternatively, you can use the sslcfg command to disable SSL if it is not required.

Refer to the Advanced Management Module User's Guide for more information about SSL.

0x00016015   IPv4 address of primary MM is the same as the IPv4 address of standby MM. Standby network interface is disabled.

Explanation: The IP address of primary advanced management module is the same as the IP address of standby advanced management module. The network interface of the standby advanced management module has been disabled.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Assign a different IP address to the standby advanced management module.

0x00016016   User account now active:

Explanation: The specified login profile (user account) has been changed to the active state. The user can now access the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User account now active: 'TEST'.

User response: Information only; no action is required.

0x00016017   Account has been inactive for more than the configured inactivity alert limit for user

Explanation: The specified login profile (user account) is in a dormant state because it has made no attempts to log in to the advanced management module for a specified period of time (inactivity alert period).

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account has been inactive for more than the configured inactivity alert limit for user 'TEST'.

User response: If the specified login profile has a need for continued access to the advanced management module, perform one of the following steps:
- Notify the owner of the login profile to log in to the advanced management module. This will reset the login profile to an active state.
- Reset the login profile to an active state. You must have Supervisor or Chassis Configuration authority to reset the login profile.

0x00016018   Account has been disabled because of inactivity for more than the configured limit for user

Explanation: The specified login profile (user account) has been disabled due to inactivity.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account has been disabled because of inactivity for more than the configured limit for user 'TEST'.

User response: If the specified login profile has a need for continued access to the advanced management module, reset the login profile to an active state. You must have Supervisor or Chassis Configuration authority to reset the login profile. See the Advanced Management Module User's Guide for more information.

0x00016019   Account has been inactive for longer than the configured disable and alert limit for supervisor

Explanation: The amount of time that the supervisor account has been inactive exceeds the configured alert and disable limits.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account has been inactive for longer than the configured disable and alert limit for supervisor 'USERID'.

User response: If this account is still required, the owner of the account needs to log in to the advanced management module.

0x0001601A   Remote logoff successful for user

Explanation: The specified user has logged out of the advanced management module successfully.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Remote logoff successful for user 'USERID' from FTP at IP 192.168.0.1

User response: Information only; no action is required.

0x0001601B   All audit messages deleted from event log

Explanation: Audit events have been cleared from the event log by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016020   Account password will expire for user

Explanation: The password for the specified account will expire within 7 days.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account password will expire for user USERID:5.

User response: If this user account is required, the owner of the account needs to change the password..

0x00016021   'Account security level'

Explanation: The account security level for the specified user account has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Account security level' successfully changed to 'Legacy' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016022   **'Maximum number of login failures' setting**

Explanation: The account security setting, Maximum number of login failures, has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Maximum number of login failures' setting successfully changed to '7' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required. However, the number of times that a specified user account login can fail before the account is disabled has changed.

0x00016023   **'Password expiration period' setting**

Explanation: The password expiration time interval (the amount of time that a password is valid before it expires) has changed. The setting determines the amount of time that a password is in effect before it automatically expires.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Password expiration period' setting successfully changed to '100' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016024   **'Factory default 'USERID' account password must be changed on next login' setting**

Explanation: The setting "Factory default 'USERID' account password must be changed on next login" has changed. The setting determines whether or not the USERID account must change the password when it is next used to log on to the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- 'Factory default 'USERID' account password must be changed on next login' setting successfully changed to 'Disabled' by 'USERID' from '192.168.0.1 (Web)'.
- 'Factory default 'USERID' account password must be changed on next login' setting successfully changed to 'Enabled' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016025   **'Minimum password reuse cycle' setting**

Explanation: The setting "Minimum password reuse cycle" has changed. The setting determines how often an older password can be reused (when you change passwords).

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Minimum password reuse cycle' setting successfully changed to '2' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016026   **'Complex password rules' setting**

Explanation: The setting "Complex password rules" has changed. The setting determines what kind of password is acceptable.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- 'Complex password rules' setting successfully changed to 'Enabled' by 'USERID' from '192.168.0.1 (Web)'.
- 'Complex password rules' setting successfully changed to 'Disabled' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016027   **'Minimum different characters in passwords' setting**

Explanation: The setting "Minimum different characters in passwords" has changed. The setting determines how many unique characters must be used when creating or changing a password.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Minimum different characters in passwords' setting successfully changed to '3' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016028   **'Force user to change password on first login' setting**

Explanation: The setting "Force user to change password on first access" has changed. The user will be required to change the password the next time the user logs in to the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:

0x00016029 • 0x0001602B

- 'Factory default 'USERID' account password must be changed on next login' setting successfully changed to 'Disabled' by 'USERID' from '192.168.0.1 (Web)'.
- 'Factory default 'USERID' account password must be changed on next login' setting successfully changed to 'Enabled' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016029   'Inactivity alert period' setting

Explanation: The setting "Inactivity alert period" has changed. The setting determines how long a user account can be inactive (not used to log in) before going dormant

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Inactivity alert period' setting successfully changed to '2' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001602A   'Inactivity alert and disable period' setting

Explanation: The setting "Inactivity alert and disable period" has changed. This setting determines how long a user account can be inactive (not used to log in) before it is disabled. An alert will be generated before a user account is actually disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Inactivity alert and disable period' setting successfully changed to '3' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001602B   'Lockout period after maximum login failures' setting

Explanation: The setting "Lockout period after maximum login failures" has changed. This setting determines the length of time that a user account is locked out after exceeding the maximum number of login failures.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'Lockout period after maximum login failures' setting successfully changed to '5' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001602C **'User login password required' setting**

Explanation: The setting "User login password required" has changed. The setting determines whether or not a password is required when a user account logs in to the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- 'User login password required' setting successfully changed to 'Enabled' by 'USERID' from '192.168.0.1 (Web)'.
- 'User login password required' setting successfully changed to 'Disabled' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001602D **Account**

Explanation: The specified user account has been disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account successfully disabled manually for user 'test' by 'USERID' from '192.168.0.1 (Web)'.

User response: If this user account is supposed to be disabled, no action is required. Otherwise, enable the user account. See the Advanced Management Module User's Guide for more information about enabling accounts.

0x0001602E **Account**

Explanation: The specified user account has been enabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account successfully enabled manually for user 'test' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001602F **Account**

Explanation: The specified user account has been unlocked.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account successfully unlocked manually for user 'test' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016030   LDAP authentication method

Explanation: The setting "User authentication method" has changed. The setting determines how users are authenticated when they log in.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: LDAP authentication method successfully changed to 'Local first, then LDAP' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016031   Web inactivity timeout

Explanation: The setting "Inactive session timeout value" has changed. The setting determines how long a Web interface session is idle before the session times out.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Web inactivity timeout successfully changed to 'User picks timeout' by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x00016032   Telnet inactivity timeout

Explanation: The "command-line session timeout" setting has changed. The setting determines how long a command-line session can be idle before the session times out.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Telnet inactivity timeout successfully changed to '600' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016033   HTTP port number

Explanation: The HTTP port number has changed. New HTTP connections must use the new port number.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: HTTP port number successfully changed from '80' to '800' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016034   SSL port number

Explanation: The Secure Sockets Layer (SSL) port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL port number successfully changed from '444' to '443' by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x00016035   TELNET port number

Explanation: The telnet port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: TELNET port number successfully changed from '230' to '23' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016036   SSH port number

Explanation: The Secure Shell (SSH) port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSH port number successfully changed from '220' to '22' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016037   SNMP agent port number

Explanation: The Simple Network Management Protocol (SNMP) agent port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SNMP agent port number successfully changed from '1610' to '161' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016038   SNMP traps port number

Explanation: The Simple Network Management Protocol (SNMP) traps port number has changed by certain user. You must restart the advanced management module for the new port number to take effect. Then, SNMP traps will be sent and received using the new port number.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SNMP traps port number successfully changed from '1620' to '162' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016039   TCP command mode port number

Explanation: The Transmission Control Protocol (TCP) command mode port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: TCP command mode port number successfully changed from '6346' to '6090' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001603A   Secure TCP command mode port number

Explanation: The secure transmission control protocol command mode port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001603B   FTP port number

Explanation: The File Transfer Protocol (FTP) port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: FTP port number successfully changed from '21' to '222' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001603C   FTP data port number

Explanation: The File Transfer Protocol (FTP) data port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: FTP data port number successfully changed from '20' to '200' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001603D   TFTP port number

Explanation: The Trivial File Transfer Protocol (TFTP) port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: TFTP port number successfully changed from '690' to '69' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001603F   SMASH telnet port number

Explanation: The SMASH Command-Line Protocol (CLP) port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SMASH telnet port number successfully changed from '50020' to '50023' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016040   Secure SMASH port number

Explanation: The Secure SMASH Command Line Protocol (CLP) port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Secure SMASH port number successfully changed from '50021' to '50022' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016044   SLP port number

Explanation: The Service Location Protocol (SLP) port number has changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SLP port number successfully changed from '428' to '427' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016048   SLP service

Explanation: The Service Location Protocol (SLP) service has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- SLP service successfully enabled by 'USERID' from '192.168.0.1 (Web)'.
- SLP service successfully disabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016049   Web server port

Explanation: The Web server port has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Web server port successfully enabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.
- Web server port successfully disabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x0001604A   IP port numbers

Explanation: All network port numbers have been reset to their default values. You must restart the advanced management module for these changes to take effect.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IP port numbers successfully reset to defaults by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only. No action required.

0x0001604B   TCP command mode port numbers

Explanation: The Transmission Control Protocol (TCP) Command Mode port number has been reset to its default value. Changes will take effect when the advanced management module is restarted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: TCP command mode port numbers successfully reset to defaults by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x0001604C   SMASH telnet port number

Explanation: The SMASH Command-Line Protocol (CLP) has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- SMASH telnet port number successfully enabled by 'USERID' from '192.168.0.1 (Web)'.
- SMASH telnet port number successfully disabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001604D   Secure SMASH port number

Explanation: The Secure SMASH Command Line Protocol (CLP) port number has changed, been enabled, or been disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

0x0001604E • 0x00016050

Recoverable: No

Example Message:
- Secure SMASH port number successfully enabled by 'USERID' from '192.168.0.1 (Web)'.
- Secure SMASH port number successfully disabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001604E   Data encryption

Explanation: Data encryption has changed. If it is enabled, user passwords are stored in NVRAM in encrypted format. Otherwise, passwords are stored in plain text.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Data encryption successfully enabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.
- There was an error disabling data encryption by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x0001604F   The account

Explanation: The specified user account has been deleted successfully by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: The account successfully deleted for user 'test' by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x00016050   The password expired for user

Explanation: The password for the specified user has expired.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: The password expired for user 'USERID'.

User response: Change the password for the specified user.

0x00016051   A password is required for user

Explanation: A password is required for the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Set the password for the specified user.

0x00016053   Serial port baud rate

Explanation: The baud rate for the advanced management module serial port has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Serial port baud rate successfully changed to '57600' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016054   Serial port parity

Explanation: The parity setting for the serial port has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Serial port parity successfully changed to 'ODD' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016055   Serial port stop bits number

Explanation: The stop bits setting for the serial port has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Serial port stop bits number successfully changed to '1' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016057   Telnet Protocol

Explanation: Telnet has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Telnet Protocol successfully enabled by 'USERID' from '192.168.0.1 (Web)'.
- Telnet Protocol successfully disabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016058   FTP server

Explanation: File transfer protocol (FTP) has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- FTP server successfully disabled by 'USERID' from '192.168.0.1 (Web)'.
- FTP server successfully enabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016059   TFTP server

Explanation: Trivial file transfer protocol (TFTP) has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- TFTP server successfully enabled by 'USERID' from '192.168.0.1 (Web)'.
- TFTP server successfully disabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001605B   NTP server

Explanation: Network time protocol (NTP) settings have been changed, or NTP has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- NTP server successfully disabled by 'USERID' from '192.168.0.1 (Web)'.
- NTP server successfully enabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001605C FTP timeout

Explanation: The file transfer protocol (FTP) timeout has been changed by the specified user account. This value determines the amount of time that an FTP connection can be inactive before it is closed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: FTP timeout successfully changed to '400' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001605E TCP Command mode

Explanation: The maximum number of user connections has been changed for TCP command mode by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: TCP Command mode successfully changed to '2' Connection(s) by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001605F SNMP Traps

Explanation: Simple Network Management Protocol (SNMP) traps have been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016060   SNMP

Explanation: The SNMP-v1 or SNMPv3 agent has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SNMP v1 agent successfully enabled by 'USERID' from '10.11.20.48 (Web)'.

User response: Information only; no action is required.

0x00016061   SNMPv1 configuration

Explanation: An SNMPv1 community configuration change has occurred.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016068   Date/Time changed by

Explanation: The date and time for the advanced management module have been changed by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016069   Time zone changed by

Explanation: The time zone has been changed by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001606A   Daylight Savings Time setting changed by

Explanation: The Daylight Savings Time has been changed by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001606B   SSH Protocol

Explanation: The Secure Shell (SSH) server has been enabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSH Protocol successfully enabled by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x0001606C   SSH Protocol

Explanation: The Secure Shell (SSH) server has been disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSH Protocol successfully disabled by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x0001606E   SSH host key generation completed successfully

Explanation: The Secure Shell (SSH) host key generation has completed successfully.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001606F   'Minimum password change interval' setting

Explanation: The "minimum password change interval" has changed. This change applies to all local users.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

0x00016070 • 0x00016073

Example Message: 'Minimum password change interval' setting successfully changed to '6' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016070   SNMP configuration

Explanation: The Simple Network Management Protocol (SNMP) configuration has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SNMP configuration successfully changed by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x00016071   DNS configuration

Explanation: The Domain Name System (DNS) configuration has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: DNS configuration successfully changed by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x00016072   SMTP server address is

Explanation: The Simple Mail Transfer Protocol (SMTP) configuration has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SMTP configuration successfully changed by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x00016073   LDAP configuration

Explanation: The Lightweight Directory Access Protocol (LDAP) configuration has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: LDAP configuration successfully changed by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x00016074   Trespass warning message has been

Explanation: The trespass warning message has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Trespass warning message has been enabled by 'USERID' from '192.168.0.1 (Web)'.
- Trespass warning message has been disabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016075   Trespass warning message changed by

Explanation: The trespass warning message has been changed by specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Trespass warning message changed by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016076   Account has been disabled for user

Explanation: The specified user account has been disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Account has been disabled for user 'TEST'.

User response: Information only; no action is required.

0x00016077   Account

Explanation: The specified user account has been created.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

0x00016078 • 0x0001607B

Recoverable: No

Example Message: Account successfully created for user 'test' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016078   Multiple concurrent remote video sessions per blade is

Explanation: The setting "Allow multiple concurrent remote video sessions per blade" has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Multiple concurrent remote video sessions per blade is enabled
- Multiple concurrent remote video sessions per blade is disabled

User response: Information only; no action is required.

0x00016079   NTP server host

Explanation: The Network Time Protocol (NTP) server host name or IP address has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: NTP server host successfully changed to '192.168.0.2' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001607A   NTP update frequency

Explanation: The Network Time Protocol (NTP) update frequency has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: NTP update frequency successfully changed to '60' minutes by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001607B   NTP v3 authentication

Explanation: The Network Time Protocol (NTP) v3 authentication has been is enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- NTP v3 authentication successfully disabled by 'USERID' from '192.168.0.1 (Web)'.
- NTP v3 authentication successfully enabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001607C   NTP v3 authentication settings

Explanation: The Network Time Protocol (NTP) v3 authentication settings have been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: NTP v3 authentication settings successfully changed by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001607D   The password

Explanation: The password has been changed for the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: The password successfully changed for user 'USERID' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001607E   The access rights

Explanation: The user authority level has been changed for the specified account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: The access rights successfully changed for user 'USERID' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001607F   Alert Recipient

Explanation: The remote alert recipient configuration has been modified or reset by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

0x00016080 • 0x00016082

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Alert Recipient 127 successfully changed by 'USERID' from '192.168.0.1 (Web)'. Status changed to enabled/disabled.
- Alert Recipient 127 successfully changed by 'USERID' from '192.168.0.1 (Web)'. Name changed to abcd.
- Alert Recipient 127 successfully changed by 'USERID' from '192.168.0.1 (Web)'. Method changed to SNMP over LAN/E-mail over LAN/IBM Director (comprehensive)/System Management Software (comprehensive).
- Alert Recipient 127 successfully changed by 'USERID' from '192.168.0.1 (Web)'. Address changed to 192.168.0.1.
- Alert Recipient 127 successfully changed by 'USERID' from '192.168.0.1 (Web)'. Filter changed to receives all alerts/receives critical alerts only.
- Alert Recipient 127 reset to defaults by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016080   Syslog filtering level has been changed to

Explanation: The severity filtering level has been changed for the syslog protocol.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Syslog filtering level has been changed to Warning by user 'USERID'.

User response: Information only; no action is required.

0x00016081   Syslog Collector 1 has been

Explanation: Syslog Collector 1 has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Syslog Collector 1 has been enabled by user 'USERID'.
- Syslog Collector 1 has been disabled by user 'USERID'.

User response: Information only; no action is required.

0x00016082   Syslog Collector 2 has been

Explanation: Syslog Collector 2 has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Syslog Collector 2 has been enabled by user 'USERID'.
- Syslog Collector 2 has been disabled by user 'USERID'.

User response: Information only; no action is required.

0x00016083   Hostname of Syslog Collector 1 has been changed to

Explanation: The hostname or IP address used for Syslog Collector 1 has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Hostname of Syslog Collector 1 has been changed to 10.10.10.30 by user 'USERID'.

User response: Information only; no action is required.

0x00016084   Hostname of Syslog Collector 2 has been changed to

Explanation: The hostname or IP address used for Syslog Collector 2 has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Hostname of Syslog Collector 2 has been changed to mysyslog.com by user 'USERID'.

User response: Information only; no action is required.

0x00016085   Port number of Syslog Collector 1 has been changed to

Explanation: The port number used for the Syslog Collector 1 has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Port number of Syslog Collector 1 has been changed to 515 by user 'USERID'.

User response: Information only; no action is required.

0x00016086   Port number of Syslog Collector 2 has been changed to

Explanation: The port number used for the Syslog Collector 2 has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

0x00016087 • 0x0001608A

Recoverable: No

Example Message: Port number of Syslog Collector 2 has been changed to 516 by user 'USERID'.

User response: Information only; no action is required.

0x00016087   SSH public key deleted

Explanation: The Secure Shell (SSH) public key has been deleted. A new SSH public key must be generated before any new SSH session can be established.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016088   SSH public key modified

Explanation: The Secure Shell (SSH)public key has been modified.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016089   SSH public key installed

Explanation: The Secure Shell (SSH) public key has been installed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001608A   SSH host key generation started

Explanation: The Secure Shell (SSH) host key generation has been started. Key generation normally completes in less than 2 minutes.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only. No action required.

0x0001608B   SSH host key generation failed

Explanation: The Secure Shell (SSH) host key generation failed.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Attempt to regenerate the host key again. See the Advanced Management Module User's Guide or the Advanced Management Module Command-Line Interface Reference for more information about SSH.

0x0001608C   SSH host key auto-generation started

Explanation: The Secure Shell (SSH) host key auto-generation has started. Key generation normally is completed in less than 2 minutes.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001608D   SSH host key auto-generation completed successfully

Explanation: The Secure Shell (SSH) host key auto-generation completed successfully. SSH clients that attempt to connect to the advanced management module may get a warning that the SSH key is unknown or an error that the key is not the same as the old key which is kept in their known_hosts file at the client.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001608E   SSH host key auto-generation failed

Explanation: The Secure Shell (SSH) host key auto-generation failed.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Attempt to generate the SSH host key. See the Advanced Management Module User's Guide or the Advanced Management Module Command-Line Interface Reference for more information about SSH

0x00016090   Maximum concurrent active sessions for

Explanation: The maximum concurrent active sessions for local users has been set.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Maximum concurrent active sessions for 'test' successfully changed to '3' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016091   Maximum concurrent active sessions, for LDAP login profile,

Explanation: The maximum concurrent active sessions has been set for the specified LDAP login profile.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Maximum concurrent active sessions, for LDAP login profile, successfully changed to '2' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016092   Login failed due to maximum number of concurrent sessions opened for

Explanation: Login failed for the specified user. The specified user already has the maximum number of concurrent sessions opened.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016093   Session for

Explanation: The specified user session has been terminated by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Session for 'test' from '192.168.0.2 (Web)', terminated by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x00016094   Local KVM switching

Explanation: Local KVM switching has been enabled or disabled by the specified user account. If disabled, users will not be able to switch KVM control from the front panel of a blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Local KVM switching disabled by user 'USERID' from 192.168.0.1 (Web)
- Local KVM switching enabled by user 'USERID' from 192.168.0.1 (Web)

User response: Information only; no action is required.

0x00016095   Local media tray switching

Explanation: Local media tray switching has been enabled or disabled by the specified user account. If disabled, users will not be able to switch media tray control from the front panel of a blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Local media tray switching disabled by user 'USERID' from 192.168.0.1 (Web)
- Local media tray switching enabled by user 'USERID' from 192.168.0.1 (Web)

User response: Information only; no action is required.

0x00016096   Remote media tray switching

Explanation: Remote media tray switching has been enabled or disabled by the specified user account. If disabled, users will not be able to switch media tray control remotely.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Remote media tray switching disabled by user 'USERID' from 192.168.0.1 (Web)
- Remote media tray switching enabled by user 'USERID' from 192.168.0.1 (Web)

User response: Information only; no action is required.

0x00016097   Local power control for blade

Explanation: Local power control for the specified blade server has been enabled or disabled by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

0x00016098 • 0x0001609A

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Local power control for blade 1 disabled by user 'USERID' from 192.168.0.1 (Web)
- Local power control for blade 1 enabled by user 'USERID' from 192.168.0.1 (Web)

User response: Information only; no action is required.

0x00016098   Local power control for all blades

Explanation: Local power control for the all blade servers has been enabled or disabled by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Local power control for all blades disabled by user 'USERID' from 192.168.0.1 (Web)
- Local power control for all blades enabled by user 'USERID' from 192.168.0.1 (Web)

User response: Information only; no action is required.

0x00016099   SSL server

Explanation: The secure socket layer (SSL) server has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- SSL server successfully disabled by 'USERID' from '192.168.0.1 (Web)'.
- SSL server successfully enabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001609A   SSL client

Explanation: The secure sockets layer (SSL) client has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- SSL client successfully disabled by 'USERID' from '192.168.0.1 (Web)'.
- SSL client successfully enabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0001609B   Standby MM SSL server

Explanation: The secure socket layer (SSL) server on the standby advanced management module has been enabled or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Standby MM SSL server successfully disabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.
- Standby MM SSL server successfully enabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x0001609C   SSL server certificate

Explanation: The advanced management module has detected that the SSL server certificate has been deleted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL server certificate successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x0001609D   SSL server certificate signing request

Explanation: The advanced management module has detected that the SSL server CSR has been created or deleted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL server certificate signing request successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x0001609E   SSL client certificate

Explanation: The advanced management module has detected that the SSL client certificate has been deleted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

0x0001609F • 0x000160A2

Recoverable: No

Example Message: SSL client certificate certificate successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x0001609F   SSL client certificate signing request

Explanation: The advanced management module has detected that the SSL client CSR has been created or deleted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL client certificate signing request successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160A0   Standby MM SSL server certificate

Explanation: The advanced management module has detected that the standby SSL server certificate has been deleted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Standby MM SSL server certificate successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160A1   Standby MM SSL server certificate signing request

Explanation: The advanced management module has detected that the alternate SSL server CSR has been created or deleted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Standby MM SSL server certificate signing request successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160A2   SSL server CA-signed certificate

Explanation: The advanced management module has detected that CA-signed certificate on the SSL server has been imported.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL server CA-signed certificate successfully imported by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only. No action required.

0x000160A3   SSL client CA-signed certificate

Explanation: The advanced management module has detected that CA-signed certificate on the SSL client has been imported.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL client CA-signed certificate successfully imported by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only. No action required.

0x000160A4   Standby MM SSL server CA-signed certificate

Explanation: The advanced management module has detected that CA-signed certificate on the standby SSL server has been imported.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Standby MM SSL server CA-signed certificate successfully imported by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160A5   SSL server self-signed certificate

Explanation: The advanced management module has detected that self-signed certificate on the SSL server has been created.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL server self-signed certificate successfully created by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only. No action required.

0x000160A6   SSL client self-signed certificate

Explanation: The advanced management module has detected that self-signed certificate on the SSL client has been created.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SSL client self-signed certificate successfully created by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only. No action required.

0x000160A7   Standby MM SSL server self-signed certificate

Explanation: The advanced management module has detected that self-signed certificate on the standby SSL server has been created.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Standby MM SSL server self-signed certificate successfully created by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160A8   SSL client trusted certificate 1

Explanation: The advanced management module has detected that the specified trusted certificate on the SSL client has been deleted/imported.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:

- SSL client trusted certificate 1 successfully imported by 'USERID' from '192.168.0.1 (Web)'.
- SSL client trusted certificate 1 successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160A9   SSL client trusted certificate 2

Explanation: The advanced management module has detected that the specified trusted certificate on the SSL client has been deleted/imported.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- SSL client trusted certificate 2 successfully imported by 'USERID' from '192.168.0.1 (Web)'.
- SSL client trusted certificate 2 successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160AA   SSL client trusted certificate 3

Explanation: The advanced management module has detected that the specified trusted certificate on the SSL client has been deleted/imported.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- SSL client trusted certificate 3 successfully imported by 'USERID' from '192.168.0.1 (Web)'.
- SSL client trusted certificate 3 successfully deleted by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only. No action required.

0x000160AB   Secure TCP Command mode

Explanation: The specified user account changed the maximum number of concurrent Secure TCP Command Mode connections.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Secure TCP Command mode successfully changed to '5' Connection(s) by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x000160AC   Test syslog generated

Explanation: A syslog test event was generated by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Test syslog generated by Web user 'USERID'

User response: This event is generated when the user clicks the Test Syslog button from the advanced management module user interface. If the test event was received by the syslog collector, no action is required. If it was not received:

1. Check that that syslog collector is configured correctly and that it is running.
2. Verify that the syslog collector can be reached from the advanced management module.

0x00016100   Login failed due to expired password for user

Explanation: The specified user cannot log in because the password has expired.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Login failed due to expired password for user 'USERID' from Web.

User response: Users (except SNMP an FTP users) will be prompted to change their password. SNMP and FTP users should log in using the Web interface or the command-line interface to change the password, or they should contact the administrator.

0x00016101   Security settings now require passwords. An SNMP v3 authentication protocol must be specified for user

Explanation: The security settings have been changed; and passwords are now required for all users. SNMPv3 users must specify an authentication protocol.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: All users must specify a password. SNMPv3 users must specify an authentication protocol (it cannot be set to None).

0x00016102   Login failed due to non-compliant password for user

Explanation: The password used to log in to the specified user account no longer meets the requirements for a password.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Login failed due to non-compliant password for user 'USERID' from Web.

User response: Users (except SNMP an FTP users) will be prompted to change their password. SNMP and FTP users should log in using the Web interface or the command-line interface to change the password, or they should contact the administrator.

0x00016103   Remote login failed, unsupported SNMPv3 security level for user

Explanation: The specified user cannot log in because either the authentication protocol or the security protocol setting is not correct.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Attempt to log in again, specifying the correct SNMPv3 privacy protocol and authentication protocol.

0x00016104   Remote login failed, SNMPv3 packet decryption error for user

Explanation: The specified user cannot log in because either the privacy password is incorrect or encryption is enabled and the privacy password cannot be decrypted.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Perform these steps:

1. Log in again, making sure that you specify the correct SNMPv3 privacy password.
2. Log in to the advanced management module through either the Web interface or the command-line interface (CLI) and reset the SNMPv3 privacy password.

0x00016105   Remote login failed, password required for user

Explanation: The specified user cannot log in because the user did not specify a password, and a password is required.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Attempt to log in again, specifying a valid password. See the Advanced Management Module User's Guide for more information about user accounts and passwords.

0x00016201   Blade Bay Data for bay 01 uploaded to AMM.

Related messages:
- 0x00016202 : Blade Bay Data for bay 02 uploaded to AMM.
- 0x00016203 : Blade Bay Data for bay 03 uploaded to AMM.
- 0x00016204 : Blade Bay Data for bay 04 uploaded to AMM.
- 0x00016205 : Blade Bay Data for bay 05 uploaded to AMM.
- 0x00016206 : Blade Bay Data for bay 06 uploaded to AMM.
- 0x00016207 : Blade Bay Data for bay 07 uploaded to AMM.
- 0x00016208 : Blade Bay Data for bay 08 uploaded to AMM.
- 0x00016209 : Blade Bay Data for bay 09 uploaded to AMM.
- 0x0001620A : Blade Bay Data for bay 10 uploaded to AMM.
- 0x0001620B : Blade Bay Data for bay 11 uploaded to AMM.
- 0x0001620C : Blade Bay Data for bay 12 uploaded to AMM.
- 0x0001620D : Blade Bay Data for bay 13 uploaded to AMM.
- 0x0001620E : Blade Bay Data for bay 14 uploaded to AMM.

Explanation: Blade bay data for the specified blade server bay has been uploaded to the advanced management module. This data is stored in the advanced management module non-volatile RAM (NVRAM), and is associated with the BladeCenter unit blade bay.

0x00016301 • 0x00016310

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016301   Blade Bay Data

Related messages:
- 0x00016302 : Blade Bay Data
- 0x00016303 : Blade Bay Data
- 0x00016304 : Blade Bay Data
- 0x00016305 : Blade Bay Data
- 0x00016306 : Blade Bay Data
- 0x00016307 : Blade Bay Data
- 0x00016308 : Blade Bay Data
- 0x00016309 : Blade Bay Data
- 0x0001630A : Blade Bay Data
- 0x0001630B : Blade Bay Data
- 0x0001630C : Blade Bay Data
- 0x0001630D : Blade Bay Data
- 0x0001630E : Blade Bay Data

Explanation: Blade bay data for the specified blade server has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Blade Bay Data successfully changed for bay 01 by 'USERID' from '192.168.0.1 (Web)'.
- There was an error changing blade Bay Data for bay 01 by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x00016310   SLP mode

Explanation: The address type for the Service Location Protocol (SLP) server has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SLP mode successfully changed to broadcast by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016311   SLP address

Explanation: The IP address for the Service Location Protocol (SLP) server has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SLP address successfully changed to 239.255.255.253 by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016400   Invalid encryption keys detected. Regenerating encryption keys. Verify local login profile configurations

Explanation: The advanced management module has detected that encryption keys are not valid. It will regenerate encryption keys.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Attempt to log in again.
2. Verify local login configuration and authentication keys.

0x00016401   Invalid login profile. Reconfigure the password for user

Explanation: The login profile for the specified user account is not valid because of a problem with the password.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Attempt to log in again using the specified user account.
2. Contact the system administrator to reconfigure the password.

0x00016402   Invalid login profile. Reconfigure the privacy password for user

Explanation: The login profile for the specified user account is not valid because of a problem with the SNMPv3 privacy password.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

0x00016500 • 0x00016702

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Log in through the Web interface or the command-line interface to reset the SNMPv3 privacy password.

0x00016500   File Transfer Failed

Explanation: The file cannot be transferred to the advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: File Transfer Failed for user 'USERID' from '192.168.0.1 (Web)'. Unsupported protocol.

User response: Perform these steps:
1. Verify that the filename was entered correctly and that permissions are set correctly.
2. Verify that you can see the file on the network.
3. Verify that the advanced management module has sufficient space to store the file. From the advanced management module Web interface, go to the File Management tab to determine how much space is available. A list of files that can be deleted to make more space is also displayed.

   Refer to the Advanced Management Module User's Guide for more information about the File Management tab. The guide is available on the Web.

0x00016700   Call Home

Explanation: Call home functionality used by Service Advisor has been enabled or disabled. If enabled, a test call home message will be generated automatically.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Call Home successfully disabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.
- Call Home successfully enabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x00016702   HTTP Proxy for Call Home

Explanation: The HTTP proxy used by Service Advisor has been changed, enabled, or disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:

- The HTTP Proxy for Call Home successfully disabled by 'USERID' from '192.168.0.1 (Web)'.
- The HTTP Proxy for Call Home successfully enabled by 'USERID' from '192.168.0.1 (Web)'.
- The location of HTTP Proxy for Call Home successfully changed to 'abcd' by 'USERID' from '192.168.0.1 (Web)'.
- The port of HTTP Proxy for Call Home successfully changed from '8080' to '8090' by 'USERID' from '192.168.0.1 (Web)'.
- The username of HTTP Proxy for Call Home successfully changed to 'test' by 'USERID' from '192.168.0.1 (Web)'.
- The password of HTTP Proxy for Call Home successfully changed by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x00016704   **Terms and Conditions of Service Advisor have been accepted**

Explanation: The license agreement for Service Advisor has been accepted by the specified user.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00016705   **for Call Home changed to**

Explanation: The Service Advisor configuration required by Call Home has been changed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Company Name of contact information for Call Home changed to 'My company' by 'USERID'.

User response: Information only; no action is required.

0x00016706   **Invalid configuration for Call Home is not saved.**

Explanation: Service Advisor detected that a user tried to save incorrect configuration required by Call Home. Invalid data will not be saved.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Invalid configuration for Call Home is not saved. Company Name: .

User response: Correct the Call Home configuration and retry.

0x00016800   **Call Home generated Service Request Number**

Explanation: The call home of the specified event was successful, and the specified service request number was generated.

Severity: Informational

0x00016801 • 0x00016802

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Event 0x00026a02 Call Home generated Service Request Number '7060167ZTK' for 'Cool_02 '.

User response: Information only; no action is required.

0x00016801   Call Home failed

Explanation: The attempt to call home the specified event was not successful.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message:
- Event 0x00026801 Call Home failed for 'SERVPROC'. Connection Path Error. Please verify network setup.
- Event 0x00026801 Call Home failed for 'SERVPROC'. [114] Electronic Service not available at selected Support
- Event 0x00026801 Call Home failed for 'SERVPROC'. [1020] Invalid value 'AB' in field 'MACHINE_TYPE'.
- Event 0x00026801 Call Home failed for 'SERVPROC'. [1110] Authentication Error. Please verify Service Advisor settings and test call home.
- Event 0x00026801 Call Home failed for 'SERVPROC'. Authentication Error. Please verify Service Advisor settings and test call home.
- Event 0x00026801 Call Home failed for 'SERVPROC'. [9001] General Error.
- Event 0x00026801 Call Home failed for 'SERVPROC'. General Error.

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Verify that the proxy settings for Service Advisor are correct.
2. Attempt to perform a test call home.
3. Check the network connectivity between the advanced management module and the external Internet.

0x00016802   Test Call Home generated

Explanation: A test call home event was generated, either manually or by enabling Service Advisor. Because this is a test, an actual problem report is not being generated by this call, and no service personnel will be contacting you.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: No

Example Message: Test Call Home generated by USERID.

User response: Information only; no action is required.

Note to service personnel:

If a call home message is received for this event, you can close the call. This is a test call; no action is required.

0x00016803   Call Home

Explanation: A call home event was generated by the specified user account.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: No

Example Message: Call Home by USERID: it is a manual call home

User response: Information only; no action is required.

Note to service personnel:

Read manual description provided and review the log that is generated with this event. Then, place a call to the customer.

0x00017001   Alarm Panel LED does not match with the system management states.

Explanation: The state of the alarm panel minor or major LED does not match one of the system management states on the BladeCenter HT chassis.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Reseat the alarm panel.

0x00017002   Management module reset.

Explanation: The advanced management module has been reset.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00017003   There are no valid login profiles. Resetting login profile 1 to factory defaults.

Explanation: The advanced management module requires at least one valid login profile (user account). If none are found, the first user profile will be enabled with the default user name and password.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required. Login profiles can be created through the advanced management module user interface.

Chapter 2. Messages   **93**

0x00017004   There are no login profiles with Supervisor or User Account Management roles.

Explanation: The advanced management module requires that at least one login profile (user account) have the authority to manage user accounts. Therefore, the advanced management module has given that authority to the specified user account.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: There are no login profiles with Supervisor or User Account Management roles. Assigning User Account Management role to login profile 1.

User response: Information only; no action is required. Roles for login profiles can be modified through the advanced management module user interface.

0x00017100   requested to shut down OS and power off blade

Explanation: The specified user requested that the operating system for the specified blade server be shut down and the blade server be powered off.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' requested to shut down OS and power off blade 01

User response: Information only; no action is required.

0x00017101   requested NMI reset for blade

Explanation: The specified user requested a Non-Maskable Interrupt (NMI) reset for a specified blade.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' requested NMI reset for blade 01

User response: Information only; no action is required.

0x00017102   New chassis detected, reading configuration from midplane

Explanation: The advanced management module has been installed in a chassis that is different from the last chassis in which it was installed. The advanced management module will attempt to use the configuration settings previously saved on the chassis, if available.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00017103   Both management modules are active. Resetting MM.

Explanation: Both advanced management modules are identified as primary, so they will both be reset.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00017104   Cannot determine management module bay location, defaulting to bay 1.

Explanation: The advanced management module is unable to determine the management module bay in which it is installed. Therefore, it will use management module bay 1 as the installed bay.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the advanced management module.
2. Install the advanced management module in the other management module bay, if available.

0x00017105   Management module switch over from bay 1 to bay 2.

Explanation: The advanced management module in management module bay 1 has failed over to the advanced management module in management module bay 2. The advanced management module in module bay 2 is now the primary advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Check the event log for other events related to the advanced management module in management module bay 1 and resolve those events.

0x00017106   Management module switch over from bay 2 to bay 1.

Explanation: The advanced management module in management module bay 2 has failed over to the advanced management module in management module bay 1. The advanced management module in module bay 1 is now the primary advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Check the event log for other event related to the advanced management module in management module bay 2 and resolve those events.

0x00017107   Power state restored after an unexpected power loss.

Explanation: The power state to the specified blade server has been restored after an unexpected power loss.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that might be related to the blade server or to power modules.

0x00017108   interface is now active.

Explanation: The advanced management module external Ethernet interface is functioning.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Ethernet[0] interface is now active

User response: Information only; no action is required.

0x00017109   interface is no longer active.

Explanation: The advanced management module external Ethernet interface is not functioning.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Ethernet[0] interface is no longer active

User response: Perform these steps:
1. Make sure that the external Ethernet cable is connected on both ends.
2. Verify that the cable is working:
   a. Swap both ends of the cable.
   b. Verify that there is a link LED lit on the RJ-45 connector on the advanced management module and the network device to which the advanced management module is attached.
3. Verify that the network switch has power.

0x0001710A   Starting background firmware transfer of Standby Management Module

Explanation: The transfer of firmware from the primary advanced management module to the standby advanced management module has started.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0001710B   Firmware update of Standby Management Module

Explanation: The firmware update from the primary advanced management module to the standby advanced management module has been cancelled because the standby has become the new primary advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required. The new primary advanced management module will attempt to update the firmware on the new standby advanced management module.

0x0001710C   Firmware transfer of Standby Management Module

Explanation: The transfer of firmware from the primary advanced management module to the standby advanced management module failed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Firmware transfer of Standby Management Module from MM 1 to MM 2 failed

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:
1. Reseat the standby advanced management module.
2. Fail over the primary advanced management module to the standby advanced management module.
3. Update the firmware on the new primary advanced management module through the advanced management module user interface.

0x0001710D   I/O module Protected Mode configured

Explanation: The protected mode setting on the specified I/O module has changed.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Example Message: I/O module Protected Mode configured by user 'USERID' from '9.37.177.105(TCP Cmd)'

User response: Information only; no action is required.

0x0001710E   Firmware update detected for blade service processor.

Explanation: >A service processor firmware for the specified blade service is being updated.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x0001710F   I/O module has restarted.

Explanation: The specified I/O module has been restarted.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00017111   uploaded from

Explanation: The specified user uploaded a file to the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- File 'CNETCMUS.pkt' uploaded from FTP client at 9.123.198.70 by 'USERID'
- File 'CNETCMUS.pkt' uploaded from TFTP client at 9.123.198.70

User response: Information only; no action is required.

0x00017112   Configuration restored from a configuration file by user

Explanation: The specified user restored the advanced management module configuration from a previously saved configuration file. Some configuration settings might require that the advanced management module be restarted before they take effect.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Configuration restored from a configuration file by user 'USERID'

User response: Information only; no action is required.

0x00017113   ENET DHCP-HstNme=%s,DN=%s,IP@=%s,GW@=%s,SN=%s,DNS1@=%s.

Explanation: The external Ethernet port on the advanced management module is using a DHCP IP address for the specified hostname. The host name, IP address, gateway address and network mask are provided.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: ENET DHCP Hstme=,DN=raliegh.datacentertech.net,IP@=10.12.200.14,GW@=10.12.1.1,SN=255.255.255.0,DNS1@=10.12.100.108

User response: Information only; no action is required.

0x00017114   ENET Hostname=%s, IP=%s, GW=%s, Mask=%s.

Explanation: The external Ethernet port on the advanced management module is using a static IP address for the specified hostname. The host name, IP address, gateway address and network mask are provided.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: ENET Hostname=MM000000C30596,IP=10.10.11.12,GW=10.10.11.14,MASK=255.255.255.0

User response: Information only; no action is required.

0x00017115   DHCP setting has been changed

Explanation: The specified user changed the DHCP setting of the advanced management module external network interface.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: DHCP setting has been changed to 'Disabled - Use static IP configuration' by 'USERID'

User response: Information only; no action is required.

0x00017116   %s AMM hostname has been changed %s

Explanation: The specified user changed the hostname of the advanced management module to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

0x00017117 • 0x00017119

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Primary AMM hostname has been changed from 'ABC' to 'DEF' by user 'USERID' from '10.12.200.35 (Web)'

User response: Information only; no action is required.

0x00017117   IP address of network interface has been changed

Explanation: The specified user changed the IP address of the advanced management module external network interface to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IP address of network interface has been changed from '9.123.198.14' to '9.123.253.14' by 'USERID'.

User response: Information only; no action is required.

0x00017118   Ethernet data rate of network interface has been changed

Explanation: The specified user changed Ethernet data rate of the advanced management module external network interface to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Ethernet data rate of network interface has been changed from '100Mb' to 'Auto' by 'USERID'

User response: Information only; no action is required.

0x00017119   Ethernet duplex setting of network interface has been changed

Explanation: The specified user changed the Ethernet duplex setting of the advanced management module external network interface to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Ethernet duplex setting of network interface has been changed from 'Full' to 'Auto' by 'USERID'.

User response: Information only; no action is required.

0x0001711A   Ethernet locally administered MAC address of network interface has been changed

Explanation: The specified user changed the Ethernet locally administered MAC address of the advanced management module external network interface to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Ethernet locally administered MAC address of network interface has been changed from '00:00:58:7f:00:98' to '00:00:59:4f:00:90' by 'USERID'.

User response: Information only; no action is required.

0x0001711B   Gateway address of network interface has been changed

Explanation: The specified user changed the gateway address of the advanced management module external network interface to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Gateway address of network interface has been changed from '9.123.198.1' to '9.123.253.1' by 'USERID'.

User response: Information only; no action is required.

0x0001711C   Ethernet MTU setting of network interface has been changed

Explanation: The specified user has changed the Ethernet maximum transmission unit (MTU) setting of the advanced management module external network interface to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Ethernet MTU setting of network interface has been changed from '1400' to '1500' by 'USERID'

User response: Information only; no action is required.

0x0001711D   Subnet mask of network interface has been changed

Explanation: The specified user changed the subnet mask of the advanced management module external network interface to the specified value.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Subnet mask of network interface has been changed from '255.255.255.0' to '255.255.254.0' by 'USERID'

User response: Information only; no action is required.

0x00018001   The following process has been permanently disabled due to a recurring internal error: %s

Explanation: An internal error in the specified process has caused the function to be disabled.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Perform these steps:
1. Check the IBM Support Web page for any service bulletins that might be related to failures of this process/function.
2. Check to see if a core file exists for the indicated process and retrieve it for IBM support.
3. If possible, attempt to try the operation again from the advanced management module.

0x0001C482   Chassis ambient over temperature fault

Explanation: The current chassis temperature is above the recommended ambient temperature for this chassis.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
4. Make sure that there is nothing covering the media tray (that will disrupt the airflow to the ambient temperature sensor).
5. Replace the media tray.

0x0001C500   Management module over temperature

Explanation: The advanced management module has exceeded the temperature fault threshold.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Check the event log for other over temperature events and resolve them.

2. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.

3. Make sure that all fan/blower modules are running. Replace fan modules if necessary.

4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

5. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x0001C800   System ambient under temperature fault.

Explanation: The ambient temperature for the chassis has fallen below the temperature fault threshold.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: From the System Status Summary page of the advanced management module Web interface, click the status icon to display the temperature readings for each of the chassis components.

- If the values for all components are in low range of the operating temperature, raise the ambient temperature in the room.

- If all other temperature readings are in the normal operating range, perform these steps:

  1. Reseat the media tray.

  2. Restart the advanced management module.

0x0001D400   Management module is over recommended temperature.

Explanation: The advanced management module has exceeded the recommended temperature threshold.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Check the event log for other over temperature events and resolve them.

2. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.

3. Make sure that all fan/blower modules are running. Replace fan modules if necessary.

4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

5. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x0001D502   Chassis over recommended ambient temperature.

Explanation: The current chassis temperature is above the recommended ambient temperature for this chassis.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:
1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
4. Make sure that there is nothing covering the media tray (that will disrupt the airflow to the ambient temperature sensor).
5. Replace the media tray.

0x0001D800   System under recommended ambient temperature

Explanation: The ambient temperature for the chassis has fallen below the recommended temperature threshold.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT):   Minor

User response: From the System Status Summary page of the advanced management module Web interface, click the status icon to display the temperature readings for each of the chassis components.
- If the values for all components are in low range of the operating temperature, raise the ambient temperature in the room.
- If all other temperature readings are in the normal operating range, perform these steps:
  1. Hot swap the media tray.
  2. Restart the advanced management module.

0x00020000   Failure reading device on system management bus 00.

Related messages:
- 0x00020001 : Failure reading device on system management bus 01.
- 0x00020002 : Failure reading device on system management bus 02.
- 0x00020003 : Failure reading device on system management bus 03.
- 0x00020004 : Failure reading device on system management bus 04.
- 0x00020005 : Failure reading device on system management bus 05.
- 0x00020006 : Failure reading device on system management bus 06.
- 0x00020007 : Failure reading device on system management bus 07.

- 0x00020008 : Failure reading device on system management bus 08.
- 0x00020009 : Failure reading device on system management bus 09.
- 0x0002000A : Failure reading device on system management bus 10.
- 0x0002000B : Failure reading device on system management bus 11.
- 0x0002000C : Failure reading device on system management bus 12.
- 0x0002000D : Failure reading device on system management bus 13.
- 0x0002000E : Failure reading device on system management bus 14.
- 0x0002000F : Failure reading device on system management bus 15.
- 0x00020010 : Failure reading device on system management bus 16.
- 0x00020011 : Failure reading device on system management bus 17.
- 0x00020012 : Failure reading device on system management bus 18.
- 0x00020013 : Failure reading device on system management bus 19.
- 0x00020014 : Failure reading device on system management bus 20.
- 0x00020015 : Failure reading device on system management bus 21.
- 0x00020016 : Failure reading device on system management bus 22.
- 0x00020017 : Failure reading device on system management bus 23.
- 0x00020018 : Failure reading device on system management bus 24.
- 0x00020019 : Failure reading device on system management bus 25.
- 0x0002001A : Failure reading device on system management bus 26.
- 0x0002001B : Failure reading device on system management bus 27.
- 0x0002001C : Failure reading device on system management bus 28.
- 0x0002001D : Failure reading device on system management bus 29.
- 0x0002001E : Failure reading device on system management bus 30.
- 0x0002001F : Failure reading device on system management bus 31.
- 0x00020020 : Failure reading device on system management bus 32.
- 0x00020021 : Failure reading device on system management bus 33.
- 0x00020022 : Failure reading device on system management bus 34.
- 0x00020023 : Failure reading device on system management bus 35.
- 0x00020024 : Failure reading device on system management bus 36.
- 0x00020025 : Failure reading device on system management bus 37.
- 0x00020026 : Failure reading device on system management bus 38.
- 0x00020027 : Failure reading device on system management bus 39.
- 0x00020028 : Failure reading device on system management bus 40.
- 0x00020029 : Failure reading device on system management bus 41.
- 0x0002002A : Failure reading device on system management bus 42.
- 0x0002002B : Failure reading device on system management bus 43.
- 0x0002002C : Failure reading device on system management bus 44.
- 0x0002002D : Failure reading device on system management bus 45.
- 0x0002002E : Failure reading device on system management bus 46.
- 0x0002002F : Failure reading device on system management bus 47.
- 0x00020030 : Failure reading device on system management bus 48.
- 0x00020031 : Failure reading device on system management bus 49.
- 0x00020032 : Failure reading device on system management bus 50.
- 0x00020033 : Failure reading device on system management bus 51.
- 0x00020034 : Failure reading device on system management bus 52.
- 0x00020035 : Failure reading device on system management bus 53.
- 0x00020036 : Failure reading device on system management bus 54.

Explanation: The advanced management module cannot communicate with a device over the I2C bus. Typically, this

0x00022001 • 0x00022002

is because a component on the specified device I2C bus cannot respond to the advanced management module.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. If you have only one advanced management module installed and your chassis supports two management modules, try the management module in the other advanced management module bay.
2. Reseat the specified device (such as I/O module or power module).
3. Reseat the advanced management module.
4. Check the IBM Support Web page for any service bulletins that might be related to this problem.
5. Check the event log for additional errors related to the system management bus:
    a. If there are no other system management bus errors, replace the specified device.
    b. If there are system management bus errors for multiple components, replace the advanced management module.

0x00022001   Blade management bus 1 failed.

Explanation: An internal communication bus on the primary advanced management module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Reseat the advanced management module.
2. Initiate a failover to the other advanced management module, if possible. You can initiate a failover to the other advanced management module using the advanced management module Web interface. See the Advanced Management Module User's Guide for more information.
3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x00022002   Blade management bus 2 failed.

Explanation: An internal communication bus on the advanced management module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. If the primary advanced management module is the active advanced management module, check the IBM Support Web page for any service bulletins that might be related to this problem.

2. If the standby advanced management module is the active advanced management module, perform these steps:

   a. Reseat the advanced management module.

   b. Initiate a failover to the other advanced management module, if possible. You can initiate a failover to the other advanced management module using the advanced management module Web interface. See the Advanced Management Module User's Guide for more information.

   c. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x00022003   Primary MM real-time clock failed.

Explanation: The primary advanced management module real-time clock failed during built-in self test (BIST). Time stamps displayed in the event log may not be accurate.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Restart the advanced management module.

2. Replace the advanced management module with the failed real-time clock.

0x00022004   Primary MM local management bus failed.

Explanation: An internal management bus on the primary advanced management module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Restart the advanced management module.

2. Flash (update if applicable) the firmware for the advanced management module and restart the advanced management module.

3. Fail over to the standby advanced management module if available. Then reseat the advanced management module that had the error. Fail back to see if error persists. If a standby advanced management module is not present, reseat the advanced management module.

4. Replace the failed advanced management module.

0x00022005 • 0x00022007

0x00022005   Primary MM primary file system failed.

Explanation: The primary firmware image for the primary advanced management module failed during built-in self test (BIST); it may be corrupt. The advanced management module will run the backup firmware image, which may not be the same level as the primary image.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
2. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022006   Primary MM secondary file system failed.

Explanation: The backup firmware image on the primary advanced management module failed during built-in self test (BIST); it may be corrupt. The advanced management module will run the primary firmware image, but if the primary firmware image fails, a backup will not be available.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
2. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022007   Primary MM bootrom failed.

Explanation: Primary Management Module boot ROM has failed. It might be corrupted.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
2. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022008   Primary MM Ethernet port 0 failed.

Explanation: Ethernet port 0 on the primary advanced management module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the event log for a recovery message. If present, no action is required.
2. Restart the advanced management module.
3. Flash (update if applicable) the firmware for the advanced management module and restart the advanced management module.
4. Fail over to the standby advanced management module if available. Then reseat the advanced management module that had the error. Fail back to see if error persists. If the standby advanced management module is not present, reseat the advanced management module.

0x00022009   Primary MM external management bus timed out and was reset.

Explanation: There was a communications problem on the advanced management module external communication bus. The bus has been reset.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x0002200A   Primary MM internal ethernet switch failed.

Explanation: Ethernet port 0 on the primary advanced management module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the event log for a recovery message, if so, no action is required.
2. Contact IBM.

0x0002200B   Primary MM video capture failed.

Explanation: Primary MM video capture has failed. However Video Capture on the AMM is used for displaying the video remotely and may not affect local users.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
2. Reseat the advanced management module.
3. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022011   Primary MM USB keyboard/mouse emulation failed.

Explanation: The USB keyboard/mouse emulation for the advanced management module failed during built-in self test (BIST).

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Restart the advanced management module.
2. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
3. Replace the advanced management module.

0x00022012   Primary MM USB mass storage emulation failed.

Explanation: The USB mass storage emulation for the advanced management module failed during built-in self test (BIST).

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Restart the advanced management module.
2. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
3. Replace the advanced management module.

0x00022015   Standby MM real-time clock failed.

Explanation: The standby (redundant) advanced management module real-time clock failed during built-in self test (BIST).

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:
1. Restart the standby advanced management module.
2. Flash (update if applicable) the firmware for the advanced management module and restart the advanced management module.
3. Reseat the standby advanced management module.
4. Replace the standby advanced management module.

0x00022016   Standby MM local management bus failed.

Explanation: An internal management bus on the standby (redundant) advanced management module has failed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:
1. Restart the standby advanced management module.
2. Flash (update if applicable) the firmware for the advanced management module and restart the advanced management module.
3. Reseat the standby advanced management module.
4. Replace the standby advanced management module.

0x00022017   Standby MM primary file system failed.

Explanation: The primary firmware image for the standby advanced management module failed during built-in self test (BIST); it may be corrupt.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

0x00022018 • 0x00022019

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps at your earliest convenience:

1. Update the firmware for the advanced management module. You might need to initiate a failover to make this advanced management module the primary advanced management module to update the firmware.
2. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022018   Standby MM secondary file system failed.

Explanation: The backup firmware image on the standby primary advanced management module failed during built-in self test (BIST); it may be corrupt.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps at your earliest convenience:

1. Update the firmware for the advanced management module. You might need to initiate a failover to make this advanced management module the primary advanced management module to update the firmware.
2. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022019   Standby MM internal I/O expander failed.

Explanation: The internal I/O Expander on the standby advanced management module failed during built-in self test (BIST).

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Restart the standby advanced management module.
2. Flash (update if applicable) the firmware for the advanced management module and restart the advanced management module.
3. Reseat the standby advanced management module.
4. Replace the standby advanced management module.

0x0002201B   Standby MM bootrom failed.

Explanation: The standby MM boot ROM has failed. It may due to the corrupted boot ROM.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Users can update the standby MM firmware. If it does not work, it is possibly a MM hardware problem. Call IBM for help or possible parts replacement.

0x0002201C   Standby MM ethernet port 0 failed.

Explanation: Ethernet port 0 on the standby advanced management module has failed during built in self test (BIST).

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the Ethernet connection from the standby advanced management module (the one without the active light at the back of the chassis) to ensure that the Ethernet connection is functional.
2. Make sure the Ethernet cable is properly seated at both ends.
3. Try another Ethernet cable.
4. Make sure the Ethernet switch at the other end is active and working (try another port or other switch).
5. Generate a manual call home using Service Advisor.

0x0002201D   Standby MM internal ethernet switch failed.

Explanation: Ethernet port 0 on the standby advanced management module has failed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the Ethernet connection from the standby advanced management module (the one without the active light at the back of the chassis) to ensure that the Ethernet connection is functional.
2. Make sure the Ethernet cable is properly seated at both ends.

3. Try another Ethernet cable.
4. Make sure the Ethernet switch at the other end is active and working (try another port or other switch).
5. Generate a manual call home using Service Advisor.

0x0002201E   Alternate MM communication failed.

Explanation: The primary advanced management module cannot communicate with the standby advanced management module.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Restart the primary advanced management module.
2. Restart the standby advanced management module.
3. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
4. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022049   BIST blade management bus 1 failed.

Explanation: An internal communication bus on the standby advanced management module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Restart the primary advanced management module.
2. Restart the standby advanced management module.
3. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
4. Generate a manual call home using Service Advisor to replace the advanced management module.

0x0002204A   BIST blade management bus 2 failed.

Explanation: An internal communication bus on the standby advanced management module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Restart the primary advanced management module.
2. Restart the standby advanced management module.
3. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
4. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022052   Standby MM primary core failed.

Explanation: The primary core on the standby advanced management module failed during built-in self test (BIST). This event is typically caused by an issue with the firmware image itself. Reloading the firmware image will normally correct the situation.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps at your earliest convenience:

1. Restart the primary advanced management module.
2. Restart the standby advanced management module.
3. Initiate a failover to the standby advanced management module and either reload the advanced management module firmware or update the firmware to the latest level. After reloading or updating the firmware, you will need to restart the advanced management module.
4. Reseat the advanced management module.
5. Reload or update the advanced management module firmware again. After reloading or updating the firmware, you will need to restart the advanced management module.
6. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022053   Standby MM backup core failed.

Explanation: The backup core on the standby advanced management module failed during built-in self test (BIST). This event is typically caused by an issue with the firmware image itself. Reloading the firmware image will normally correct the situation.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps at your earliest convenience:

1. Restart the primary advanced management module.
2. Restart the standby advanced management module.

0x00022054 • 0x00022055

3. Initiate a failover to the standby advanced management module and either reload the advanced management module firmware or update the firmware to the latest level.

4. Reseat the advanced management module.

5. Reload or update the advanced management module firmware again.

6. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022054   Primary MM USB keyboard/mouse firmware failed.

Explanation: The USB keyboard/mouse firmware update on the primary advanced management module has failed because the advanced management module could not access the firmware storage.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Verify that the keyboard and mouse are functioning correctly (either the remote keyboard and mouse, or the keyboard and mouse that are attached to the advanced management module). If so, no action is required.

If the keyboard and mouse are not functioning correctly, perform these steps:

1. Restart the advanced management module.

2. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.

3. Reseat the advanced management module.

4. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022055   Primary MM USB mass storage firmware failed.

Explanation: The primary advanced management module mass storage firmware update on the primary advanced management module has failed because the advanced management module could not access the firmware storage.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Verify that the remote drive is still functioning correctly. If so, no action is required.

If the remote drive is not functioning correctly, perform these steps:

1. Restart the advanced management module.

2. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.

3. Reseat the advanced management module.

4. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022058   **Primary MM primary core failed.**

Explanation: The primary core on the primary advanced management module failed during built-in self test (BIST). The advanced management module will run the backup firmware image.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
2. Reseat the advanced management module.
3. Generate a manual call home using Service Advisor to replace the advanced management module.

0x00022059   **Primary MM backup core failed.**

Explanation: Primary MM backup core has failed. It may due to the corrupted core which has CRC error. The advanced management module will run the primary firmware image.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Update the firmware for the advanced management module. After updating the firmware, you will need to restart the advanced management module.
2. Reseat the advanced management module.
3. Generate a manual call home using Service Advisor to replace the advanced management module.

0x0002205A   **Primary MM internal I/O expander failed.**

Explanation: The internal I/O Expander on the primary advanced management module failed during built-in self test (BIST).

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform this steps:

0x00026801 • 0x00026A01

1. Restart the advanced management module.
2. Flash (update if applicable) the firmware for the advanced management module and restart the advanced management module.
3. Fail over to the standby advanced management module if available. Then reseat the advanced management module that had the error. Fail back to see if the error persists. If the standby advanced management module is not present, reseat the advanced management module.
4. Replace the failed advanced management module.

0x00026801   Chassis Cooling Device 01 failure.

Related messages:
- 0x00026802 : Chassis Cooling Device 02 failure.
- 0x00026803 : Chassis Cooling Device 03 failure.
- 0x00026804 : Chassis Cooling Device 04 failure.
- 0x00026805 : Chassis Cooling Device 05 failure.
- 0x00026806 : Chassis Cooling Device 06 failure.
- 0x00026807 : Chassis Cooling Device 07 failure.
- 0x00026808 : Chassis Cooling Device 08 failure.
- 0x00026809 : Chassis Cooling Device 09 failure.
- 0x0002680A : Chassis Cooling Device 10 failure.

Explanation: The specified fan or blower module is no longer operating.

Severity: Error

Alert Category: Cooling Devices (Critical) - mmTrapFanC

Log Source: Cool_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Check to make sure that the rear fan or blower module is receiving power. To do this, check the System Status page through the advanced management module Web interface.

   Note: The BladeCenter T chassis has an illuminated green power LED when power is present. An amber LED indicates lack of power or a failed component.
2. Check your power source and cabling.

   Note: All power cords must be attached.
3. Reseat the fan or blower module.
4. Replace the fan or blower module.

0x00026A01   Chassis Cooling Device 01 failure.

Related messages:
- 0x00026A02 : Chassis Cooling Device 02 failure.
- 0x00026A03 : Chassis Cooling Device 03 failure.
- 0x00026A04 : Chassis Cooling Device 04 failure.

Explanation: The specified fan or blower module is no longer operating.

Severity: Error

Alert Category: Cooling Devices (Critical) - mmTrapFanC

Log Source: Cool_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Check to make sure that the rear fan or blower module is receiving power. To do this, check the System Status page through the advanced management module Web interface.

   Note: The BladeCenter T chassis has an illuminated green power LED when power is present. An amber LED indicates lack of power or a failed component.

2. Check your power source and cabling.

   Note: All power cords must be attached.

3. Reseat the fan or blower module.

4. Replace the fan or blower module.

0x00028000   Power fault

Explanation: The specified blade server has encountered a power fault.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Check the event log to see if this is happening on multiple blades. If so, suspect the power module. See the IBM Support Web page for service bulletins related to troubleshooting power issues.

2. If this is happening for a single blade server:
   a. Update the systems management firmware (BMC) for the blade server through the advanced management module Web interface.
   b. Reseat the blade server.
   c. Replace the system board (trained service technician only).

0x00028001   Blade power fault

Explanation: A power fault has occurred for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: If the call home to IBM was successful, you can expect a service call from IBM. In the meantime, perform these steps:

1. If the over voltage problem is occurring on multiple blade servers, look for other events in the log related to power and resolve those events. See the IBM Support Web page for service bulletins related to troubleshooting power issues.

2. If this event is isolated to a single blade server, replace the system board (trained service technician only).

0x00029400   Power module 3 or 4 is required to power blades in power domain 2.

Related messages:

*   0x00029402 : Power module 3 or 4 is required to power blades in power domain 2.

Explanation: A blade server has been installed in a blade server bay that receives power from power module bay 3 or power module bay 4. Power modules are not detected in either of those bays.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Make sure that you have a functioning power module installed in power module bay 3 and power module bay 4.

0x00029401   Power module 1 or 2 is required to power blades in power domain 1.

Explanation: A blade server has been installed in a blade server bay that receives power from power module bay 1 or power module bay 2. Power modules are not detected in either of those bays. (BladeCenter H and BladeCenter HT only, the BladeCenter E and BladeCenter T chassis require power modules in power domain 1 for the advanced management module to be active)

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Make sure that you have a functioning power module installed in power module bay 1 or power module bay 2.

0x00036801   Power Module Cooling Device 01 failure

Related messages:
*   0x00036002 : Power Module Cooling Device 02 failure
*   0x00036003 : Power Module Cooling Device 03 failure
*   0x00036004 : Power Module Cooling Device 04 failure
*   0x00036005 : Power Module Cooling Device 05 failure
*   0x00036006 : Power Module Cooling Device 06 failure

Explanation: The fan in the power module is not operating at all.

Severity: Error

Alert Category: Cooling Devices (Critical) - mmTrapFanC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Replace the power module.

0x000A2001   Chassis Cooling Device 1 communication failed.

Explanation: A communication error occurred between the advanced management module and the fan or blower module in fan bay 1.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Examine the event log. Communication problems on the I2C management bus can cause this error as well as a failed fan or blower module. Actions for bus issues include restarting the advanced management module, failing over to a standby advanced management module, and reseating the components on the bus, including the advanced management module and blower or fan modules.
2. Replace the fan or blower module.

0x000A2002   Chassis Cooling Device 2 communication failed.

Explanation: A communication error occurred between the advanced management module and the fan or blower module in fan bay 2.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Examine the event log. Communication problems on the I2C management bus can cause this error as well as a failed fan or blower module. Actions for bus issues include restarting the advanced management module, failing over to a standby advanced management module, and reseating the components on the bus, including the advanced management module and blower or fan modules.
2. Replace the fan or blower module.

0x000A2003   Chassis Cooling Device 3 communication failed.

Explanation: A communication error occurred between the advanced management module and the fan or blower module in fan bay 3.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

0x000A2004 • 0x000A6001

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1.   Examine the event log. Communication problems on the I2C management bus can cause this error as well as a failed fan or blower module. Actions for bus issues include restarting the advanced management module, failing over to a standby advanced management module, and reseating the components on the bus, including the advanced management module and blower or fan modules.

2.   Replace the fan or blower module.

0x000A2004   Chassis Cooling Device 4 communication failed.

Explanation: A communication error occurred between the advanced management module and the fan or blower module in fan bay 4.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1.   Examine the event log. Communication problems on the I2C management bus can cause this error as well as a failed fan or blower module. Actions for bus issues include restarting the advanced management module, failing over to a standby advanced management module, and reseating the components on the bus, including the advanced management module and blower or fan modules.

2.   Replace the fan or blower module.

0x000A6000   Constant fan speed override enabled

Explanation: The constant fan speed has been set through the management module user interface.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x000A6001   Chassis Cooling Device 01 outside of recommended speed

Related messages:

- 0x000A6002 : Chassis Cooling Device 02 outside of recommended speed
- 0x000A6003 : Chassis Cooling Device 03 outside of recommended speed
- 0x000A6004 : Chassis Cooling Device 04 outside of recommended speed
- 0x000A6005 : Chassis Cooling Device 05 outside of recommended speed
- 0x000A6006 : Chassis Cooling Device 06 outside of recommended speed
- 0x000A6007 : Chassis Cooling Device 07 outside of recommended speed

- 0x000A6008 : Chassis Cooling Device 08 outside of recommended speed
- 0x000A6009 : Chassis Cooling Device 09 outside of recommended speed
- 0x000A600A : Chassis Cooling Device 10 outside of recommended speed

Explanation: The fan or blower module is not operating at the expected speed.

Severity: Error

Alert Category: Cooling Devices (Critical) - mmTrapFanC

Log Source: Cool_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:
1. Flash (update if applicable) the advanced management module firmware and restart the advanced management module.
2. Reseat the fan or blower module.
3. Make sure nothing is blocking air flow of the fan or blower module.
4. Replace the fan or blower module.

0x000A7001 Power Module Cooling Device 01 not present.

Related messages:
- 0x000A7002 : Power Module Cooling Device 02 not present.
- 0x000A7003 : Power Module Cooling Device 03 not present.
- 0x000A7004 : Power Module Cooling Device 04 not present.
- 0x000A7005 : Power Module Cooling Device 05 not present.
- 0x000A7006 : Power Module Cooling Device 06 not present.

Explanation: A power module has been removed from the chassis or a power module without a fan pack has been installed in the chassis.

Severity: Error

Alert Category: Cooling Devices (Critical) - mmTrapFanC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Make sure that you install a fan pack on the power module (if applicable) and install the fan module in the chassis.

0x000A7801 Chassis Cooling Device 01 outside of recommended speed

Related messages:
- 0x000A7802 : Chassis Cooling Device 02 outside of recommended speed
- 0x000A7803 : Chassis Cooling Device 03 outside of recommended speed
- 0x000A7804 : Chassis Cooling Device 04 outside of recommended speed

Explanation: The fan module is not operating at the expected speed.

Severity: Error

0x000A8001 • 0x000A9001

Alert Category: Cooling Devices (Critical) - mmTrapFanC

Log Source: Cool_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:
1. Flash (update if applicable) the advanced management module firmware and restart the advanced management module.
2. Reseat the fan or blower module.
3. Make sure nothing is blocking air flow of the fan or blower module.
4. Replace the fan or blower module.

0x000A8001   Power Module Cooling Device 01 controller firmware was not updated.

Related messages:
- 0x000A8002 : Power Module Cooling Device 02 controller firmware was not updated.
- 0x000A8003 : Power Module Cooling Device 03 controller firmware was not updated.
- 0x000A8004 : Power Module Cooling Device 04 controller firmware was not updated.
- 0x000A8005 : Power Module Cooling Device 05 controller firmware was not updated.
- 0x000A8006 : Power Module Cooling Device 06 controller firmware was not updated.

Explanation: The controller firmware for the specified fan pack was not updated.

Severity: Informational

Alert Category: Cooling Devices (Informational) - mmTrapFanS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for problems related to cooling. If none are found, no action is required.

0x000A9001   Chassis Cooling Device 01 controller firmware was not updated.

Related messages:
- 0x000A9002 : Chassis Cooling Device 02 controller firmware was not updated.
- 0x000A9003 : Chassis Cooling Device 03 controller firmware was not updated.
- 0x000A9004 : Chassis Cooling Device 04 controller firmware was not updated.
- 0x000A9005 : Chassis Cooling Device 05 controller firmware was not updated.
- 0x000A9006 : Chassis Cooling Device 06 controller firmware was not updated.
- 0x000A9007 : Chassis Cooling Device 07 controller firmware was not updated.
- 0x000A9008 : Chassis Cooling Device 08 controller firmware was not updated.
- 0x000A9009 : Chassis Cooling Device 09 controller firmware was not updated.
- 0x000A900A : Chassis Cooling Device 10 controller firmware was not updated.
- 0x000A9101 : Chassis Cooling Device 01 controller firmware was not updated.
- 0x000A9102 : Chassis Cooling Device 02 controller firmware was not updated.
- 0x000A9103 : Chassis Cooling Device 03 controller firmware was not updated.
- 0x000A9104 : Chassis Cooling Device 04 controller firmware was not updated.

Explanation: The controller firmware for the specified blower was not updated by the advanced management module.

Severity: Informational

Alert Category: Cooling Devices (Informational) - mmTrapFanS

Log Source: Cool_##

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for problems related to cooling. If none are found, no action is required.

0x000AA020 The chassis has mismatched cooling devices.

Explanation: Only one enhanced blower is installed in the chassis. Enhanced blower modules must be installed in pairs.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Install the second enhanced blower module.

0x000B6001 Power Module Cooling Device 01 outside recommended speed

Related messages:
- 0x000B6002 : Power Module Cooling Device 02 outside recommended speed
- 0x000B6003 : Power Module Cooling Device 03 outside recommended speed
- 0x000B6004 : Power Module Cooling Device 04 outside recommended speed
- 0x000B6005 : Power Module Cooling Device 05 outside recommended speed
- 0x000B6006 : Power Module Cooling Device 06 outside recommended speed

Explanation: The fan in the power module is not operating at the recommended speed.

Severity: Warning

Alert Category: Cooling Devices (Warning) - mmTrapFanN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: If this is a BladeCenter H or BladeCenter HT chassis, replace the fan pack on the power module. Otherwise, replace the power module.

0x000FF1BA The SMTP server is not reachable

Explanation: The configured Simple Mail Transfer Protocol (SMTP) server address is not responding and appears to be unreachable.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

0x00101000 • 0x00101007

Recoverable: Yes

Example Message: The SMTP server is not reachable. SMTP server address: 9.37.177.12

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform this steps:

1. Make sure that the DNS server is enabled and configured correctly.
2. Make sure that the SMTP server is operational, and that you can communicate with the SMTP server through the advanced management module.
3. Check for network connectivity issues, such as user network cabling and network status.

0x00101000   One or more blades are isolated from the management bus.

Explanation: The advanced management module was not able to communicate with one or more blade servers, so it isolated those blade servers from the management bus.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. View the System Status Summary page through the advanced management module Web interface to determine which blade servers have been isolated.
2. Attempt to reset the service processor for each of the blade servers. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
3. Reseat each of the blade servers.

0x00101007   Unable to isolate bus fault. Bus was not recovered.

Explanation: A bus fault has occurred between the advanced management module and one or more blade servers. The advanced management module cannot isolate the fault. Therefore, the advanced management module cannot communicate with these blade servers.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:

1. Look in the event log for other communication problems with blade servers.
2. View the System Status Summary page through the advanced management module Web interface to determine which blade servers are affected.
3. Reset the service processor for each of the blade servers. You can reset the service processor through the advanced management module Web interface, from the Blade Power/Restart page.
4. Restart the advanced management module.
5. Check the IBM Support Web page for any service bulletins that might be related to this problem.
6. Reseat the blade server.

0x00104201   Default values restored and MM reset from long pinhole button press

Explanation: The default configuration has been restored for the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x00104202   Default values restored and MM reset by user

Explanation: The default configuration has been restored for the advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x00104203   MM reset was initiated by short pinhole button press

Explanation: The advanced management module was reset.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x00104204   Primary Management Module reset was initiated by user

Explanation: The primary advanced management module was reset.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x00104205   Standby Management Module reset was initiated by user

Explanation: The standby advanced management module was reset.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

0x00104206 • 0x0011C881

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00104206   AMM reset was initiated on the standby AMM by user

Explanation: The primary advanced management module was reset from the standby advanced management module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x0011C501   Management module is over recommended temperature.

Explanation: The advanced management module has exceeded the recommended temperature threshold.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:
1. Check the event log for other over temperature events and resolve them.
2. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
3. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
5. Make sure that there is nothing covering the media tray (that will disrupt the airflow to the ambient temperature sensor).
6. Update the firmware for the advanced management module. You can find firmware on the IBM BladeCenter software and device drivers Web page.
7. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x0011C881   Management module under temperature

Explanation: The temperature for the advanced management module has fallen below the temperature fault threshold.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: From the System Status Summary page of the advanced management module Web interface, click the status icon to display the temperature readings for each of the chassis components.
* If the values for all components are in low range of the operating temperature, raise the ambient temperature in the room.
* If all other temperature readings are in the normal operating range,
    1. Restart the advanced management module.
    2. Reseat the advanced management module.

0x0011C901   Management module under recommended temperature

Explanation: The temperature for the advanced management module has fallen below the recommended temperature threshold.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Major

User response: From the System Status Summary page of the advanced management module Web interface, click the status icon to display the temperature readings for each of the chassis components.
* If the values for all components are in low range of the operating temperature, raise the ambient temperature in the room.
* If all other temperature readings are in the normal operating range, perform these steps:
    1. Hot swap the media tray.
    2. Restart the advanced management module.

0x0011D801   Management module under recommended temperature

Explanation: The temperature for the advanced management module has fallen below the recommended temperature threshold.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Minor

User response: From the System Status Summary page of the advanced management module Web interface, click the status icon to display the temperature readings for each of the chassis components.
* If the values for all components are in low range of the operating temperature, raise the ambient temperature in the room.
* If all other temperature readings are in the normal operating range,
    1. Restart the advanced management module.
    2. Reseat the advanced management module.

0x00120000   System management bus re-initialized

Explanation: The advanced management module external management bus has been reset.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00200000   Remote login failed for user

Explanation: The specified user cannot log in.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Remote login failed for user 'USERID' from Web at IP 192.168.0.1

User response: Make sure that you have the correct user account and password, and then attempt to log in again.

0x00216000   Problem communicating with BSMP.

Explanation: The communication between the advanced management module and the service processor on the blade server has failed.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Reseat the blade server.
2. Update the service processor firmware for the blade server to latest level.

0x00216002   Blade System Management Processor reset, persistent events will be regenerated.

Explanation: The service processor on the specified blade server has been reset. Events related to the blade server before it was reset will be regenerated if these events are still applicable. However, events related to firmware may not be regenerated.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00216004   Blade System Management Processor reset NMI, persistent events will be regenerated.

Explanation: The specified blade server has been restarted with Non-Maskable Interrupt (NMI)successfully.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Verify that the blade server is powered on and that it restarted successfully. If not, check the event log for additional errors related to that blade server and resolve those errors.

0x00216005   BSMP reset NMI failed.

Explanation: An attempt was made to restart the specified blade server with Non-Maskable Interrupt (NMI). That attempt failed.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Perform these steps:
1. Reset the server processor for the blade server and attempt to restart the blade server with NMI again. To reset the server processor from the advanced management module Web interface, go to **Blade Tasks**, click **Power Restart** and then click **Restart Blade System Mgmt Processor**.
2. Reseat the blade server.

0x00216010   PCI PERR: parity error.

Explanation: The service processor on the specified blade server has reported a PCI parity error for the specified component. The blade server will reboot.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Continue to monitor the event log for more occurrences of this error. If the error persists, perform these steps:
1. Verify that the PCI adapter is supported in the blade server (go to the IBM ServerProven Web site).
2. Update the firmware for the PCI adapter.
3. Flash (update if applicable) the firmware for the service processor (BMC), BIOS, and firmware for the advanced management module.
4. Reseat the PCI adapter.
5. Replace the PCI adapter.

0x00216011   PCI system error.

Explanation: The service processor on the specified blade server has reported a PCI system error for the specified component. The blade server will reboot.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: Continue to monitor the event log for more occurrences of this error. If the error persists, perform these steps:

1. Verify that the PCI adapter is supported in the blade server (go to the IBM ServerProven Web site).
2. Update the firmware for the PCI adapter.
3. Flash (update if applicable) the firmwware for the service processor (BMC), BIOS, and firmware for the advanced management module.
4. Reseat the PCI adapter.
5. Replace the PCI adapter.

0x00216012   Uncorrectable bus error.

Explanation: The specified blade server has encountered an uncorrectable memory/system bus error.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: If the call home to IBM was successful, you can expect a service call for this event. In the meantime, perform these steps:

1. Flash (update if applicable) the firmware for the service processor (BMC), BIOS, and firmware for the advanced management module.
2. Reseat the memory DIMMs and any expansion card options.
3. Replace the system board (trained service technician only).

0x00216018   Blade reset.

Explanation: The main processor on the specified blade server has performed a power cycle.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0021601C   FW/BIOS backup ROM corruption. System board failure

Explanation: A blade server has encountered an error due to a problem with the backup ROM.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Major

User response: Update the firmware for the blade server.

0x0021603E   PCI bus timeout: system error.

Explanation: A Peripheral Component Interconnect (PCI) bus timeout has occurred for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Continue to monitor the event log for more occurrences of this error. If the error persists, perform these steps:
1. Verify that the PCI adapter is supported in the blade server (go to the IBM ServerProven Web site).
2. Update the firmware for the PCI adapter.
3. Flash (update if applicable) the firmware for the service processor (BMC), BIOS, and firmware for the advanced management module.
4. Reseat the PCI adapter.
5. Replace the PCI adapter.

0x00217000   Management module external network physical link lost.

Explanation: The advanced management module physical link to the external network has been lost.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Make sure the Ethernet cable is plugged in (check the connection on both ends of the cable), and that the cable is intact.
2. Make sure that both the devices on both ends of the cable are powered on and functioning.

0x00217001 • 0x00217004

0x00217001 Management module %s external network logical link lost.

Explanation: The advanced management module logical link to the external network has been lost.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Verify that your network is configured properly and is functioning.

0x00217002 Physical uplink failover delay setting

Explanation: The setting, "Failover delay for physical link loss" was changed by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Physical uplink failover delay settings were changed by USERID

User response: Information only; no action is required.

0x00217003 Logical uplink failover delay setting

Explanation: The setting "Failover delay for logical link loss" has been changed by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Logical uplink failover delay settings were changed by USERID

User response: Information only; no action is required.

0x00217004 Physical uplink failover setting

Explanation: The failover on the loss of a physical link has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Physical uplink failover enabled by USERID

User response: Information only; no action is required.

0x00217005   Logical uplink failover setting

Explanation: The failover on the loss of a logical link has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Logical uplink failover disabled by USERID.
- Logical uplink failover enabled by USERID.

User response: Information only; no action is required.

0x00222000   Standby MM failure on system management bus, check devices

Explanation: The advanced management module encountered a failure on system management bus. A failover was initiated and the advanced management module is now the standby advanced management module.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. At your earliest convenience, initiate a failover to make the advanced management module the primary advanced management module. This will reset the advanced management module.
2. Verify that the advanced management module can communicate with other components in the chassis.
   - If it cannot communicate with other any devices, perform these steps:
     a. Reset the advanced management module.
     b. Replace the advanced management module.
   - If it can communicate with other devices, go to the built-in self test (BIST) results from the AMM Status page of the advanced management module Web interface to determine which component may be causing a problem.

0x00282001   Management module 01 installed

Related messages:
- 0x00282002 : Management module 02 installed

Explanation: The specified advanced management module has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x00282005   Configuration of mismatched management modules is not supported

Explanation: Installing a management module and an advanced management module in the same chassis at the same time is not supported.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: If two advanced management modules are required, replace the management module with an advanced management module.

0x00284001   Management module 01 removed

Related messages:

• 0x00284002 : Management module 02 removed

Explanation: The specified advanced management module has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x04000000   FW/BIOS ROM corruption detected.

Explanation: The BIOS ROM for the specified blade server is corrupt.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Update the BIOS firmware for the blade server. Firmware is available at the IBM BladeCenter software and device drivers Web site.

0x04000080   Multi Processor Expansion board fault.

Explanation: A fault has occurred in the Multiprocessor Expansion Unit for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Flash (update if applicable) the firmware for the service processor (BMC), BIOS, and firmware for the advanced management module.
2. Reseat the Multiprocessor Expansion Unit.
3. Remove all components in the Multiprocessor Expansion Unit. Then add the components back in, one at a time. Restart the blade server each time to see if the issue has been corrected.
4. Replace the following components one at a time, in the order shown, restarting the blade server each time:

   a. Multiprocessor Expansion Unit

   b. Base system board assembly (trained service technician only)

Refer to the Problem Determination and Service Guide for the specified blade server type for information about the Multiprocessor Expansion Unit. The Problem Determination and Service Guide is available on the Web.

0x04000300   Power jumper not present

Explanation: The power jumper in the specified blade server is not present. The blade server must either have a power jumper or be attached to an I/O Expansion Blade to power up.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. If the blade server does not have an I/O Expansion Blade installed, make sure that the power jumper is correctly installed in power connector J164.
2. Reattach the I/O expansion blade.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about installing power jumpers. The Problem Determination and Service Guide is available on the Web.

0x04000381   Blade 01 incompatible with chassis

Related messages:
- 0x04000382 : Blade 02 incompatible with chassis
- 0x04000383 : Blade 03 incompatible with chassis
- 0x04000384 : Blade 04 incompatible with chassis
- 0x04000385 : Blade 05 incompatible with chassis
- 0x04000386 : Blade 06 incompatible with chassis
- 0x04000387 : Blade 07 incompatible with chassis
- 0x04000388 : Blade 08 incompatible with chassis
- 0x04000389 : Blade 09 incompatible with chassis
- 0x0400038A : Blade 10 incompatible with chassis
- 0x0400038B : Blade 11 incompatible with chassis
- 0x0400038C : Blade 12 incompatible with chassis
- 0x0400038D : Blade 13 incompatible with chassis
- 0x0400038E : Blade 14 incompatible with chassis

Explanation: The specified blade server is not compatible with chassis.

Severity: Warning

0x04018000 • 0x0401E000

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Use a compatible blade server in the chassis. See the IBM ServerProven Web site to determine which blade servers are compatible with the chassis.

0x04018000   Blade voltage fault.

Explanation: Blade CPU has encountered voltage fault.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the event log to see if this is happening on multiple blades, suspect the power module, not the blade server.
   a. Identify the power module that is causing the problem (the AC or DC LED is not lit).

      Note: If you cannot easily identify which power module is bad, you should schedule downtime before going further.
   b. Remove the power module in the power domain that powers the failing blade servers, one power module at a time.
   c. Wait 5 minutes.
   d. If the issue persists, swap the other power module in the power domain.
2. If this is happening for a single blade server:
   a. Reseat the blade server.
   b. Update the firmware for the blade server through the advanced management module Web interface (go to Blade Tasks).
   c. Replace the system board (trained service technician only).

0x0401E000   Invalid CPU configuration

Explanation: Invalid CPU configuration

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: See the Configuration and Options Guide - Servers and Intellistation for information about CPU configuration and to determine which CPUs are supported in the blade server. The Configuration and Options Guide is available on the Web.

0x04110000   Detected a duplicate IPv6 address

Explanation: The advanced management module received an ARP request or reply from the specified MAC address. The IPv6 address that was received in the request or reply is already being used by the advanced management module.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Detected a duplicate IPv6 address '2001:1::214:5eff:fe5a:82f5' configured at MAC@=00:15:58:7f:05:98

Alarm Panel LED (BC T and BC HT): Minor

User response: Make sure that the IPv6 address for all network devices is unique. Change the IPv6 address for the advanced management module or for the network device with the specified MAC address.

0x04110001   SNMPv3 trap receiver configured for user

Explanation: The advanced management module SNMPv3 trap receiver configuration was changed for the specified login profile by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SNMPv3 trap receiver configured for Login Profile 1 by 'USERID' from '2001:1::214:5eff:fe5a:82f5 (Web)'. IP address: 3ffe:302:11:2:214:5eff:fe5a:82f5.

User response: Information only; no action is required.

0x04200201   CPU 01 Fault

Related messages:
- 0x04200202 : CPU 02 Fault
- 0x04200203 : CPU 03 Fault
- 0x04200204 : CPU 04 Fault

Explanation: There is a fault on the specified processor on the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:
1. Restart the service processor for the specified blade server. You can restart the service processor from the advanced management module Web interface.
2. Reboot the blade server and press F1 to display the BIOS menu:
   a. Verify that both processors are being seen by BIOS.

   b. Load the default settings.

   c. Go to the advanced setup menu, select the CPU settings, and attempt to re-enable the CPU slot.

3. Swap processors on the blade server to determine if the problem is related to the CPU slot or the processor.

   Note: This step does not apply to JSxx blade servers.

4. Go to the IBM BladeCenter software and device drivers Web page for firmware updates.

5. Refer to the Problem Determination and Service Guide for the blade server type for information related to this event. You can find the Problem Determination and Service Guide on the Web.

6. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x04204001   CPU 01 disabled

Related messages:

- 0x04204002 : CPU 02 disabled
- 0x04204003 : CPU 03 disabled
- 0x04204004 : CPU 04 disabled
- 0x04204005 : CPU 05 disabled
- 0x04204006 : CPU 06 disabled
- 0x04204007 : CPU 07 disabled
- 0x04204008 : CPU 08 disabled

Explanation: The specified CPU on the specified blade server has been disabled.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:

1. Restart the service processor for the specified blade server. You can restart the service processor from the advanced management module Web interface.

2. Reboot the blade server and press F1 to display the BIOS menu:

   a. Verify that both processors are being seen by BIOS.

   b. Load the default settings.

   c. Go to the advanced setup menu, select the CPU settings, and attempt to re-enable the CPU slot.

3. Swap processors on the blade server to determine if the problem is related to the CPU slot or the processor.

4. If this error is occurring for both processors, go to the IBM BladeCenter software and device drivers Web page for firmware updates.

0x04210001   Service processor exited update mode.

Explanation: The service processor on the blade server exited update mode.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Example Message: Service processor exited update mode.

User response: Information only; no action is required.

0x0421C081   CPU 01 over temperature

Related messages:
- 0x0421C082 : CPU 02 over temperature
- 0x0421D081 : CPU 01 over temperature
- 0x0421D082 : CPU 02 over temperature
- 0x0421D083 : CPU 03 over temperature
- 0x0421D084 : CPU 04 over temperature

Explanation: The service processor has detected that the CPU has exceed a critical thermal threshold(overheating due to an overload).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
4. Make sure that there is nothing covering the media tray (that will disrupt the airflow to the ambient temperature sensor).
5. Update the firmware for the advanced management module. You can find firmware on the IBM BladeCenter software and device drivers Web page.
6. Update the firmware for the blade server.
7. For all blade servers other than the JSxx blade servers, make sure the heat sink and CPU are secured on the system board.

    Note: Be careful when handling the heat sink and CPU, they may be extremely hot.
8. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x0421C481   CPU 01 temperature fault.

Related messages:
- 0x0421C482 : CPU 02 temperature fault.
- 0x0421C483 : CPU 03 temperature fault.
- 0x0421C484 : CPU 04 temperature fault.

Explanation: The temperature for the specified CPU is the specified blade server is over the fault threshold.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Replace the blade server.

0x0421D401   CPU 01 temperature warning

Related messages:

- 0x0421D402 : CPU 02 temperature warning

Explanation: The temperature for the specified CPU in the specified blade server is over recommended threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
4. Make sure that there is nothing covering the media tray (that will disrupt the airflow to the ambient temperature sensor).

0x0421D501   CPU 01 over recommended temperature

Related messages:

- 0x0421D502 : CPU 02 over recommended temperature
- 0x0421D503 : CPU 03 over recommended temperature
- 0x0421D504 : CPU 04 over recommended temperature

Explanation: The temperature for the specified CPU in the specified blade server is over recommended value.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.

3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

4. Make sure that there is nothing covering the media tray (that will disrupt the airflow to the ambient temperature sensor).

0x04300201   CPU 01 internal fault

Related messages:
- 0x04300202 : CPU 02 internal fault
- 0x04300203 : CPU 03 internal fault
- 0x04300204 : CPU 04 internal fault

Explanation: The specified CPU on the blade server has encountered an internal error.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:
1. Check the change history for the blade server firmware to see if there have been any fixes for this issue. If so, update the firmware for the blade server.
2. Check the IBM Support Web page for any service bulletins that might be related to this problem.
3. Initiate a call home action to potentially replace the service processor.

0x04306201   CPU 01 halted

Related messages:
- 0x04306202 : CPU 02 halted
- 0x04306203 : CPU 03 halted
- 0x04306204 : CPU 04 halted
- 0x04306205 : CPU 05 halted
- 0x04306206 : CPU 06 halted
- 0x04306207 : CPU 07 halted
- 0x04306208 : CPU 08 halted

Explanation: Specified CPU in blade has halted due to undefined hardware fault.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:
1. Restart the blade server.
2. Restore the default CPU configuration.

0x04401501   Voltage regulator 01 over recommended voltage.

Related messages:

- 0x04401502 : Voltage regulator 02 over recommended voltage.

Explanation: Voltage of specified voltage regulator rises up over recommended threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:
1. Check the event log for other errors related to this blade server or system power and resolve them.
2. If the blade server was turned off, attempt to restart the blade server.

0x04401801   Voltage regulator 01 under recommended voltage.

Related messages:

- 0x04401802 : Voltage regulator 02 under recommended voltage.

Explanation: Voltage of specified voltage regulator drops down under recommended threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:
1. Check the event log for other errors related to this blade server or system power and resolve them.
2. If the blade server was turned off, attempt to restart the blade server.

0x04428000   Voltage regulator fault.

Explanation: The CPU voltage regulator on the specified blade server encountered a fault.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: If the call home to IBM was successful, you can expect a service call from IBM. In the meantime, perform these steps:
1. If voltage problem are occurring on multiple blade servers, look for other events in the event log related to power and resolve those events.

Note: If voltage problems are occurring on multiple blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Therefore, replace the power modules, one at a time, to see if the problem is resolved.

2. Check the change history for blade server service processor firmware and BIOS for any issues related to this problem. If so, update the blade server firmware and BIOS.

3. (Trained service personnel only)Replace the system board.

0x04428001   Voltage regulator 01 fault

Related messages:
- 0x04428002 : Voltage regulator 02 fault
- 0x04428003 : Voltage regulator 03 fault
- 0x04428004 : Voltage regulator 04 fault

Explanation: The specified CPU voltage regulator on the specified blade server encountered a fault.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: If the call home to IBM was successful, you can expect a service call from IBM. In the meantime, perform these steps:

1. If voltage problem are occurring on multiple blade servers, look for other events in the event log related to power and resolve those events.

   Note: If voltage problems are occurring on multiple blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Therefore, replace the power modules, one at a time, to see if the problem is resolved.

2. Check the change history for blade server service processor firmware and BIOS for any issues related to this problem. If so, update the blade server firmware and BIOS.

3. (Trained service personnel only) Replace the system board.

0x05200000   Blade memory fault

Explanation: Blade memory has encountered faults.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: No

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:

1. Check in the event log for other more specific messages related to this event.

2. Check the IBM Support Web page for related service bulletins.

3. Check the blade server BIOS change history on the Web for any memory related fixes. Update the BIOS if applicable.

4. Use Light Path diagnostics to verify the affected DIMM bank.

    a. Record the DIMM part number and size for future reference.

        Note: For some blade servers, the DIMM part number is available through the advanced management module Web interface.

    b. Verify that the memory DIMM is supported on the IBM ServerProven Web site.

5. Check to make sure the DIMMs are seated properly (especially if this is a new installation). If the DIMMs required reseating, boot the blade into BIOS setup and enable the memory bank.

6. Replace the DIMMs in the memory bank, boot the blade server to BIOS setup and enable the memory bank.

0x06000000   The real time clock battery in the blade needs service.

Explanation: The real-time clock battery for the specified component on the specified blade server has failed.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Reseat the battery.
2. Replace the battery.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about reseating and replacing the battery.

0x06000201   Management Module in bay 01 is primary.

Related messages:

• 0x06000202 : Management Module in bay 02 is primary.

Explanation: The advanced management module in the specified bay is the primary advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x06000301   Management Module in bay 01 is standby.

Related messages:

• 0x06000302 : Management Module in bay 02 is standby.

Explanation: The advanced management module in the specified bay is now the standby advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x06002001   Request to release MT failed - MT seized by Management Module -- for

Explanation: A request to release the media tray failed. The advanced management module will attempt to reassign ownership to the new blade server.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Request to release MT failed - MT seized by Management Module -- for Blade in bay (1).

Alarm Panel LED (BC T and BC HT): Minor

User response: If the I/O devices on the media tray, such as DVD or USB ports are working or not being used, no action is required. Otherwise, perform these steps:

1. Determine which blade server previously owned the media tray. You can determine ownership from the Blades LED page in the advanced management module Web interface.
2. Reset the system management processor for the blade server that previously owned the media tray from the advanced management module Web interface (from the Blade Power/Restart page.

See the Advanced Management Module User's Guide for more information about the Blades LED page and the Blade Power/Restart page. The guide is available from the Web.

0x06002002   Request to release KVM failed - KVM seized by Management Module -- for

Explanation: A request to release the Keyboard, Video, Mouse (KVM) failed. The advanced management module will attempt to reassign ownership to the new blade server.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Request to release KVM failed - KVM seized by Management Module -- for Blade in bay (1).

Alarm Panel LED (BC T and BC HT): Minor

User response: If the keyboard and video are working or not being used, no action is required. Otherwise, perform these steps:

1. Determine which blade server previously owned the KVM. You can determine ownership from the Blades LED page in the advanced management module Web interface.
2. Reset the system management processor for the blade server that previously owned the KVM from the advanced management module Web interface (from the Blade Power/Restart page.

See the Advanced Management Module User's Guide for more information about the Blades LED page and the Blade Power/Restart page. The guide is available from the Web.

0x06002003   Request to acquire MT denied by Management Module for

Explanation: A request to acquire the media tray failed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

0x06002004 • 0x06016000

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Request to acquire MT denied by Management Module for Blade in bay (1).

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Attempt to assign the media tray to another blade server, and then attempt to assign the media tray to the desired blade server.

0x06002004 Request to acquire KVM denied by Management Module for

Explanation: A request to acquire the keyboard, video, mouse (KVM) failed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Request to acquire KVM denied by Management Module for Blade in bay (1).

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Attempt to assign the KVM to another blade server, and then attempt to assign the KVM to the desired blade server.

0x06016000 I/O board fault

Explanation: A fault has occurred in the I/O expansion blade.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Flash (update if applicable) the firmware for the service processor (BMC), BIOS, and firmware for the advanced management module.
2. Reseat the I/O Expansion Unit.
3. Remove all components in the I/O Expansion Unit. Then, add the components back in, one at a time. Restart the blade server each time to see if the issue has been corrected.
4. Replace the following components one at a time, in the order shown, restarting the blade server each time:
   a. I/O Expansion Unit
   b. Base system board assembly (trained service technician only)

Refer to the Problem Determination and Service Guide for the specified blade server type for information about removing and installing components. The Problem Determination and Service Guide is available on the Web.

0x06018000   I/O board voltage fault.

Explanation: A fault has occurred in the I/O expansion blade.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:

1. If voltage problem are occurring on multiple blade servers, look for other events in the event log related to power and resolve those events.

   Note: If voltage problems are occurring on multiple blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Therefore, replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the I/O-expansion blade.
3. Replace the following components one at a time, in the order shown, restarting the blade server each time:
   a. I/O-expansion blade
   b. System board assembly (trained service technician only)

Refer to the Problem Determination and Service Guide for the specified blade server type for information about removing and installing components. The Problem Determination and Service Guide is available on the Web.

0x0601A000   I/O board power fault.

Explanation: A fault has occurred in the I/O expansion blade.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:

1. If voltage problem are occurring on multiple blade servers, look for other events in the event log related to power and resolve those events.

   Note: If voltage problems are occurring on multiple blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Therefore, Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the I/O-expansion blade.
3. Replace the following components one at a time, in the order shown, restarting the blade server each time:
   a. I/O-expansion blade
   b. System board assembly (trained service technician only)

Refer to the Problem Determination and Service Guide for the specified blade server type for information about removing and installing components. The Problem Determination and Service Guide is available on the Web.

0x06026080   Critical Chassis Cooling Device failure. Blade powered off

Explanation: A blade server has been powered off due to a critical chassis cooling device failure. Typically, this is a result of multiple fan or blower module failures.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Check power to the fan or blower modules.
2. Check the event log to see which fan or blower modules are failing and reseat them.
3. Replace the failing fan or blower modules.

0x06035500   Blade 5V over recommended voltage

Explanation: The service processor on the specified blade server has detected that voltage of chassis power module has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:
1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

    Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0603550A   Chassis 5V over recommended voltage

Explanation: The voltage of a power module in the chassis, which has a nominal output of +5V, exceeds the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x06035800   Blade 5V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the server power module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about under voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x06035801   Chassis 5V under recommended voltage

Explanation: The voltage of the power module, which has a nominal output of +5V, has fallen below the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x06037500   Blade 12V over recommended voltage.

Explanation: The service processor on the specified blade server has detected that the blade server power module has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x06037503   Chassis 12V over recommended voltage.

Explanation: The voltage of a power module in the chassis, which has a nominal output of +12V exceeds the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x06037800   Blade 12V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the chassis power module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x06037801   Chassis 12V under recommended voltage

Explanation: The voltage of the power module, which has a nominal output of +12V has fallen below the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x0621C481   BEM temperature fault.

Explanation: The service processor on the specified blade server has detected that the Blade Expansion Module has reached or exceeded the fault threshold.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

0x0621D481   BEM over recommended temperature.

Explanation: The service processor on the specified blade server has detected that the Blade Expansion Module has reached or exceeded the recommended temperature threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

0x06500000   PCI Parity Error

Explanation: The service processor on the specified blade server has detected a PCI parity error for the specified component. The blade server will reboot.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: No

Alarm Panel LED (BC T and BC HT): Major

0x06800000 • 0x06802000

User response: Continue to monitor the event log for more occurrences of this error. If the error persists, perform these steps:

1. If this is a new blade server or a new PCI adapter was added to an existing blade server, reseat the PCI adapter.
   a. Verify that this PCI adapter is supported in the blade server. See the IBM ServerProven Web site to determine if the PCI adapter is supported.
   b. Update the service processor firmware and BIOS for the blade server.
   c. Update the firmware for the PCI adapter.
2. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x06800000   BEM failure

Explanation: A blade storage expansion unit has failed. This will typically result in a hard drive failure on the expansion board.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response:

1. Check the event log for voltage events. If the voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x06802000   Hard drive 00 fault

Related messages:
- 0x06800001 : Hard drive 01 fault
- 0x06800002 : Hard drive 02 fault
- 0x06800003 : Hard drive 03 fault
- 0x06800004 : Hard drive 04 fault
- 0x06800005 : Hard drive 05 fault

Explanation: A fault has occurred for the specified hard disk drive number for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Replace hard disk drive.
2. Check the IBM Support Web page for related service bulletins.
3. Update the hard drive firmware, RAID controller firmware, drivers, etc., if applicable.

0x0681C482   System shutoff due to DASD Option temperature.

Explanation: The service processor on the specified blade server has shut down because the Direct Access Storage Device (DASD) has reached or exceeded the over-temperature threshold.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

0x0681E000   Hard drive 00 removal detected.

Related messages:
- 0x0681E001 : Hard drive 01 removal detected.
- 0x0681E002 : Hard drive 02 removal detected.
- 0x0681E003 : Hard drive 03 removal detected.
- 0x0681E004 : Hard drive 04 removal detected.
- 0x0681E005 : Hard drive 05 removal detected.

Explanation: The specified hot-swap hard disk drive for the specified blade server has been removed or replaced.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x06A02001   Media Tray 1 installed.

Explanation: Media tray 1 has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x06A02002 Media Tray 2 installed.

Explanation: Media tray 2 has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x06A03001 Media Tray 01 controller firmware was not updated.

Related messages:

• 0x06A03002 : Media Tray 02 controller firmware was not updated.

Explanation: The firmware for the specified media tray was not updated. Existing firmware will continue to be used.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Perform these steps:
1. Reseat the media tray.
2. Check the event log for other errors related to the management module and resolve them.
3. Attempt to update the management module firmware again.

0x06A16001 Media Tray 01 re-enabled by user

Related messages:

• 0x06A16002 : Media Tray 02 re-enabled by user

Explanation: The specified user has re-enabled the specified media tray.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x06A17001 Media Tray 01 prepared for safe removal by user

Related messages:

• 0x06A17002 : Media Tray 02 prepared for safe removal by user

Explanation: The specified user has prepared the specified media tray for safe removal.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x06A1E001 Media Tray 1 removed.

Explanation: Media tray 1 has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x06A1E002 Media Tray 2 removed.

Explanation: Media tray 2 has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x06A2E001 Chassis temperature device is unavailable. Cooling capacity set to maximum.

Related messages:

- 0x06A2E002 : Chassis temperature device is unavailable. Cooling capacity set to maximum.

Explanation: The chassis temperature is unavailable or unreadable from any media tray. The cooling capacity for the chassis has been set to the maximum, and the fan modules are running at full speed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Check the event log for communication failures for multiple components, such as I/O modules, fan modules, and power modules. If there are communication failures for multiple components, restart the advanced management module.

If there are no other communication failures, perform these steps:

1. Reseat the media tray.
2. Replace the media tray.

0x08001400   Blade 1.25V over recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08001401   Blade 1.2V over recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08001800   Blade 1.25V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08001801 Blade 1.2V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about under voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08006001 Mismatched power modules in power domain 01

Related messages:

- 0x08006002 : Mismatched power modules in power domain 02

Explanation: Power modules with different power capacities have been installed in the same chassis. The power modules remain functional, but the capacity used for every power module will be the capacity of the lower-capacity power module.

Severity: Warning

Alert Category: Power Modules (Warning) - mmTrapPowerN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Make sure that the power modules of the same capacity are installed in the chassis.

0x0800A401   Acoustic mode policy

Explanation: The acoustic mode policy has been enabled or disabled.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message:
- Acoustic mode policy was successfully changed to 'enabled' by 'USERID' from '192.168.0.1 (Web)'.
- Acoustic mode policy was successfully changed to 'disabled' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0800A402   NEBS mode policy

Explanation: The NEBS cooling policy has been changed.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- NEBS mode policy was successfully changed to 'enabled' by 'USERID' from '192.168.0.1 (Web)'.
- NEBS mode policy was successfully changed to 'disabled' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0800B401   Power policy

Explanation: The power management policy for the specified domain has been changed.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Power policy was successfully changed to 'Basic Power Management' by 'USERID' from '192.168.0.1 (Web)' for domain 1.

User response: Information only; no action is required.

0x0800C401   Data Sampling interval

Explanation: The power trend sampling interval has been changed.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Data Sampling interval was successfully changed to 20 minutes by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x0800D401   Power capping level

Explanation: The power capping level has been changed for a blade server.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Power capping level was successfully changed to '1' by 'USERID' from '192.168.0.1 (Web)' for blade 1.

User response: Information only; no action is required.

0x0800E401   Aggregate power capping level

Explanation: The aggregate power capping level has been changed for a blade server

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Aggregate power capping level was successfully changed to '1' by 'USERID' from '192.168.0.1 (Web)' for blade 1.

User response: Information only; no action is required.

0x0800F401   Power control

Explanation: The power capping control of a blade server has been enabled or disabled.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message:
- Power control successfully changed to 'Measurement' enabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Power Capping' enabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Static Low Power Saver' enabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Dynamic Power Saver' enabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Favor Performance over Power' enabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Measurement' disabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Power Capping' disabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.

0x08016080 • 0x08028001

- Power control successfully changed to 'Static Low Power Saver' disabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Dynamic Power Saver' disabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.
- Power control successfully changed to 'Favor Performance over Power' disabled for blade 1 by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x08016080   Power controller timeout

Explanation: A power controller timeout has occurred for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the blade server.
2. Update the service processor firmware and BIOS for the blade server.
3. Replace system board assembly (trained service technician only).

0x08028001   Power module 01 is off. DC fault.

Related messages:
- 0x08028002 : Power module 02 is off. DC fault.
- 0x08028003 : Power module 03 is off. DC fault.
- 0x08028004 : Power module 04 is off. DC fault.

Explanation: A DC fault has occurred in the specified power module, and the power module is shut down.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Verify that the AC LED is lit on the power module.
2. Look for other power module events (such as over current or over temperature events) in the event log and resolve them.
   a. Reseat the power module.
   b. Replace the power module.

0x08028081   **Power Module 01 failed to power on because of input AC mismatch.**

Related messages:

- 0x08028082 : Power Module 02 failed to power on because of input AC mismatch.
- 0x08028083 : Power Module 03 failed to power on because of input AC mismatch.
- 0x08028084 : Power Module 04 failed to power on because of input AC mismatch.

Explanation: There are two different types of input power sources (such as 110V and 220V) being used in the same chassis. All power modules must be powered by the same input voltage.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Make sure that all power modules are plugged into the same type of input power voltage. All power modules must be using either 110V or 220V.

0x08028481   **Power module 01 is off. AC fault**

Related messages:

- 0x08028482 : Power module 02 is off. AC fault
- 0x08028483 : Power module 03 is off. AC fault
- 0x08028484 : Power module 04 is off. AC fault

Explanation: The specified power module does not have AC input power.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Restore AC input to the power module:

1. Make sure that the power cord is attached to the power module.
2. Make sure that power is available.

0x08031480   **Blade 2.5V over recommended voltage**

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

0x08031481 • 0x08031881

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08031481   Chassis 2.5V over recommended voltage

Explanation: The voltage of a power module in the chassis, which has a nominal output of +2.5V, exceeds the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x08031880   Blade 2.5V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08031881   Chassis 2.5V under recommended voltage

Explanation: The voltage of the power module, which has a nominal output of +2.5V, has fallen below the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x08033480   Blade 3.3V over recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

    Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08033481   Chassis 3.3V over recommended voltage

Explanation: The voltage of a power module in the chassis, which has a nominal output of +3.3V, exceeds the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x08033880   Blade 3.3V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08033881   Chassis 3.3V under recommended voltage

Explanation: The voltage of the power module, which has a nominal output of +3.3V, has fallen below the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x08035500   Blade 5V over recommended voltage.

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08035800   Blade 5V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about under voltage conditions.
2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08039480   Blade 1.6V over recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08039880   Blade 1.6V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

0x0803D500 • 0x0803D800

Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0803D500   Blade -5V over recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0803D501   Chassis -5V over recommended voltage

Explanation: The voltage of a power module in the chassis, which has a nominal output of -5V, exceeds the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x0803D800   Blade -5V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about under voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0803D801   Chassis -5V under recommended voltage

Explanation: The voltage of the power module, which has a nominal output of -5V, has fallen below the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x08041400   Blade 1.5V over recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x08041800   Blade 1.5V under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

0x0807B400 • 0x0807B401

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about under voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0807B400   Blade 1.8V over recommended voltage.

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0807B401   Chassis 1.8V over recommended voltage.

Explanation: The voltage of a power module in the chassis, which has a nominal output of +1.8V, exceeds the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x0807B800   Blade 1.8V under recommended voltage.

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about under voltage conditions.
2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0807B801   Chassis 1.8V under recommended voltage.

Explanation: The voltage of the power module, which has a nominal output of +1.8V, has fallen below the recommended voltage threshold.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

User response: Check the event log for other events that are occurring at the same time as this event and resolve them. If there are no other events, no action is required.

0x08080001   Insufficient chassis power to support redundancy

Explanation: Based on the number of power modules within a power domain, redundancy cannot be supported. This can occur because there are not enough power modules installed, or because a power module has failed.

Severity: Informational

Alert Category: Power Modules (Informational) - mmTrapPowerS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:
1. If redundancy is required, install additional power modules.
2. If the power module has failed, other events will also be generated. In this case:
   a. Reseat the power module.
   b. Replace the power module.

0x08100080   Incompatible power controller firmware

Explanation: Incompatible power controller firmware has been detected in the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Replace system board assembly (trained service technician only).

0x08200001   Power module 01 communication failure

Related messages:
- 0x08200002 : Power module 02 communication failure
- 0x08200003 : Power module 03 communication failure
- 0x08200004 : Power module 04 communication failure

Explanation: The advanced management module cannot communicate with the specified power module.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Check the event log for other power related events and resolve them (for example, a blade server has throttled or fan modules are running at full speed).
2. Verify that the DC LED is lit on the power module.

   If the DC LED is lit:

   a. Reseat the power module.

      Note: Before reseating or replacing a power module, make sure that you have sufficient power modules in the chassis to power the remaining components in the chassis. Otherwise, components might be powered off, which might disrupt BladeCenter system operations.

   b. Check the event log for any other communications events and resolve them.

   c. Replace the power module.

   If the DC LED is not lit, make sure that there is power coming to the power module.

0x08216001   Power module 01 installed.

Related messages:
- 0x08216002 : Power module 02 installed.
- 0x08216003 : Power module 03 installed.
- 0x08216004 : Power module 04 installed.

Explanation: The specified power module has been installed in the chassis.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: Power_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0821A001   Power module 01 current share mismatch

Related messages:
- 0x0821A002 : Power module 02 current share mismatch
- 0x0821A003 : Power module 03 current share mismatch
- 0x0821A004 : Power module 04 current share mismatch

Explanation: The power load within the chassis is not being shared evenly; the specified power module is supplying most of the power.

Severity: Informational

Alert Category: Power Modules (Informational) - mmTrapPowerS

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x0821C001   Power module 01 has exceeded the warning temperature.

Related messages:
- 0x0821C002 : Power module 02 has exceeded the warning temperature.
- 0x0821C003 : Power module 03 has exceeded the warning temperature.
- 0x0821C004 : Power module 04 has exceeded the warning temperature.

Explanation: The temperature for the specified power module has exceeded the warning threshold. If fan modules or blower modules are not operating at maximum speed, the BladeCenter chassis will increase the fan or blower speed to maximum speed in response to this warning.

Severity: Warning

Alert Category: Power Modules (Warning) - mmTrapPowerN

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Make sure the fan modules are working properly.
2. Make sure the ambient temperature is within the operating requirements for the chassis.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the power module.

0x0821C080   Blade powered off because power modules exceeded temperature threshold

Explanation: All blade servers have been powered off because all power modules within a power domain exceed the temperature threshold.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Check the event log to determine which power modules have exceeded the temperature threshold.

0x0821C081   Power module 01 temperature fault

Related messages:
- 0x0821C082 : Power module 02 temperature fault
- 0x0821C083 : Power module 03 temperature fault
- 0x0821C084 : Power module 04 temperature fault

Explanation: A temperature fault has occurred in the specified power module. A power module can turn itself off within 30 to 60 seconds after a temperature fault has been indicated.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the room ambient temperature to ensure that the room itself is not too hot. You can also check the temperature on the media tray by viewing the System Status page through the management module Web interface.
2. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
4. Check the LEDs on the fans to ensure that all fans are functioning normally. If the fans are not functioning normally, the event log may be displaying over temperature messages for multiple components in the chassis.
5. The advanced management module will attempt to restart the power module if the power module has cooled sufficiently. After waiting a sufficient amount of time to allow the power module to cool, check the DC LED on the power module.
   - If the DC LED is not lit, reseat the power module to force a power on cycle. If the DC LED is still not lit, replace the power module.
   - If the DC LED is lit, check the IBM BladeCenter software and device drivers Web site to see if are any updates to the management module firmware. If so, update the firmware for the management module.

0x0821E001   Power module 01 removed

Related messages:
- 0x0821E002 : Power module 02 removed
- 0x0821E003 : Power module 03 removed
- 0x0821E004 : Power module 04 removed

Explanation: The specified power module was removed from the chassis.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Install a power module in the power module bay.

0x08236001   Power module 01 over current fault

Related messages:
- 0x08236002 : Power module 02 over current fault
- 0x08236003 : Power module 03 over current fault
- 0x08236004 : Power module 04 over current fault

Explanation: The power current for the specified power module has exceeded the current fault threshold.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Reseat the power module.
2. Check the event log for other system devices that might be having a similar problem, which might indicate that the problem was caused by an external short. If no external short is found, replace the power module.
3. If the problem persists, verify that you have a stable power input source.

0x08236481   Power module 01 over voltage fault

Related messages:
- 0x08236482 : Power module 02 over voltage fault
- 0x08236483 : Power module 03 over voltage fault
- 0x08236484 : Power module 04 over voltage fault

Explanation: The voltage output for the specified power module exceeds +12V.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

0x08236801 • 0x08238001

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the power module.
2. If this error persists or continues to occur, replace the power module.

0x08236801   Power module 01 under voltage fault

Related messages:
*   0x08236802 : Power module 02 under voltage fault
*   0x08236803 : Power module 03 under voltage fault
*   0x08236804 : Power module 04 under voltage fault

Explanation: The voltage output for the specified power module has dropped below +12V, and the power module has been shut down.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the power module.
2. If this error persists or continues to occur, replace the power module.

0x08238001   Power module 01 48V over current fault

Related messages:
*   0x08238002 : Power module 02 48V over current fault
*   0x08238003 : Power module 03 48V over current fault
*   0x08238004 : Power module 04 48V over current fault

Explanation: The current in the specified power module exceeded the current fault threshold.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the power module.
2. Check the event log for other system devices that might be having a similar problem, which might indicate that the problem was caused by an external short. If no external short is found, replace the power module.

3. If the problem persists, verify that you have a stable power input source.

Note: (DC Current) Only trained service personnel, other than IBM service technicians, are authorized to make the connections to and disconnections from the -48 volt DC power source. IBM service technicians are not certified or authorized to install or remove the -48 volt power cable. The customer is responsible for ensuring that only trained service personnel install or remove the -48 volt power cable.

0x08238481   **Power module 01 48V over voltage fault**

Related messages:
- 0x08238482 : Power module 02 48V over voltage fault
- 0x08238483 : Power module 03 48V over voltage fault
- 0x08238484 : Power module 04 48V over voltage fault

Explanation: The voltage in the specified power module exceeded the fault threshold. The nominal voltage output is +48V.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the power module.
2. If this error persists or continues to occur, replace the power module.

0x08238801   **Power module 01 48V under voltage fault**

Related messages:
- 0x08238802 : Power module 02 48V under voltage fault
- 0x08238803 : Power module 03 48V under voltage fault
- 0x08238804 : Power module 04 48V under voltage fault

Explanation: The voltage in the specified power module has dropped below the fault threshold. The nominal voltage output is +48V.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the power module.
2. If this error persists or continues to occur, replace the power module.

0x08240001   Power module 01 PSOC Controller communication failed

Related messages:

- 0x08240002 : Power module 02 PSOC Controller communication failed
- 0x08240003 : Power module 03 PSOC Controller communication failed
- 0x08240004 : Power module 04 PSOC Controller communication failed

Explanation: The advanced management module cannot communicate with the fan pack on the specified power module.

Severity: Error

Alert Category: Power Modules (Critical) - mmTrapPsC

Log Source: Power_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Check the event log for other temperature related events and resolve them.
2. Reseat the fan pack and power module.

   Note: Before reseating or replacing a power module, make sure that you have sufficient power modules in the chassis to power the remaining components in the chassis. Otherwise, components might be powered off, which might disrupt BladeCenter system operations.

0x09025000   Front panel cable is not connected to system board

Explanation: The connection between the front bezel on the blade and the system board has become loose or damaged. The buttons on the front bezel will not be useable and the LEDs will not light.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Reseat the control panel cable.
2. Replace the following components one at a time, in the order shown, restart the blade server each time:
   a. Bezel assembly
   b. System board assembly (trained service technician only)

Refer to the Problem Determination and Service Guide for the specified blade server type for information about replacing components. The Problem Determination and Service Guide is available on the Web.

0x0A000000   Concurrent KVM card fault detected.

Explanation: A fault has occurred for the concurrent KVM keyboard/video/mouse (cKVM) feature card in the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Check the change history on the Web for firmware updates that may be related to this problem, including cKVM, BIOS, and advanced management module firmware. Update the firmware if applicable.
2. Reseat the cKVM feature card.
3. Replace the Concurrent KVM feature card.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about removing and installing a cKVM feature card. The Problem Determination and Service Guide is available on the Web.

0x0A000280   Uncorrectable memory error

Explanation: An uncorrectable memory error has occurred for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:

1. Check the IBM Support Web page for related service bulletins.
2. Check the blade server BIOS change history on the Web for any memory related fixes. Update the BIOS if applicable.
3. Use Light Path diagnostics to verify the affected DIMM bank.

   a. Record the DIMM part number and size for future reference.

   Note: For some blade servers, the DIMM part number is available through the advanced management module Web interface.

   b. Verify that the memory DIMM is supported on the IBM ServerProven Web site.
4. Check to make sure the DIMMs are seated properly (especially if this is a new installation). If the DIMMs required reseating, boot the blade into BIOS setup and enable the memory bank.
5. Replace the DIMMs in the memory bank, boot the blade server to BIOS setup and enable the memory bank.

0x0A000281   Uncorrectable memory error detected on DIMM 01

Related messages:

- 0x0A000282 : Uncorrectable memory error detected on DIMM 02
- 0x0A000283 : Uncorrectable memory error detected on DIMM 03
- 0x0A000284 : Uncorrectable memory error detected on DIMM 04
- 0x0A000285 : Uncorrectable memory error detected on DIMM 05
- 0x0A000286 : Uncorrectable memory error detected on DIMM 06
- 0x0A000287 : Uncorrectable memory error detected on DIMM 07
- 0x0A000288 : Uncorrectable memory error detected on DIMM 08
- 0x0A000289 : Uncorrectable memory error detected on DIMM 09
- 0x0A00028A : Uncorrectable memory error detected on DIMM 10
- 0x0A00028B : Uncorrectable memory error detected on DIMM 11

0x0A000400 • 0x0A000401

- 0x0A00028C : Uncorrectable memory error detected on DIMM 12
- 0x0A00028D : Uncorrectable memory error detected on DIMM 13
- 0x0A00028E : Uncorrectable memory error detected on DIMM 14
- 0x0A00028F : Uncorrectable memory error detected on DIMM 15
- 0x0A000290 : Uncorrectable memory error detected on DIMM 16

Explanation: An uncorrectable memory error has occurred on the specified DIMM for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the IBM Support Web page for related service bulletins.
2. Check the blade server BIOS change history on the Web for any memory related fixes. Update the BIOS if applicable.
3. Use Light Path diagnostics to verify the affected DIMM bank.
   a. Record the DIMM part number and size for future reference.

      Note: For some blade servers, the DIMM part number is available through the advanced management module Web interface.
   b. Verify that the memory DIMM is supported on the IBM ServerProven Web site.
4. Check to make sure the DIMMs are seated properly (especially if this is a new installation). If the DIMMs required reseating, boot the blade into BIOS setup and enable the memory bank.
5. Replace the DIMMs in the memory bank, boot the blade server to BIOS setup and enable the memory bank.

0x0A000400   Correctable memory error logging limit reached

Explanation: The correctable memory error logging threshold for the specified blade server was reached.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: At a convenient time, perform these steps:
1. Update the service processor firmware and BIOS for the blade server.
2. Reseat the memory DIMM. Take note of the DIMM part number and size for future reference.
3. Re-enable the memory bank in BIOS. Boot the blade server to BIOS and re-enable the memory bank.
4. Replace the memory DIMM. Refer to the Problem Determination and Service Guide for the specified blade server type for information about replacing memory. The Problem Determination and Service Guide is available on the Web.

0x0A000401   Correctable memory error logging limit reached on DIMM 01

Related messages:
- 0x0A000402 : Correctable memory error logging limit reached on DIMM 02
- 0x0A000403 : Correctable memory error logging limit reached on DIMM 03

- 0x0A000404 : Correctable memory error logging limit reached on DIMM 04
- 0x0A000405 : Correctable memory error logging limit reached on DIMM 05
- 0x0A000406 : Correctable memory error logging limit reached on DIMM 06
- 0x0A000407 : Correctable memory error logging limit reached on DIMM 07
- 0x0A000408 : Correctable memory error logging limit reached on DIMM 08
- 0x0A000409 : Correctable memory error logging limit reached on DIMM 09
- 0x0A00040A : Correctable memory error logging limit reached on DIMM 10
- 0x0A00040B : Correctable memory error logging limit reached on DIMM 11
- 0x0A00040C : Correctable memory error logging limit reached on DIMM 12
- 0x0A00040D : Correctable memory error logging limit reached on DIMM 13
- 0x0A00040E : Correctable memory error logging limit reached on DIMM 14
- 0x0A00040F : Correctable memory error logging limit reached on DIMM 15
- 0x0A000410 : Correctable memory error logging limit reached on DIMM 16

Explanation: The correctable memory error logging threshold for the specified blade server was reached.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: At your earliest convenience, perform these steps:
1. Update the service processor firmware and BIOS for the blade server.
2. Reseat the memory DIMM. Take note of the DIMM part number and size for future reference.
3. Re-enable the memory bank in BIOS. Boot the blade server to BIOS and re-enable the memory bank.
4. Replace the memory DIMM. Refer to the Problem Determination and Service Guide for the specified blade server type for information about replacing memory. The Problem Determination and Service Guide is available on the Web.

0x0A000580   Memory disabled

Explanation: The specified DIMM for the specified blade server has been disabled. This is a result of a previous uncorrectable memory error.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: This error generally follows another memory error. If you already performed the actions for the previous uncorrectable memory error, no additional action is required. If not, perform these steps:
1. Check the IBM Support Web page for related service bulletins.
2. Check the blade server BIOS change history on the Web for any memory related fixes. Update the BIOS if applicable.
3. Use Light Path diagnostics to verify the affected DIMM bank.
   a. Record the DIMM part number and size for future reference.

0x0A000581

Note: For some blade servers, the DIMM part number is available through the advanced management module Web interface.

b. Verify that the memory DIMM is supported on the IBM ServerProven Web site.

4. Check to make sure the DIMMs are seated properly (especially if this is a new installation). If the DIMMs required reseating, boot the blade into BIOS setup and enable the memory bank.

5. Replace the DIMMs in the memory bank, boot the blade server to BIOS setup and enable the memory bank.

0x0A000581   Memory disabled on DIMM 01

Related messages:
- 0x0A000582 : Memory disabled on DIMM 02
- 0x0A000583 : Memory disabled on DIMM 03
- 0x0A000584 : Memory disabled on DIMM 04
- 0x0A000585 : Memory disabled on DIMM 05
- 0x0A000586 : Memory disabled on DIMM 06
- 0x0A000587 : Memory disabled on DIMM 07
- 0x0A000588 : Memory disabled on DIMM 08
- 0x0A000589 : Memory disabled on DIMM 09
- 0x0A00058A : Memory disabled on DIMM 10
- 0x0A00058B : Memory disabled on DIMM 11
- 0x0A00058C : Memory disabled on DIMM 12
- 0x0A00058D : Memory disabled on DIMM 13
- 0x0A00058E : Memory disabled on DIMM 14
- 0x0A00058F : Memory disabled on DIMM 15
- 0x0A000590 : Memory disabled on DIMM 16

Explanation: The specified DIMM for the specified blade server has been disabled. This is a result of a previous uncorrectable memory error.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Memory device 01 (DIMM 01 Status) memory disabled

Alarm Panel LED (BC T and BC HT):   Critical

User response: This error generally follows another memory error. If you already performed the actions for the previous uncorrectable memory error, no additional action is required. If not, perform these steps:

1. Check the IBM Support Web page for related service bulletins.

2. Check the blade server BIOS change history on the Web for any memory related fixes. Update the BIOS if applicable.

3. Use Light Path diagnostics to verify the affected DIMM bank.

a. Record the DIMM part number and size for future reference.

Note: For some blade servers, the DIMM part number is available through the advanced management module Web interface.

b. Verify that the memory DIMM is supported on the IBM ServerProven Web site.

4. Check to make sure the DIMMs are seated properly (especially if this is a new installation). If the DIMMs required reseating, boot the blade into BIOS setup and enable the memory bank.

5. Replace the DIMMs in the memory bank, boot the blade server to BIOS setup and enable the memory bank.

0x0A002001   Chassis Cooling Device 01 installed

Related messages:
- 0x0A002002 : Chassis Cooling Device 02 installed
- 0x0A002003 : Chassis Cooling Device 03 installed
- 0x0A002004 : Chassis Cooling Device 04 installed
- 0x0A002005 : Chassis Cooling Device 05 installed
- 0x0A002006 : Chassis Cooling Device 06 installed
- 0x0A002007 : Chassis Cooling Device 07 installed
- 0x0A002008 : Chassis Cooling Device 08 installed
- 0x0A002009 : Chassis Cooling Device 09 installed
- 0x0A00200A : Chassis Cooling Device 10 installed

Explanation: A fan module has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: Cool_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0A003001   Chassis Cooling Device 01 removed

Related messages:
- 0x0A003002 : Chassis Cooling Device 02 removed
- 0x0A003003 : Chassis Cooling Device 03 removed
- 0x0A003004 : Chassis Cooling Device 04 removed
- 0x0A003005 : Chassis Cooling Device 05 removed
- 0x0A003006 : Chassis Cooling Device 06 removed
- 0x0A003007 : Chassis Cooling Device 07 removed
- 0x0A003008 : Chassis Cooling Device 08 removed
- 0x0A003009 : Chassis Cooling Device 09 removed
- 0x0A00300A : Chassis Cooling Device 10 removed

Explanation: A fan module has been removed from the chassis.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: Cool_##

Automatically notify service: No

Recoverable: No

User response: Make sure that all fan modules are installed in the chassis.

0x0A00AC02 1.2V standby under recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server standby power module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0A00BC02 1.2V standby over recommended voltage

Explanation: The service processor on the specified blade server has detected that the voltage of the blade server standby power module has reached or exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

2. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x0A027000   Insufficient Chassis Cooling to support blade operations. Blades will be shutdown

Explanation: The management module is starting the process of shutting down blade servers because of fan modules failures.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Replace the fan modules.
2. Power on all blade servers.

0x0A027100 **Reduced cooling capacity in the chassis. Loss of an additional Chassis Cooling Device will cause blade(s) to shutdown.**

Explanation: The cooling capacity for the chassis has been reduced because a fan module has failed or has been removed. If additional fan modules fail or are removed, blade servers might be shut down.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Major

User response: Perform these steps:

1. If you removed a fan module, replace the fan module.
2. Look in the event log for errors related to fan module events and resolve them.

0x0A02CC00 **I/O board 3.3V under recommended voltage**

Explanation: Voltage of I/O board power module whose nominal output is +3.3V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A02CC01 **I/O board 3.3V standby under recommended voltage**

Explanation: Voltage of I/O board standby power module whose nominal output is +3.3V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board.

0x0A02CC02 **3.3V standby under recommended voltage**

Explanation: The voltage of the standby power module in the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

0x0A02DC00 • 0x0A02DC02

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A02DC00 I/O board 3.3V over recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +3.3V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board.

0x0A02DC01 I/O board 3.3V standby over recommended voltage

Explanation: Voltage of I/O board standby power module whose nominal output is +3.3V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A02DC02 3.3V standby over recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A030C00   I/O board 2.5V under recommended voltage.

Explanation: Voltage of I/O board power module whose nominal output is +2.5V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A030C01   I/O board 2.5V standby under recommended voltage

Explanation: Voltage of I/O board standby power module whose nominal output is +2.5V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A030C02   2.5V standby under recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response:

0x0A031C00 • 0x0A031C02

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A031C00   I/O board 2.5V over recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +2.5V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A031C01   I/O board 2.5V standby over recommended voltage

Explanation: Voltage of I/O board standby power module whose nominal output is +2.5V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A031C02   2.5V standby over recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response:
1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A034C00 I/O board 5V under recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +5V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board. If no functional problems exist with the blade then this log can be ignored.

0x0A034C02 5V standby under recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A035C00 I/O board 5V over recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +5V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board. If no functional problems exist with the blade then this log can be ignored.

0x0A035C02 5V standby over recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A036C00 I/O board 12V under recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +12V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A036C01 I/O board 12V standby under recommended voltage

Explanation: Voltage of I/O board standby power module whose nominal output is +12V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A036C02   12V standby under recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A037C00   I/O board 12V over recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +12V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A037C01   I/O board 12V standby over recommended voltage

Explanation: Voltage of I/O board standby power module whose nominal output is +12V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board. If no functional problems exist with the blade then this log can be ignored.

0x0A037C02 12V standby over recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A03CC00 I/O board -5V under recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is -5V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board. If no functional problems exist with the blade then this log can be ignored.

0x0A03DC00 I/O board -5V over recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is -5V rises up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board. If no functional problems exist with the blade then this log can be ignored.

0x0A040C00 I/O board 1.5V under recommended voltage

Explanation: Voltage of I/O board standby power module whose nominal output is +1.5V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A040C02 1.5V standby under recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A041C00 I/O board 1.5V over recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +1.5V rises up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board.

0x0A041C02 • 0x0A07AC02

0x0A041C02 1.5V standby over recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A07AC00 I/O board 1.8V under recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +1.8V drops down under recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A07AC02 1.8V standby under recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0A07BC00 I/O board 1.8V over recommended voltage

Explanation: Voltage of I/O board power module whose nominal output is +1.8V rise up over recommended voltage.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: It is possibly a hardware problem of the I/O board, if no functional problems exist with the blade then this log can be ignored.

0x0A07BC02 1.8V standby over recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0B026001   Unrecognized Chassis Cooling Device 01

Related messages:

- 0x0B026002 : Unrecognized Chassis Cooling Device 02
- 0x0B026003 : Unrecognized Chassis Cooling Device 03
- 0x0B026004 : Unrecognized Chassis Cooling Device 04
- 0x0B026005 : Unrecognized Chassis Cooling Device 05
- 0x0B026006 : Unrecognized Chassis Cooling Device 06
- 0x0B026007 : Unrecognized Chassis Cooling Device 07
- 0x0B026008 : Unrecognized Chassis Cooling Device 08
- 0x0B026009 : Unrecognized Chassis Cooling Device 09
- 0x0B02600A : Unrecognized Chassis Cooling Device 10

Explanation: The management module does not recognize the vital product data for the fan module.

Severity: Error

Alert Category: Cooling Devices (Critical) - mmTrapFanC

0x0D000281 • 0x0D01E000

Log Source: Cool_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these actions:
1. Wait approximately 15 minutes to see if a recovery message is generated.
2. If the problem persists (or a recovery message is not generated), replace the fan module.

0x0D000281   Expansion card in slot 01 is not supported in current BSE configuration

Related messages:
- 0x0D000282 : Expansion card in slot 02 is not supported in current BSE configuration

Explanation: The specified expansion option card is not operational in the specified BladeCenter Storage Expansion Unit because the expansion unit is installed on a BladeCenter Memory and I/O Expansion blade.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: If the function of the expansion option card is not needed, no action is required. Otherwise, perform one of these steps:
- Install the expansion option cards on either the blade server or the BladeCenter Memory and I/O Expansion Blade.
- Install the BladeCenter Storage Expansion Unit directly on a blade server.

0x0D01E000   High speed expansion card fault

Explanation: A fault has occurred in the high-speed expansion card in the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Verify that the high-speed expansion card is supported in the blade server (go to the IBM ServerProven Web site).
2. Update the firmware for the high-speed expansion card.
3. Flash (update if applicable) the firmware for the service processor (BMC), BIOS, and firmware for the advanced management module.
4. Reseat the high-speed expansion card.
5. Replace the high-speed expansion card.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about removing and installing a high-speed expansion card. The Problem Determination and Service Guide is available on the Web.

0x0E002001   Blade 01 installed

Related messages:

- 0x0E002002 : Blade 02 installed
- 0x0E002003 : Blade 03 installed
- 0x0E002004 : Blade 04 installed
- 0x0E002005 : Blade 05 installed
- 0x0E002006 : Blade 06 installed
- 0x0E002007 : Blade 07 installed
- 0x0E002008 : Blade 08 installed
- 0x0E002009 : Blade 09 installed
- 0x0E00200A : Blade 10 installed
- 0x0E00200B : Blade 11 installed
- 0x0E00200C : Blade 12 installed
- 0x0E00200D : Blade 13 installed
- 0x0E00200E : Blade 14 installed

Explanation: The specified blade server has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0E004001   Blade 01 removed

Related messages:

- 0x0E004002 : Blade 02 removed
- 0x0E004003 : Blade 03 removed
- 0x0E004004 : Blade 04 removed
- 0x0E004005 : Blade 05 removed
- 0x0E004006 : Blade 06 removed
- 0x0E004007 : Blade 07 removed
- 0x0E004008 : Blade 08 removed
- 0x0E004009 : Blade 09 removed
- 0x0E00400A : Blade 10 removed
- 0x0E00400B : Blade 11 removed
- 0x0E00400C : Blade 12 removed
- 0x0E00400D : Blade 13 removed
- 0x0E00400E : Blade 14 removed

Explanation: The specified blade server has been removed from the chassis.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

0x0E006001 • 0x0E008001

User response: Information only; no action is required.

0x0E006001   Blade 01 incompatible with I/O module configuration

Related messages:
- 0x0E006002 : Blade 02 incompatible with I/O module configuration
- 0x0E006003 : Blade 03 incompatible with I/O module configuration
- 0x0E006004 : Blade 04 incompatible with I/O module configuration
- 0x0E006005 : Blade 05 incompatible with I/O module configuration
- 0x0E006006 : Blade 06 incompatible with I/O module configuration
- 0x0E006007 : Blade 07 incompatible with I/O module configuration
- 0x0E006008 : Blade 08 incompatible with I/O module configuration
- 0x0E006009 : Blade 09 incompatible with I/O module configuration
- 0x0E00600A : Blade 10 incompatible with I/O module configuration
- 0x0E00600B : Blade 11 incompatible with I/O module configuration
- 0x0E00600C : Blade 12 incompatible with I/O module configuration
- 0x0E00600D : Blade 13 incompatible with I/O module configuration
- 0x0E00600E : Blade 14 incompatible with I/O module configuration

Explanation: The fabric type of an expansion card option in the specified blade server is not compatible with an I/O module in the I/O module bay. Data might not be passed on one or more possible connections.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Verify that the network is set up as desired. To verify the network configuration from the advanced management module Web interface, click **Blades** and then click **I/O compatibility**. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card option in the specified blade server is compatible with the fabric type of the I/O module.

0x0E008001   Blade 01 is not responding on the management bus

Related messages:
- 0x0E008002 : Blade 02 is not responding on the management bus
- 0x0E008003 : Blade 03 is not responding on the management bus
- 0x0E008004 : Blade 04 is not responding on the management bus
- 0x0E008005 : Blade 05 is not responding on the management bus
- 0x0E008006 : Blade 06 is not responding on the management bus
- 0x0E008007 : Blade 07 is not responding on the management bus
- 0x0E008008 : Blade 08 is not responding on the management bus
- 0x0E008009 : Blade 09 is not responding on the management bus
- 0x0E00800A : Blade 10 is not responding on the management bus
- 0x0E00800B : Blade 11 is not responding on the management bus
- 0x0E00800C : Blade 12 is not responding on the management bus
- 0x0E00800D : Blade 13 is not responding on the management bus
- 0x0E00800E : Blade 14 is not responding on the management bus

Explanation: The specified blade is not responding to the advanced management module on the blade management bus.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the advanced management module.
2. Initiate a failover to the standby advanced management module.
3. Reset the service processor on the blade server.
4. Reseat the blade server.
5. Update the firmware for the service processor on the blade server. You can find firmware on the IBM BladeCenter software and device drivers Web page.

0x0E00A001   Blade 01 not allowed to power on due to insufficient power.

Related messages:
- 0x0E00A002 : Blade 02 not allowed to power on due to insufficient power.
- 0x0E00A003 : Blade 03 not allowed to power on due to insufficient power.
- 0x0E00A004 : Blade 04 not allowed to power on due to insufficient power.
- 0x0E00A005 : Blade 05 not allowed to power on due to insufficient power.
- 0x0E00A006 : Blade 06 not allowed to power on due to insufficient power.
- 0x0E00A007 : Blade 07 not allowed to power on due to insufficient power.
- 0x0E00A008 : Blade 08 not allowed to power on due to insufficient power.
- 0x0E00A009 : Blade 09 not allowed to power on due to insufficient power.
- 0x0E00A00A : Blade 10 not allowed to power on due to insufficient power.
- 0x0E00A00B : Blade 11 not allowed to power on due to insufficient power.
- 0x0E00A00C : Blade 12 not allowed to power on due to insufficient power.
- 0x0E00A00D : Blade 13 not allowed to power on due to insufficient power.
- 0x0E00A00E : Blade 14 not allowed to power on due to insufficient power.

Explanation: The specified blade server cannot be powered on due to insufficient power capacity in the power budget.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Select a different power management policy to increase the power budget.
2. Add additional power modules or upgrade the power modules to increase power capacity (if applicable).
3. Reseat the blade server.
4. Shut down other devices in the chassis.

0x0E00B001   I/O module 01 is not allowed to power on due to insufficient power.

Related messages:
* 0x0E00B002 : I/O module 02 is not allowed to power on due to insufficient power.
* 0x0E00B003 : I/O module 03 is not allowed to power on due to insufficient power.
* 0x0E00B004 : I/O module 04 is not allowed to power on due to insufficient power.
* 0x0E00B005 : I/O module 05 is not allowed to power on due to insufficient power.
* 0x0E00B006 : I/O module 06 is not allowed to power on due to insufficient power.
* 0x0E00B007 : I/O module 07 is not allowed to power on due to insufficient power.
* 0x0E00B008 : I/O module 08 is not allowed to power on due to insufficient power.
* 0x0E00B009 : I/O module 09 is not allowed to power on due to insufficient power.
* 0x0E00B00A : I/O module 10 is not allowed to power on due to insufficient power.

Explanation: The management module has detected that there is not sufficient power capacity in the power budget to allow the specified I/O module to power on.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Select a different power management policy to increase the power budget.
2. Add additional power modules or upgrade the power modules to increase power capacity.
3. Reseat the blade server.
4. Shut down other devices in the chassis.

0x0E00C001   Blade 01 throttled

Related messages:
* 0x0E00C002 : Blade 02 throttled
* 0x0E00C003 : Blade 03 throttled
* 0x0E00C004 : Blade 04 throttled
* 0x0E00C005 : Blade 05 throttled
* 0x0E00C006 : Blade 06 throttled
* 0x0E00C007 : Blade 07 throttled
* 0x0E00C008 : Blade 08 throttled
* 0x0E00C009 : Blade 09 throttled
* 0x0E00C00A : Blade 10 throttled
* 0x0E00C00B : Blade 11 throttled
* 0x0E00C00C : Blade 12 throttled
* 0x0E00C00D : Blade 13 throttled
* 0x0E00C00E : Blade 14 throttled

Explanation: The specified blade server has throttled; it is achieving lower power consumption by temporarily reducing the CPU throughput. This might be because the chassis has been set to acoustic mode (set from the Power Management page of the advanced management module Web interface), there is a problem with a power module, or the power module has been removed from the chassis.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Check the event log for other events related to the power module and resolve those messages.
2. If acoustic mode is set for the chassis:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
   c. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
   d. Make sure that there is nothing covering the media tray (that will disrupt the airflow to the ambient temperature sensor).
   e. Update the firmware for the advanced management module. You can find firmware on the IBM BladeCenter software and device drivers Web page.
   f. Update the firmware for the blade server.
   g. For all blade servers other than the JSxx blade servers, make sure the heat sink and CPU are secured on the system board.

   Note: Be careful when handling the heat sink and CPU, they may be extremely hot.
3. Verify that all power modules are functional (the DC LEDs are lit).
4. Reseat the blade server.
5. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x0E00C28F   Blade will not throttle

Explanation: The server processor will not throttle the blade server. Throttling refers to achieving lower power consumption for a blade by temporarily reducing the CPU throughput.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x0E00D001   Storage Module 01 is not allowed to power on due to insufficient power.

Related messages:

- 0x0E00D002 : Storage Module 02 is not allowed to power on due to insufficient power.

Explanation: The advanced management module has detected that there is insufficient power capacity in the power budget to allow the specified storage module to power on.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

0x0E00D281 • 0x0E00D381

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Select a different power management policy to increase the power budget.
2. Add additional power modules to increase power capacity.
3. Shut down other devices in the chassis.

0x0E00D281 Storage Module 01 is not allowed to power on due to insufficient cooling.

Related messages:

- 0x0E00D282 : Storage Module 02 is not allowed to power on due to insufficient cooling.

Explanation: There is insufficient cooling capacity to power on the specified storage module. This typically occurs because there is no power module installed (or it has failed) in the power module bay directly behind the specified storage module.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Make sure that you have a functioning power module installed behind the specified storage module. For storage module 1, you must have functioning power modules installed in power module bays 1 and 2. For storage module 2, you must have functioning power modules installed in power module bays 3 and 4.
2. Check the event log for errors related to power modules.
3. Resolve any errors that you find.

0x0E00D381 Storage Module 01 reported an early power off event.

Related messages:

- 0x0E00D382 : Storage Module 02 reported an early power off event.

Explanation: A power module located behind the specified storage module has been removed or failed.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. If you removed a power module, this event is informational only; no action is required.
2. If you did not remove a power module, check for other power related events in the event log and resolve those errors.

0x0E010001   Blade 01 VPD cannot be read

Related messages:

- 0x0E010002 : Blade 02 VPD cannot be read
- 0x0E010003 : Blade 03 VPD cannot be read
- 0x0E010004 : Blade 04 VPD cannot be read
- 0x0E010005 : Blade 05 VPD cannot be read
- 0x0E010006 : Blade 06 VPD cannot be read
- 0x0E010007 : Blade 07 VPD cannot be read
- 0x0E010008 : Blade 08 VPD cannot be read
- 0x0E010009 : Blade 09 VPD cannot be read
- 0x0E01000A : Blade 10 VPD cannot be read
- 0x0E01000B : Blade 11 VPD cannot be read
- 0x0E01000C : Blade 12 VPD cannot be read
- 0x0E01000D : Blade 13 VPD cannot be read
- 0x0E01000E : Blade 14 VPD cannot be read

Explanation: The advanced management module cannot read the vital product data (VPD) for the specified blade server.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0E012041   Blade power meter monitoring off line

Explanation: A power monitoring fault has occurred for the specified blade server.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: If the specified blade server is operational, you can wait to perform the following steps. However, the power consumption numbers displayed in the advanced management module will not be accurate.

1. Reset the service processor on the blade server. You might need to reset it up to three times.
2. Update the service processor firmware.
3. Replace the blade server.

0x0E012042   Power control capability of blade has changed

Explanation: The power control capability of a blade server has changed.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: Blade_##

Automatically notify service: No

0x0E012047 • 0x0E200001

Recoverable: Yes

User response: Information only; no action is required.

0x0E012047   Blade has been throttled; low clock rate

Explanation: Blade has been throttled to low clock rate.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x0E200001   Power denied to blade 01 because it has unidentified hardware

Related messages:
- 0x0E200002 : Power denied to blade 02 because it has unidentified hardware
- 0x0E200003 : Power denied to blade 03 because it has unidentified hardware
- 0x0E200004 : Power denied to blade 04 because it has unidentified hardware
- 0x0E200005 : Power denied to blade 05 because it has unidentified hardware
- 0x0E200006 : Power denied to blade 06 because it has unidentified hardware
- 0x0E200007 : Power denied to blade 07 because it has unidentified hardware
- 0x0E200008 : Power denied to blade 08 because it has unidentified hardware
- 0x0E200009 : Power denied to blade 09 because it has unidentified hardware
- 0x0E20000A : Power denied to blade 10 because it has unidentified hardware
- 0x0E20000B : Power denied to blade 11 because it has unidentified hardware
- 0x0E20000C : Power denied to blade 12 because it has unidentified hardware
- 0x0E20000D : Power denied to blade 13 because it has unidentified hardware
- 0x0E20000E : Power denied to blade 14 because it has unidentified hardware

Explanation: The specified blade server contains components that cannot be identified by the management module. For example, the blade server may have an expansion card that is not recognized. Therefore, the power requirements for the component cannot be determined.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Verify that all components in the blade server are on the ServerProven list for that blade server (go to the IBM ServerProven Web site).
2. Update the blade server service processor (BMC) firmware to the latest level.
3. Update the firmware for the advanced management module.
4. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x0E418802   Expansion Module fault.

Explanation: A fault has occurred in either the BladeCenter Storage Expansion (BSE) Unit or the Peripheral Component Interconnect(PCI) Expansion Unit.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: From the advanced management module Web interface, view the hardware VPD page to determine whether the fault is in the BladeCenter Storage Expansion Unit or the Peripheral Component Interconnect (PCI) Expansion Unit.
- If the fault is in the BladeCenter Storage Expansion Unit, perform these steps:
  1. Update the service processor firmware, the BIOS, and the ServeRAID application for the blade server.
  2. Reseat the following components one at a time, in the order shown, restarting the blade server each time:
      a. ServeRAID SAS controller
      b. RAID battery
      c. BladeCenter Storage Expansion Unit
  3. Replace the BladeCenter Storage Expansion Unit.
- If the fault is in the Peripheral Component Interconnect (PCI) Expansion Unit, perform these steps:
  1. Verify that the PCI adapters are supported in the blade server. See the IBM ServerProven Web site to determine which PCI adapters are supported.
  2. Reseat the PCI expansion unit.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about the BladeCenter Storage Expansion Unit and the Peripheral Component Interconnect (PCI) Expansion Unit. The Problem Determination and Service Guide is available on the Web.

0x0E830402   BEM 2.5V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E830802 • 0x0E832802

0x0E830802   BEM 2.5V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E832402   BEM 3.3V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E832802   BEM 3.3V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E834402   BEM 5V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E834802   BEM 5V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E836402   BEM 12V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E836802   BEM 12V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E83C402   BEM 18V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E83C802   BEM 18V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E840402   BEM 1.5V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E840802   BEM 1.5V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E850402   BEM 1V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:
1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E850802   BEM 1V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E860402   BEM 12V standby over recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response:

1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E860802   BEM 12V standby under recommended voltage

Explanation: The voltage of the standby power module in the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response:

1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E87A402   BEM 1.8V over recommended voltage

Explanation: The voltage of the blade expansion module has exceeded the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response:
1. Check the event log for other over voltage events. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0E87A802   BEM 1.8V under recommended voltage

Explanation: The voltage of the blade expansion module has reached or fallen below the recommended voltage threshold.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response:
1. Check the event log for other under voltage events. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the under voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
2. Reseat the blade server, the blade I/O expansion module (if installed), and the blade expansion module.

0x0EA00001   I/O module 01 fault

Related messages:
- 0x0EA00002 : I/O module 02 fault
- 0x0EA00003 : I/O module 03 fault
- 0x0EA00004 : I/O module 04 fault
- 0x0EA00005 : I/O module 05 fault
- 0x0EA00006 : I/O module 06 fault
- 0x0EA00007 : I/O module 07 fault
- 0x0EA00008 : I/O module 08 fault
- 0x0EA00009 : I/O module 09 fault

- 0x0EA0000A : I/O module 10 fault

Explanation: The advanced management module cannot read the status of the specified I/O module due to a fault.

Severity: Error

Alert Category: I/O Modules (Critical) - mmTrapIOC

Log Source: IOMod_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Examine the event log. Communication problems on the I2C management bus can cause this error as well as a failed I/O module. Actions for bus issues include restarting the advanced management module, failing over to a standby advanced management module, and reseating the components on the bus, including the advanced management module and the I/O module.
2. Update the firmware for the I/O module.
3. Replace the I/O module.

0x0EA01001 Unable to read VPD for I/O Module 01

Related messages:
- 0x0EA01002 : Unable to read VPD for I/O Module 02
- 0x0EA01003 : Unable to read VPD for I/O Module 03
- 0x0EA01004 : Unable to read VPD for I/O Module 04
- 0x0EA01005 : Unable to read VPD for I/O Module 05
- 0x0EA01006 : Unable to read VPD for I/O Module 06
- 0x0EA01007 : Unable to read VPD for I/O Module 07
- 0x0EA01008 : Unable to read VPD for I/O Module 08
- 0x0EA01009 : Unable to read VPD for I/O Module 09
- 0x0EA0100A : Unable to read VPD for I/O Module 10

Explanation: The advanced management module is not able to read the vital product data (VPD) for the specific I/O module.

Severity: Error

Alert Category: I/O Modules (Critical) - mmTrapIOC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. If you have just installed the I/O module:
   a. Reset the I/O module through the advanced management module interface.
   b. Replace the I/O module.
2. If you have recently updated the firmware for the advanced management module, revert back to the previous release of the firmware to see if this resolves the problem.
3. If the I/O module has been working and you have not recently upgraded the management module firmware:

0x0EA02001 • 0x0EA04001

  a. Use the advanced management module interface to determine if the other I/O modules are present. If so, suspect the I/O module.

  b. Fail over to the second advanced management module (if an advanced management module is available in your chassis).

  c. Reboot the advanced management module.

  d. Upgrade the advanced management module firmware.

  e. Replace the advanced management module.

0x0EA02001   I/O module 01 installed

Related messages:
- 0x0EA02002 : I/O module 02 installed
- 0x0EA02003 : I/O module 03 installed
- 0x0EA02004 : I/O module 04 installed
- 0x0EA02005 : I/O module 05 installed
- 0x0EA02006 : I/O module 06 installed
- 0x0EA02007 : I/O module 07 installed
- 0x0EA02008 : I/O module 08 installed
- 0x0EA02009 : I/O module 09 installed
- 0x0EA0200A : I/O module 10 installed

Explanation: The specified I/O module has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA04001   I/O module 01 removed

Related messages:
- 0x0EA04002 : I/O module 02 removed
- 0x0EA04003 : I/O module 03 removed
- 0x0EA04004 : I/O module 04 removed
- 0x0EA04005 : I/O module 05 removed
- 0x0EA04006 : I/O module 06 removed
- 0x0EA04007 : I/O module 07 removed
- 0x0EA04008 : I/O module 08 removed
- 0x0EA04009 : I/O module 09 removed
- 0x0EA0400A : I/O module 10 removed

Explanation: The specified I/O module has been removed from the chassis.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA05001   I/O module 01 in the interposer is not supported in this configuration.

Related messages:
- 0x0EA05002 : I/O module 02 in the interposer is not supported in this configuration.
- 0x0EA05003 : I/O module 03 in the interposer is not supported in this configuration.
- 0x0EA05004 : I/O module 04 in the interposer is not supported in this configuration.
- 0x0EA05005 : I/O module 05 in the interposer is not supported in this configuration.
- 0x0EA05006 : I/O module 06 in the interposer is not supported in this configuration.
- 0x0EA05007 : I/O module 07 in the interposer is not supported in this configuration.
- 0x0EA05008 : I/O module 08 in the interposer is not supported in this configuration.
- 0x0EA05009 : I/O module 09 in the interposer is not supported in this configuration.
- 0x0EA0500A : I/O module 10 in the interposer is not supported in this configuration.

Explanation: The specified I/O module is not compatible with the interposer into which it has been installed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Make sure the I/O module being installed in this I/O module bay is compatible with the interposer that was installed in the I/O module bay. Read the documentation provided with the interposer to determine which I/O modules are compatible.

0x0EA06001   I/O module 01 was instructed to power off.

Related messages:
- 0x0EA06002 : I/O module 02 was instructed to power off.
- 0x0EA06003 : I/O module 03 was instructed to power off.
- 0x0EA06004 : I/O module 04 was instructed to power off.
- 0x0EA06005 : I/O module 05 was instructed to power off.
- 0x0EA06006 : I/O module 06 was instructed to power off.
- 0x0EA06007 : I/O module 07 was instructed to power off.
- 0x0EA06008 : I/O module 08 was instructed to power off.
- 0x0EA06009 : I/O module 09 was instructed to power off.
- 0x0EA0600A : I/O module 10 was instructed to power off.

Explanation: The specified I/O module has been powered off.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA08001   I/O module 01 was instructed to power on.

Related messages:
- 0x0EA08002 : I/O module 02 was instructed to power on.
- 0x0EA08003 : I/O module 03 was instructed to power on.
- 0x0EA08004 : I/O module 04 was instructed to power on.
- 0x0EA08005 : I/O module 05 was instructed to power on.
- 0x0EA08006 : I/O module 06 was instructed to power on.
- 0x0EA08007 : I/O module 07 was instructed to power on.
- 0x0EA08008 : I/O module 08 was instructed to power on.
- 0x0EA08009 : I/O module 09 was instructed to power on.
- 0x0EA0800A : I/O module 10 was instructed to power on.

Explanation: The specified I/O module has powered on.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0A001   I/O module 01 IP configuration was changed.

Related messages:
- 0x0EA0A002 : I/O module 02 IP configuration was changed.
- 0x0EA0A003 : I/O module 03 IP configuration was changed.
- 0x0EA0A004 : I/O module 04 IP configuration was changed.
- 0x0EA0A005 : I/O module 05 IP configuration was changed.
- 0x0EA0A006 : I/O module 06 IP configuration was changed.
- 0x0EA0A007 : I/O module 07 IP configuration was changed.
- 0x0EA0A008 : I/O module 08 IP configuration was changed.
- 0x0EA0A009 : I/O module 09 IP configuration was changed.
- 0x0EA0A00A : I/O module 10 IP configuration was changed.

Explanation: The IP address for the specified I/O module has been changed.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0B001   I/O module 01 incompatible with other I/O modules

Related messages:
- 0x0EA0B002 : I/O module 02 incompatible with other I/O modules
- 0x0EA0B003 : I/O module 03 incompatible with other I/O modules
- 0x0EA0B004 : I/O module 04 incompatible with other I/O modules
- 0x0EA0B005 : I/O module 05 incompatible with other I/O modules

- 0x0EA0B006 : I/O module 06 incompatible with other I/O modules
- 0x0EA0B007 : I/O module 07 incompatible with other I/O modules
- 0x0EA0B008 : I/O module 08 incompatible with other I/O modules
- 0x0EA0B009 : I/O module 09 incompatible with other I/O modules
- 0x0EA0B00A : I/O module 10 incompatible with other I/O modules

Explanation: The specified I/O module is not compatible with other I/O modules (due to different I/O fabric types).

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Make sure the I/O module is in the correct I/O module bay.

0x0EA0C001 I/O module 01 incompatible with blade configuration

Related messages:
- 0x0EA0C002 : I/O module 02 incompatible with blade configuration
- 0x0EA0C003 : I/O module 03 incompatible with blade configuration
- 0x0EA0C004 : I/O module 04 incompatible with blade configuration
- 0x0EA0C005 : I/O module 05 incompatible with blade configuration
- 0x0EA0C006 : I/O module 06 incompatible with blade configuration
- 0x0EA0C007 : I/O module 07 incompatible with blade configuration
- 0x0EA0C008 : I/O module 08 incompatible with blade configuration
- 0x0EA0C009 : I/O module 09 incompatible with blade configuration
- 0x0EA0C00A : I/O module 10 incompatible with blade configuration

Explanation: The I/O fabric type for the expansion card option in the blade server is not compatible with the specified I/O module.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Make sure that the expansion card option in the blade server and the I/O module are compatible (are of the same I/O fabric type).

0x0EA0C101 I/O module 01 incompatible with Storage Module configuration

Related messages:
- 0x0EA0C102 : I/O module 02 incompatible with Storage Module configuration
- 0x0EA0C103 : I/O module 03 incompatible with Storage Module configuration
- 0x0EA0C104 : I/O module 04 incompatible with Storage Module configuration
- 0x0EA0C105 : I/O module 05 incompatible with Storage Module configuration
- 0x0EA0C106 : I/O module 06 incompatible with Storage Module configuration
- 0x0EA0C107 : I/O module 07 incompatible with Storage Module configuration

0x0EA0D001

- 0x0EA0C108 : I/O module 08 incompatible with Storage Module configuration
- 0x0EA0C109 : I/O module 09 incompatible with Storage Module configuration
- 0x0EA0C10A : I/O module 10 incompatible with Storage Module configuration

Explanation: The specified I/O module is not compatible with the storage module. You must install a SAS connectivity module or a SAS RAID controller module.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Install a SAS connectivity module or a SAS RAID controller module.

0x0EA0D001 I/O module 01 POST timeout.

Related messages:
- 0x0EA0D002 : I/O module 02 POST timeout.
- 0x0EA0D003 : I/O module 03 POST timeout.
- 0x0EA0D004 : I/O module 04 POST timeout.
- 0x0EA0D005 : I/O module 05 POST timeout.
- 0x0EA0D006 : I/O module 06 POST timeout.
- 0x0EA0D007 : I/O module 07 POST timeout.
- 0x0EA0D008 : I/O module 08 POST timeout.
- 0x0EA0D009 : I/O module 09 POST timeout.
- 0x0EA0D00A : I/O module 10 POST timeout.

Explanation: The specified I/O module is taking too long to complete POST.

Severity: Error

Alert Category: I/O Modules (Critical) - mmTrapIOC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: The I/O module may still be in the process of booting. Therefore, if you do not see a recovery message within 15 minutes, perform these steps:

1. If you recently upgraded the firmware for the advanced management module, perform these steps:
   a. Restart the advanced management module.
   b. Revert to the previous level of firmware for the advanced management module to see if the problem is resolved.
2. If you recently upgraded the I/O module firmware, revert to the previous level of firmware for the I/O module.
3. Attempt to reset the I/O module through the advanced management module interface.
4. Reset the I/O module.
5. Replace the I/O module.

0x0EA0D201 Attempt to set port link state on I/O Module 01

Related messages:

- 0x0EA0D202 : Attempt to set port link state on I/O Module 02
- 0x0EA0D203 : Attempt to set port link state on I/O Module 03
- 0x0EA0D204 : Attempt to set port link state on I/O Module 04
- 0x0EA0D205 : Attempt to set port link state on I/O Module 05
- 0x0EA0D206 : Attempt to set port link state on I/O Module 06
- 0x0EA0D207 : Attempt to set port link state on I/O Module 07
- 0x0EA0D208 : Attempt to set port link state on I/O Module 08
- 0x0EA0D209 : Attempt to set port link state on I/O Module 09
- 0x0EA0D20A : Attempt to set port link state on I/O Module 10

Explanation: A user has attempted to change the port link state on the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: No actions taken.

0x0EA0D301 Port link state is changed on I/O Module 01

Related messages:

- 0x0EA0D302 : Port link state is changed on I/O Module 02
- 0x0EA0D303 : Port link state is changed on I/O Module 03
- 0x0EA0D304 : Port link state is changed on I/O Module 04
- 0x0EA0D305 : Port link state is changed on I/O Module 05
- 0x0EA0D306 : Port link state is changed on I/O Module 06
- 0x0EA0D307 : Port link state is changed on I/O Module 07
- 0x0EA0D308 : Port link state is changed on I/O Module 08
- 0x0EA0D309 : Port link state is changed on I/O Module 09
- 0x0EA0D30A : Port link state is changed on I/O Module 10

Explanation: The port link has been changed on the specified I/O module.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0D401 Change port link state on I/O Module 01 failed

Related messages:

- 0x0EA0D402 : Change port link state on I/O Module 02 failed
- 0x0EA0D403 : Change port link state on I/O Module 03 failed
- 0x0EA0D404 : Change port link state on I/O Module 04 failed
- 0x0EA0D405 : Change port link state on I/O Module 05 failed

0x0EA0D501 • 0x0EA0D601

- 0x0EA0D406 : Change port link state on I/O Module 06 failed
- 0x0EA0D407 : Change port link state on I/O Module 07 failed
- 0x0EA0D408 : Change port link state on I/O Module 08 failed
- 0x0EA0D409 : Change port link state on I/O Module 09 failed
- 0x0EA0D40A : Change port link state on I/O Module 10 failed

Explanation: The port link state for the specified I/O module was not changed.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the user permissions to ensure that the user has the authority to change the port state. See the Advanced Management Module User's Guide for more information about user roles.
2. Attempt to change the port link state again.
3. Check the event log for other errors related to the I/O module (such as communication errors between the advanced management module and the I/O module).
4. Check the advanced management module system status panel to ensure the switch is functioning.

0x0EA0D501 Attempt to set port speed/mode on I/O Module 01

Related messages:
- 0x0EA0D502 : Attempt to set port speed/mode on I/O Module 02
- 0x0EA0D503 : Attempt to set port speed/mode on I/O Module 03
- 0x0EA0D504 : Attempt to set port speed/mode on I/O Module 04
- 0x0EA0D505 : Attempt to set port speed/mode on I/O Module 05
- 0x0EA0D506 : Attempt to set port speed/mode on I/O Module 06
- 0x0EA0D507 : Attempt to set port speed/mode on I/O Module 07
- 0x0EA0D508 : Attempt to set port speed/mode on I/O Module 08
- 0x0EA0D509 : Attempt to set port speed/mode on I/O Module 09
- 0x0EA0D50A : Attempt to set port speed/mode on I/O Module 10

Explanation: A user has attempted to set the port speed and mode on the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: No actions taken.

0x0EA0D601 Port speed/mode is changed on I/O Module 01

Related messages:
- 0x0EA0D602 : Port speed/mode is changed on I/O Module 02
- 0x0EA0D603 : Port speed/mode is changed on I/O Module 03
- 0x0EA0D604 : Port speed/mode is changed on I/O Module 04
- 0x0EA0D605 : Port speed/mode is changed on I/O Module 05

- 0x0EA0D606 : Port speed/mode is changed on I/O Module 06
- 0x0EA0D607 : Port speed/mode is changed on I/O Module 07
- 0x0EA0D608 : Port speed/mode is changed on I/O Module 08
- 0x0EA0D609 : Port speed/mode is changed on I/O Module 09
- 0x0EA0D60A : Port speed/mode is changed on I/O Module 10

Explanation: The port speed and mode has been changed on the specified I/O module.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0D701 Change port speed/mode on I/O Module 01 failed

Related messages:
- 0x0EA0D702 : Change port speed/mode on I/O Module 02 failed
- 0x0EA0D703 : Change port speed/mode on I/O Module 03 failed
- 0x0EA0D704 : Change port speed/mode on I/O Module 04 failed
- 0x0EA0D705 : Change port speed/mode on I/O Module 05 failed
- 0x0EA0D706 : Change port speed/mode on I/O Module 06 failed
- 0x0EA0D707 : Change port speed/mode on I/O Module 07 failed
- 0x0EA0D708 : Change port speed/mode on I/O Module 08 failed
- 0x0EA0D709 : Change port speed/mode on I/O Module 09 failed
- 0x0EA0D70A : Change port speed/mode on I/O Module 10 failed

Explanation: The port speed and mode for the specified I/O module was not changed.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the user permissions to ensure that the user has the authority to change the port speed and mode. See the Advanced Management Module User's Guide for more information about user roles.
2. Attempt to change the port speed and mode again.
3. Check the event log for other errors related to the I/O module (such as communication errors between the advanced management module and the I/O module).
4. Check advanced management module system status panel to ensure the switch is functioning.

0x0EA0D801 Firmware image is activated on I/O Module 01

Related messages:
- 0x0EA0D802 : Firmware image is activated on I/O Module 02
- 0x0EA0D803 : Firmware image is activated on I/O Module 03
- 0x0EA0D804 : Firmware image is activated on I/O Module 04
- 0x0EA0D805 : Firmware image is activated on I/O Module 05

0x0EA0D901 • 0x0EA0DB01

- 0x0EA0D806 : Firmware image is activated on I/O Module 06
- 0x0EA0D807 : Firmware image is activated on I/O Module 07
- 0x0EA0D808 : Firmware image is activated on I/O Module 08
- 0x0EA0D809 : Firmware image is activated on I/O Module 09
- 0x0EA0D80A : Firmware image is activated on I/O Module 10

Explanation: The firmware image for the specified I/O module has been activated.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0D901 Failed to activate firmware image on I/O Module 01

Related messages:
- 0x0EA0D902 : Failed to activate firmware image on I/O Module 02
- 0x0EA0D903 : Failed to activate firmware image on I/O Module 03
- 0x0EA0D904 : Failed to activate firmware image on I/O Module 04
- 0x0EA0D905 : Failed to activate firmware image on I/O Module 05
- 0x0EA0D906 : Failed to activate firmware image on I/O Module 06
- 0x0EA0D907 : Failed to activate firmware image on I/O Module 07
- 0x0EA0D908 : Failed to activate firmware image on I/O Module 08
- 0x0EA0D909 : Failed to activate firmware image on I/O Module 09
- 0x0EA0D90A : Failed to activate firmware image on I/O Module 10

Explanation: The firmware image on the specified I/O module could not be activated. The I/O module will continue running the previously configured firmware.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Make sure that the user has sufficient authority to activate the firmware image. See the Advanced Management Module User's Guide for more information about user roles.
2. Attempt to reload the firmware image.
3. Check the event log for other errors related to the I/O module (such as communication errors between the advanced management module and the I/O module).
4. Check advanced management module system status panel to ensure the switch is functioning.

0x0EA0DB01 Duplicate Route detected to IOM 01

Related messages:
- 0x0EA0DB02 : Duplicate Route detected to IOM 02
- 0x0EA0DB03 : Duplicate Route detected to IOM 03
- 0x0EA0DB04 : Duplicate Route detected to IOM 04

- 0x0EA0DB05 : Duplicate Route detected to IOM 05
- 0x0EA0DB06 : Duplicate Route detected to IOM 06
- 0x0EA0DB07 : Duplicate Route detected to IOM 07
- 0x0EA0DB08 : Duplicate Route detected to IOM 08
- 0x0EA0DB09 : Duplicate Route detected to IOM 09
- 0x0EA0DB0A : Duplicate Route detected to IOM 10

Explanation: The advanced management module detected a duplicate route to the specified I/O module because the internal and external management IP addresses are the same. The advanced management module will ignore the internal route.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required. If desired, you can change the setup of the I/O module so that the external management IP address is different than the internal management address and that it is on a separate subnet.

0x0EA0DC01 IO module 01 internal mangement address and external address are on the same subnet.

Related messages:

- 0x0EA0DC02 : IO module 02 internal mangement address and external address are on the same subnet.
- 0x0EA0DC03 : IO module 03 internal mangement address and external address are on the same subnet.
- 0x0EA0DC04 : IO module 04 internal mangement address and external address are on the same subnet.
- 0x0EA0DC05 : IO module 05 internal mangement address and external address are on the same subnet.
- 0x0EA0DC06 : IO module 06 internal mangement address and external address are on the same subnet.
- 0x0EA0DC07 : IO module 07 internal mangement address and external address are on the same subnet.
- 0x0EA0DC08 : IO module 08 internal mangement address and external address are on the same subnet.
- 0x0EA0DC09 : IO module 09 internal mangement address and external address are on the same subnet.
- 0x0EA0DC0A : IO module 10 internal mangement address and external address are on the same subnet.

Explanation: The specified user has attempted to assign the internal management IP address of the I/O module to the same subnet as the external management network.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Make sure that the exteral management IP address is different than the internal management address, and that it is on a separate subnet.

0x0EA0E001 I/O module 01 POST failure

Related messages:

- 0x0EA0E002 : I/O module 02 POST failure
- 0x0EA0E003 : I/O module 03 POST failure
- 0x0EA0E004 : I/O module 04 POST failure
- 0x0EA0E005 : I/O module 05 POST failure
- 0x0EA0E006 : I/O module 06 POST failure

0x0EA0E101

- 0x0EA0E007 : I/O module 07 POST failure
- 0x0EA0E008 : I/O module 08 POST failure
- 0x0EA0E009 : I/O module 09 POST failure
- 0x0EA0E00A : I/O module 10 POST failure

Explanation: The specified I/O module has encountered a problem during power on self test (POST).

Severity: Error

Alert Category: I/O Modules (Critical) - mmTrapIOC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Major

User response: Perform these steps:
1. Power off the I/O module and attempt to start it again from the Admin Power Restart page of the advanced management module Web interface.
2. Reseat the I/O module.
3. Refer to the documentation for the specified I/O module. The documentation for the specified switch might contain additional information about this problem.
4. Replace the I/O module.

0x0EA0E101   Active zone pointers

Related messages:
- 0x0EA0E102 : Active zone pointers
- 0x0EA0E103 : Active zone pointers
- 0x0EA0E104 : Active zone pointers
- 0x0EA0E105 : Active zone pointers
- 0x0EA0E106 : Active zone pointers
- 0x0EA0E107 : Active zone pointers
- 0x0EA0E108 : Active zone pointers
- 0x0EA0E109 : Active zone pointers
- 0x0EA0E10A : Active zone pointers

Explanation: All SAS I/O modules in the chassis must have the same active zone configuration. The SAS I/O modules currently do not have the same active zone configuration.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT):   Minor

User response: Apply the same active zone configuration to all SAS I/O modules.

0x0EA0E201 I/O Module 01's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

Related messages:

- 0x0EA0E202 : I/O Module 02's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E203 : I/O Module 03's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E204 : I/O Module 04's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E205 : I/O Module 05's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E206 : I/O Module 06's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E207 : I/O Module 07's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E208 : I/O Module 08's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E209 : I/O Module 09's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

- 0x0EA0E20A : I/O Module 10's current user defined zone configuration was not activated since the zone configuration was not created for this chassis.

Explanation: The user-defined zone for the specified I/O module was not activated because the zone configuration does not match what the advanced management module expects for this I/O module.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Activate an appropriate zone configuration for the specified I/O module.

0x0EA0E301 A hard disk drive PFA condition on Storage Module 1 was detected.

Explanation: A Predictive Failure Analysis (PFA) alert has been received for a hard disk drive in the specified storage module.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Log in to the SAS RAID controller either through Storage Configuration Manager* or through the command-line interface (CLI) to determine which hard drive has caused the PFA condition. *Storage Configuration Manager is not supported when configured with 12 disks storage module.

2. At your earliest convenience, replace the hard disk drive.

See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for information about PFA conditions and replacing hard disk drives. The guide is available from the Web.

0x0EA0E401   A hard disk drive PFA condition on Storage Module 2 was detected.

Explanation: A Predictive Failure Analysis (PFA) alert has been received for a hard disk drive in the specified storage module.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:

1. Log in to the SAS RAID controller either through Storage Configuration Manager* or through the command-line interface (CLI) to determine which hard drive has caused the PFA condition. *Storage Configuration Manager is not supported when configured with 12 disks storage module.
2. At your earliest convenience, replace the hard disk drive.

See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for information about PFA conditions and replacing hard disk drives. The guide is available from the Web.

0x0EA0E501   Battery Backup Unit 1 fault condition was detected by I/O Module

Explanation: A fault has occurred in the battery backup unit used to back up the cache for the specified SAS RAID controller module.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:

1. Check the update history for the SAS RAID controller module firmware for any battery related changes.
2. Replace the battery backup unit. See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for more information about replacing a battery backup unit. The guide is available on the Web.

0x0EA0E601   Battery Backup Unit 2 fault condition was detected by I/O Module

Explanation: A fault has occurred in the battery backup unit used to back up the cache for the specified SAS RAID controller module.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:

1. Check the update history for the SAS RAID controller module firmware for any battery related changes.
2. Replace the battery backup unit. See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for more information about replacing a battery backup unit. The guide is available on the Web.

0x0EA0E701   I/O Module 01 requires user attention.

Related messages:
- 0x0EA0E702 : I/O Module 02 requires user attention.
- 0x0EA0E703 : I/O Module 03 requires user attention.
- 0x0EA0E704 : I/O Module 04 requires user attention.
- 0x0EA0E705 : I/O Module 05 requires user attention.
- 0x0EA0E706 : I/O Module 06 requires user attention.
- 0x0EA0E707 : I/O Module 07 requires user attention.
- 0x0EA0E708 : I/O Module 08 requires user attention.
- 0x0EA0E709 : I/O Module 09 requires user attention.
- 0x0EA0E70A : I/O Module 10 requires user attention.

Explanation: The specified SAS RAID controller module has detected a condition that requires user attention.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Information

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:

1. Log in to SAS RAID controller through either Storage Configuration Manager* or through the Command-line interface (CLI) to determine the cause of this event. *Storage Configuration Manager is not supported when configured with 12 disks storage module.
2. See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for more information about resolving the problem. The guide is available on the Web.

0x0EA0E801   Battery Backup Unit 1 is not installed for I/O Module

Explanation: The SAS RAID controller module requires that a battery backup unit (BBU) be installed. A battery backup unit for the specified SAS RAID controller module is not installed.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: If the battery backup unit is not installed, install the battery backup unit. Refer to the IBM BladeCenter SAS RAID Controller Installation and User's Guide for information about installing a battery backup unit.

If the battery backup unit is currently installed, perform these steps:

0x0EA0E901 • 0x0EA0EA01

1. Log in to SAS RAID controller module through either Storage Configuration Manager* or through the command-line interface (CLI) to determine the cause of this event. *Storage Configuration Manager is not supported when configured with 12 disks storage module.
2. See the IBM BladeCenter SAS RAID Controller Module Installation and User's guide for more information regarding this error.

0x0EA0E901 Battery Backup Unit 2 is not installed for I/O Module

Explanation: The SAS RAID controller module requires that a battery backup unit (BBU) be installed. A battery backup unit for the specified SAS RAID controller module is not installed.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: If the battery backup unit is not installed, install the battery backup unit. Refer to the IBM BladeCenter SAS RAID Controller Installation and User's Guide for information about installing a battery backup unit.

If the battery backup unit is currently installed, perform these steps:

1. Log in to SAS RAID controller module through either Storage Configuration Manager* or through the command-line interface (CLI) to determine the cause of this event. *Storage Configuration Manager is not supported when configured with 12 disks storage module.
2. See the IBM BladeCenter SAS RAID Controller Module Installation and User's guide for more information regarding this error.

0x0EA0EA01 Drive-Array configuration error was detected by I/O Module 01.

Related messages:

- 0x0EA0EA02 : Drive-Array configuration error was detected by I/O Module 02.
- 0x0EA0EA03 : Drive-Array configuration error was detected by I/O Module 03.
- 0x0EA0EA04 : Drive-Array configuration error was detected by I/O Module 04.
- 0x0EA0EA05 : Drive-Array configuration error was detected by I/O Module 05.
- 0x0EA0EA06 : Drive-Array configuration error was detected by I/O Module 06.
- 0x0EA0EA07 : Drive-Array configuration error was detected by I/O Module 07.
- 0x0EA0EA08 : Drive-Array configuration error was detected by I/O Module 08.
- 0x0EA0EA09 : Drive-Array configuration error was detected by I/O Module 09.
- 0x0EA0EA0A : Drive-Array configuration error was detected by I/O Module 10.

Explanation: The SAS Controller Module has detected a hard disk drive configuration error during drive array configuration.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response:

1. Log in to SAS RAID controller through either Storage Configuration Manager* or through the Command-line interface (CLI) to determine the cause of this event. *Storage Configuration Manager is not supported when configured with 12 disks storage module.
2. See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for more information about resolving the problem. The guide is available on the Web.

0x0EA0EB01 I/O Modules type mismatch was detected for I/O Modules 01

Related messages:
- 0x0EA0EB02 : I/O Modules type mismatch was detected for I/O Modules 02
- 0x0EA0EB03 : I/O Modules type mismatch was detected for I/O Modules 03
- 0x0EA0EB04 : I/O Modules type mismatch was detected for I/O Modules 04
- 0x0EA0EB05 : I/O Modules type mismatch was detected for I/O Modules 05
- 0x0EA0EB06 : I/O Modules type mismatch was detected for I/O Modules 06
- 0x0EA0EB07 : I/O Modules type mismatch was detected for I/O Modules 07
- 0x0EA0EB08 : I/O Modules type mismatch was detected for I/O Modules 08
- 0x0EA0EB09 : I/O Modules type mismatch was detected for I/O Modules 09
- 0x0EA0EB0A : I/O Modules type mismatch was detected for I/O Modules 10

Explanation: The SAS modules installed in the chassis must be of the same type. You can install SAS RAID control modules or SAS connectivity modules, but you cannot install both types in the same chassis.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Make sure that either SAS RAID controller modules or SAS connectivity modules are installed in the chassis. You cannot install both types of modules in the same chassis.

0x0EA0EC01 I/O Module 01 power off request timed-out.

Related messages:
- 0x0EA0EC02 : I/O Module 02 power off request timed-out.
- 0x0EA0EC03 : I/O Module 03 power off request timed-out.
- 0x0EA0EC04 : I/O Module 04 power off request timed-out.
- 0x0EA0EC05 : I/O Module 05 power off request timed-out.
- 0x0EA0EC06 : I/O Module 06 power off request timed-out.
- 0x0EA0EC07 : I/O Module 07 power off request timed-out.
- 0x0EA0EC08 : I/O Module 08 power off request timed-out.
- 0x0EA0EC09 : I/O Module 09 power off request timed-out.
- 0x0EA0EC0A : I/O Module 10 power off request timed-out.

Explanation: A request to power down the specified SAS RAID controller module timed out.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

0x0EA0ED01 • 0x0EA0EE01

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Attempt to power down the SAS RAID controller module again.
2. Check the Activity LED on the battery backup unit.
   - If it is not lit, reseat the SAS RAID controller module.
   - If it is lit, wait a few minutes to see of the light will turn off.

   Note: Removing the SAS RAID controller module while the LED is lit can result in data loss.

0x0EA0ED01 Unrecognized I/O Module 01 is not allowed to power on.

Related messages:
- 0x0EA0ED02 : Unrecognized I/O Module 02 is not allowed to power on.
- 0x0EA0ED03 : Unrecognized I/O Module 03 is not allowed to power on.
- 0x0EA0ED04 : Unrecognized I/O Module 04 is not allowed to power on.
- 0x0EA0ED05 : Unrecognized I/O Module 05 is not allowed to power on.
- 0x0EA0ED06 : Unrecognized I/O Module 06 is not allowed to power on.
- 0x0EA0ED07 : Unrecognized I/O Module 07 is not allowed to power on.
- 0x0EA0ED08 : Unrecognized I/O Module 08 is not allowed to power on.
- 0x0EA0ED09 : Unrecognized I/O Module 09 is not allowed to power on.
- 0x0EA0ED0A : Unrecognized I/O Module 10 is not allowed to power on.

Explanation: The advanced management module does not recognized the specified I/O module type. Therefore, it cannot be powered on.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Check the event log for other events related to communications errors on the system management bus and resolve those errors.
2. The advanced management module firmware might need to be updated to support the I/O module. Check the IBM BladeCenter software and device drivers Web page to determine if a firmware update is required.
3. The firmware on the I/O module might need to be updated. Check the IBM BladeCenter software and device drivers Web page to determine if a firmware update is required.
4. Reseat the I/O module.

0x0EA0EE01 A management LAN Communication failure has occurred on I/O Module 01

Related messages:
- 0x0EA0EE02 : A management LAN Communication failure has occurred on I/O Module 02
- 0x0EA0EE03 : A management LAN Communication failure has occurred on I/O Module 03
- 0x0EA0EE04 : A management LAN Communication failure has occurred on I/O Module 04
- 0x0EA0EE05 : A management LAN Communication failure has occurred on I/O Module 05
- 0x0EA0EE06 : A management LAN Communication failure has occurred on I/O Module 06
- 0x0EA0EE07 : A management LAN Communication failure has occurred on I/O Module 07

- 0x0EA0EE08 : A management LAN Communication failure has occurred on I/O Module 08
- 0x0EA0EE09 : A management LAN Communication failure has occurred on I/O Module 09
- 0x0EA0EE0A : A management LAN Communication failure has occurred on I/O Module 10

Explanation: A management LAN communication failure has occurred between the advanced management module and the specified I/O module. The advanced management module cannot communicate with the I/O module.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: From the Advanced Configuration page in the advanced management module Web interface, attempt to ping the I/O module. If you can ping the I/O module, perform these steps:

1. Restart the I/O module.
2. Restart the advanced management module.

0x0EA0F001   I/O module 01 NAT table is activated.

Related messages:
- 0x0EA0F002 : I/O module 02 NAT table is activated.
- 0x0EA0F003 : I/O module 03 NAT table is activated.
- 0x0EA0F004 : I/O module 04 NAT table is activated.
- 0x0EA0F005 : I/O module 05 NAT table is activated.
- 0x0EA0F006 : I/O module 06 NAT table is activated.
- 0x0EA0F007 : I/O module 07 NAT table is activated.
- 0x0EA0F008 : I/O module 08 NAT table is activated.
- 0x0EA0F009 : I/O module 09 NAT table is activated.
- 0x0EA0F00A : I/O module 10 NAT table is activated.

Explanation: The Network Address Translation (NAT) table for the specified I/O module has been activated.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0F101   I/O module 01 enabled Protected Mode control of IP configuration.

Related messages:
- 0x0EA0F102 : I/O module 02 enabled Protected Mode control of IP configuration.
- 0x0EA0F103 : I/O module 03 enabled Protected Mode control of IP configuration.
- 0x0EA0F104 : I/O module 04 enabled Protected Mode control of IP configuration.
- 0x0EA0F105 : I/O module 05 enabled Protected Mode control of IP configuration.
- 0x0EA0F106 : I/O module 06 enabled Protected Mode control of IP configuration.
- 0x0EA0F107 : I/O module 07 enabled Protected Mode control of IP configuration.
- 0x0EA0F108 : I/O module 08 enabled Protected Mode control of IP configuration.
- 0x0EA0F109 : I/O module 09 enabled Protected Mode control of IP configuration.

- 0x0EA0F10A : I/O module 10 enabled Protected Mode control of IP configuration.

Explanation: The specified I/O module is in protected mode for IP configuration. IP traffic between the advanced management module and the I/O module is no longer allowed. You cannot access the I/O module through the advanced management module.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0F201 I/O module 01 enabled Protected Mode control of external ports.

Related messages:
- 0x0EA0F202 : I/O module 02 enabled Protected Mode control of external ports.
- 0x0EA0F203 : I/O module 03 enabled Protected Mode control of external ports.
- 0x0EA0F204 : I/O module 04 enabled Protected Mode control of external ports.
- 0x0EA0F205 : I/O module 05 enabled Protected Mode control of external ports.
- 0x0EA0F206 : I/O module 06 enabled Protected Mode control of external ports.
- 0x0EA0F207 : I/O module 07 enabled Protected Mode control of external ports.
- 0x0EA0F208 : I/O module 08 enabled Protected Mode control of external ports.
- 0x0EA0F209 : I/O module 09 enabled Protected Mode control of external ports.
- 0x0EA0F20A : I/O module 10 enabled Protected Mode control of external ports.

Explanation: The specified I/O module is in protected mode for external port control. You can no longer enable or disable the external ports on the I/O module from the advanced management module.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0F301 I/O module 01 enabled Protected Mode control of external management.

Related messages:
- 0x0EA0F302 : I/O module 02 enabled Protected Mode control of external management.
- 0x0EA0F303 : I/O module 03 enabled Protected Mode control of external management.
- 0x0EA0F304 : I/O module 04 enabled Protected Mode control of external management.
- 0x0EA0F305 : I/O module 05 enabled Protected Mode control of external management.
- 0x0EA0F306 : I/O module 06 enabled Protected Mode control of external management.
- 0x0EA0F307 : I/O module 07 enabled Protected Mode control of external management.
- 0x0EA0F308 : I/O module 08 enabled Protected Mode control of external management.
- 0x0EA0F309 : I/O module 09 enabled Protected Mode control of external management.
- 0x0EA0F30A : I/O module 10 enabled Protected Mode control of external management.

Explanation: The specified I/O module is in protected mode for external management control. You can no longer enable or disable the external management for the I/O module through the advanced management module.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0F401   I/O module 01 enabled Protected Mode control of reset configuration to defaults.

Related messages:
- 0x0EA0F402 : I/O module 02 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F403 : I/O module 03 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F404 : I/O module 04 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F405 : I/O module 05 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F406 : I/O module 06 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F407 : I/O module 07 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F408 : I/O module 08 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F409 : I/O module 09 enabled Protected Mode control of reset configuration to defaults.
- 0x0EA0F40A : I/O module 10 enabled Protected Mode control of reset configuration to defaults.

Explanation: The specified I/O module is in protected mode. You can no longer use the advanced management module to restore the I/O module to its default configuration.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0F501   I/O module 01 is in Protected Mode without the MM's permission.

Related messages:
- 0x0EA0F502 : I/O module 02 is in Protected Mode without the MM's permission.
- 0x0EA0F503 : I/O module 03 is in Protected Mode without the MM's permission.
- 0x0EA0F504 : I/O module 04 is in Protected Mode without the MM's permission.
- 0x0EA0F505 : I/O module 05 is in Protected Mode without the MM's permission.
- 0x0EA0F506 : I/O module 06 is in Protected Mode without the MM's permission.
- 0x0EA0F507 : I/O module 07 is in Protected Mode without the MM's permission.
- 0x0EA0F508 : I/O module 08 is in Protected Mode without the MM's permission.
- 0x0EA0F509 : I/O module 09 is in Protected Mode without the MM's permission.
- 0x0EA0F50A : I/O module 10 is in Protected Mode without the MM's permission.

Explanation: The specified I/O module is in protected mode, but the advanced management module did not give permission for the I/O module to be in protected mode.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

0x0EA0F601 • 0x0EA0F701

User response: Perform these steps:

1. If you are not using protected mode, turn off protected mode through the advanced management module interface.

2. If you are using protected mode, access the I/O module through the I/O module interface and correct the protected mode configuration.

0x0EA0F601   I/O module 01 Protected Mode permission and MM configured permission are mismatched.

Related messages:

- 0x0EA0F602 : I/O module 02 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F603 : I/O module 03 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F604 : I/O module 04 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F605 : I/O module 05 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F606 : I/O module 06 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F607 : I/O module 07 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F608 : I/O module 08 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F609 : I/O module 09 Protected Mode permission and MM configured permission are mismatched.
- 0x0EA0F60A : I/O module 10 Protected Mode permission and MM configured permission are mismatched.

Explanation: The Protected Mode permissions set for the specified I/O module do not match the permissions configured through the advanced management module.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Make sure the protected mode setting is the same on both the advanced management module and the I/O module.

0x0EA0F701   I/O module 01 - Open fuse detected. Power redundancy lost for this module.

Related messages:

- 0x0EA0F702 : I/O module 02 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F703 : I/O module 03 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F704 : I/O module 04 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F705 : I/O module 05 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F706 : I/O module 06 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F707 : I/O module 07 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F708 : I/O module 08 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F709 : I/O module 09 - Open fuse detected. Power redundancy lost for this module.
- 0x0EA0F70A : I/O module 10 - Open fuse detected. Power redundancy lost for this module.

Explanation: One of the redundant fuses has been detected in specified I/O module. If you have a full compliment of power modules installed in the chassis, the I/O module will continue to operate. However, the I/O module is now running in non-redundant mode (if the other fuse opens the I/O module will no longer function).

Severity: Error

Alert Category: I/O Modules (Critical) - mmTrapIOC

Log Source: IOMod_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Replace the I/O module at your earliest convenience.

0x0EA0F801 **The active zone configuration number has been set to**

Related messages:
- 0x0EA0F802 : The active zone configuration number has been set to
- 0x0EA0F803 : The active zone configuration number has been set to
- 0x0EA0F804 : The active zone configuration number has been set to
- 0x0EA0F805 : The active zone configuration number has been set to
- 0x0EA0F806 : The active zone configuration number has been set to
- 0x0EA0F807 : The active zone configuration number has been set to
- 0x0EA0F808 : The active zone configuration number has been set to
- 0x0EA0F809 : The active zone configuration number has been set to
- 0x0EA0F80A : The active zone configuration number has been set to

Explanation: The active zone configuration for the SAS I/O module has been set.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0F901 **A communication failure has occurred on the XML TCP command/response port for I/O Module 01.**

Related messages:
- 0x0EA0F902 : A communication failure has occurred on the XML TCP command/response port for I/O Module 02.
- 0x0EA0F903 : A communication failure has occurred on the XML TCP command/response port for I/O Module 03.
- 0x0EA0F904 : A communication failure has occurred on the XML TCP command/response port for I/O Module 04.
- 0x0EA0F905 : A communication failure has occurred on the XML TCP command/response port for I/O Module 05.
- 0x0EA0F906 : A communication failure has occurred on the XML TCP command/response port for I/O Module 06.
- 0x0EA0F907 : A communication failure has occurred on the XML TCP command/response port for I/O Module 07.
- 0x0EA0F908 : A communication failure has occurred on the XML TCP command/response port for I/O Module 08.
- 0x0EA0F909 : A communication failure has occurred on the XML TCP command/response port for I/O Module 09.
- 0x0EA0F90A : A communication failure has occurred on the XML TCP command/response port for I/O Module 10.

Explanation: The advanced management module is unable to communicate with the specified SAS I/O module. The SAS I/O module may be functioning normally, but the advanced management module will not be able to generate any additional events for the SAS I/O module.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

0x0EA0FA01 • 0x0EA0FB01

1. Wait a few minutes to see if a recovery event is generated (especially if the firmware for the SAS I/O module has just been updated).
2. Access the Web interface for the SAS I/O module to verify that it is working. If so, you might be able to wait for a scheduled outage to resolve the problem.
3. Reseat the advanced management module.
4. Reset the SAS I/O module through the advanced management module interface.

   Note: When you reset the SAS I/O module, all connections to that I/O module will be broken, which may result in loss of data. If the I/O module is the SAS RAID controller module, make sure that you stop all host I/O applications before you reset the module.

0x0EA0FA01 User %s is attempting to set the zone configuration number for I/O Module 01.

Related messages:
- 0x0EA0FA02 : User %s is attempting to set the zone configuration number for I/O Module 02.
- 0x0EA0FA03 : User %s is attempting to set the zone configuration number for I/O Module 03.
- 0x0EA0FA04 : User %s is attempting to set the zone configuration number for I/O Module 04.
- 0x0EA0FA05 : User %s is attempting to set the zone configuration number for I/O Module 05.
- 0x0EA0FA06 : User %s is attempting to set the zone configuration number for I/O Module 06.
- 0x0EA0FA07 : User %s is attempting to set the zone configuration number for I/O Module 07.
- 0x0EA0FA08 : User %s is attempting to set the zone configuration number for I/O Module 08.
- 0x0EA0FA09 : User %s is attempting to set the zone configuration number for I/O Module 09.
- 0x0EA0FA0A : User %s is attempting to set the zone configuration number for I/O Module 10.

Explanation: A user is attempting to set the zone configuration for the specified I/O module.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0FB01 Setting of the active zone configuration number failed for I/O Module 01.

Related messages:
- 0x0EA0FB02 : Setting of the active zone configuration number failed for I/O Module 02.
- 0x0EA0FB03 : Setting of the active zone configuration number failed for I/O Module 03.
- 0x0EA0FB04 : Setting of the active zone configuration number failed for I/O Module 04.
- 0x0EA0FB05 : Setting of the active zone configuration number failed for I/O Module 05.
- 0x0EA0FB06 : Setting of the active zone configuration number failed for I/O Module 06.
- 0x0EA0FB07 : Setting of the active zone configuration number failed for I/O Module 07.
- 0x0EA0FB08 : Setting of the active zone configuration number failed for I/O Module 08.
- 0x0EA0FB09 : Setting of the active zone configuration number failed for I/O Module 09.
- 0x0EA0FB0A : Setting of the active zone configuration number failed for I/O Module 10.

Explanation: The advanced management module is unable to set the active zone configuration for the specified SAS I/O module.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Wait a few minutes and attempt to apply the zone configuration again (the SAS I/O module may be busy).
2. Search the event log for other events related to this SAS I/O module and resolve those events.
3. Access the Web interface for the SAS I/O module and resolve any errors that you find.
4. Access the interface for any attached storage devices and resolve any errors that you find.

0x0EA0FC01 All zoning has been disabled for I/O Module 01.

Related messages:
- 0x0EA0FC02 : All zoning has been disabled for I/O Module 02.
- 0x0EA0FC03 : All zoning has been disabled for I/O Module 03.
- 0x0EA0FC04 : All zoning has been disabled for I/O Module 04.
- 0x0EA0FC05 : All zoning has been disabled for I/O Module 05.
- 0x0EA0FC06 : All zoning has been disabled for I/O Module 06.
- 0x0EA0FC07 : All zoning has been disabled for I/O Module 07.
- 0x0EA0FC08 : All zoning has been disabled for I/O Module 08.
- 0x0EA0FC09 : All zoning has been disabled for I/O Module 09.
- 0x0EA0FC0A : All zoning has been disabled for I/O Module 10.

Explanation: All zoning has been disabled for specified SAS I/O Module, either through the Web interface for the SAS I/O module or through Storage Configuration Manager*. *Storage Configuration Manager is not supported when configured with 12 disks storage module.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Apply an active zone to the SAS I/O module (unless the active zone was disabled on purpose).

0x0EA0FD01 I/O module 01 NAT table is activated with IP filter rules.

Related messages:
- 0x0EA0FD02 : I/O module 02 NAT table is activated with IP filter rules.
- 0x0EA0FD03 : I/O module 03 NAT table is activated with IP filter rules.
- 0x0EA0FD04 : I/O module 04 NAT table is activated with IP filter rules.
- 0x0EA0FD05 : I/O module 05 NAT table is activated with IP filter rules.
- 0x0EA0FD06 : I/O module 06 NAT table is activated with IP filter rules.
- 0x0EA0FD07 : I/O module 07 NAT table is activated with IP filter rules.
- 0x0EA0FD08 : I/O module 08 NAT table is activated with IP filter rules.
- 0x0EA0FD09 : I/O module 09 NAT table is activated with IP filter rules.
- 0x0EA0FD0A : I/O module 10 NAT table is activated with IP filter rules.

Explanation: The Network Address Translation (NAT) table for the specified I/O module has been activated with IP filter rules enabled. You must authenticate with the advanced management module before accessing the I/O module.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

0x0EA0FE01 • 0x0EA0FF01

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0FE01 I/O module 01 Stacking Mode enabled.

Related messages:
- 0x0EA0FE02 : I/O module 02 Stacking Mode enabled.
- 0x0EA0FE03 : I/O module 03 Stacking Mode enabled.
- 0x0EA0FE04 : I/O module 04 Stacking Mode enabled.
- 0x0EA0FE05 : I/O module 05 Stacking Mode enabled.
- 0x0EA0FE06 : I/O module 06 Stacking Mode enabled.
- 0x0EA0FE07 : I/O module 07 Stacking Mode enabled.
- 0x0EA0FE08 : I/O module 08 Stacking Mode enabled.
- 0x0EA0FE09 : I/O module 09 Stacking Mode enabled.
- 0x0EA0FE0A : I/O module 10 Stacking Mode enabled.

Explanation: The stacking mode feature has been enabled for the specified I/O module.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA0FF01 I/O Module 01 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.

Related messages:
- 0x0EA0FF02 : I/O Module 02 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF03 : I/O Module 03 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF04 : I/O Module 04 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF05 : I/O Module 05 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF06 : I/O Module 06 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF07 : I/O Module 07 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF08 : I/O Module 08 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF09 : I/O Module 09 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.
- 0x0EA0FF0A : I/O Module 10 has no active zone configuration since neither the AMM nor the I/O Module have an active zone configuration.

Explanation: The SAS I/O module does not have an active zone configuration.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Apply an active zone configuration for the SAS I/O modules.

0x0EA12001   I/O module 01 preserving new IP configuration on all resets

Related messages:
- 0x0EA12002 : I/O module 02 preserving new IP configuration on all resets
- 0x0EA12003 : I/O module 03 preserving new IP configuration on all resets
- 0x0EA12004 : I/O module 04 preserving new IP configuration on all resets
- 0x0EA12005 : I/O module 05 preserving new IP configuration on all resets
- 0x0EA12006 : I/O module 06 preserving new IP configuration on all resets
- 0x0EA12007 : I/O module 07 preserving new IP configuration on all resets
- 0x0EA12008 : I/O module 08 preserving new IP configuration on all resets
- 0x0EA12009 : I/O module 09 preserving new IP configuration on all resets
- 0x0EA1200A : I/O module 10 preserving new IP configuration on all resets

Explanation: The option to preserve the IP configuration on all future resets for the specified I/O module was enabled or disabled.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Example Message:
- I/O module 01 preserving new IP configuration on all resets successfully disabled.
- I/O module 01 preserving new IP configuration on all resets successfully enabled.

User response: Information only; no action is required.

0x0EA14001   I/O module 01 external management over all ports

Related messages:
- 0x0EA14002 : I/O module 02 external management over all ports
- 0x0EA14003 : I/O module 03 external management over all ports
- 0x0EA14004 : I/O module 04 external management over all ports
- 0x0EA14005 : I/O module 05 external management over all ports
- 0x0EA14006 : I/O module 06 external management over all ports
- 0x0EA14007 : I/O module 07 external management over all ports
- 0x0EA14008 : I/O module 08 external management over all ports
- 0x0EA14009 : I/O module 09 external management over all ports
- 0x0EA1400A : I/O module 10 external management over all ports

Explanation: The external management over all ports for the specified I/O module was enabled or disabled.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

0x0EA15001 • 0x0EA16001

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

Example Message:
- I/O module 01 external management over all ports successfully disabled.
- I/O module 01 external management over all ports successfully enabled.

User response: Information only; no action is required.

0x0EA15001 I/O module 01 has incorrect VPD information.

Related messages:
- 0x0EA15002 : I/O module 02 has incorrect VPD information.
- 0x0EA15003 : I/O module 03 has incorrect VPD information.
- 0x0EA15004 : I/O module 04 has incorrect VPD information.
- 0x0EA15005 : I/O module 05 has incorrect VPD information.
- 0x0EA15006 : I/O module 06 has incorrect VPD information.
- 0x0EA15007 : I/O module 07 has incorrect VPD information.
- 0x0EA15008 : I/O module 08 has incorrect VPD information.
- 0x0EA15009 : I/O module 09 has incorrect VPD information.
- 0x0EA1500A : I/O module 10 has incorrect VPD information.

Explanation: IOM has incorrect VPD information.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- I/O module 01 has incorrect VPD information.
- I/O module 01 has incorrect VPD information.

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Contact IBM support to report failure. Reference TDR H204235 to support personnel.

0x0EA16001 I/O module external port was disabled.

Explanation: The external ports for the specified I/O module have been disabled by a user.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA16002   I/O module external port was enabled.

Explanation: The external ports for the specified I/O module have been enabled by a user.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x0EA1A401   I/O module 01 current fault

Related messages:
- 0x0EA1A402 : I/O module 02 current fault
- 0x0EA1A403 : I/O module 03 current fault
- 0x0EA1A404 : I/O module 04 current fault
- 0x0EA1A405 : I/O module 05 current fault
- 0x0EA1A406 : I/O module 06 current fault
- 0x0EA1A407 : I/O module 07 current fault
- 0x0EA1A408 : I/O module 08 current fault
- 0x0EA1A409 : I/O module 09 current fault
- 0x0EA1A40A : I/O module 10 current fault

Explanation: The power current for the specified I/O module has exceeded the current fault threshold. The advanced management module will power off the I/O module to prevent any additional damage.

Severity: Error

Alert Category: I/O Modules (Critical) - mmTrapIOC

Log Source: IOMod_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Restart the I/O module through the advanced management module interface.
2. Reseat the I/O module.
3. Replace the I/O module.

0x0EA1C401   I/O module 01 temperature fault

Related messages:
- 0x0EA1C402 : I/O module 02 temperature fault
- 0x0EA1C403 : I/O module 03 temperature fault
- 0x0EA1C404 : I/O module 04 temperature fault
- 0x0EA1C405 : I/O module 05 temperature fault
- 0x0EA1C406 : I/O module 06 temperature fault
- 0x0EA1C407 : I/O module 07 temperature fault
- 0x0EA1C408 : I/O module 08 temperature fault
- 0x0EA1C409 : I/O module 09 temperature fault

0x0EA1D401

- 0x0EA1C40A : I/O module 10 temperature fault

Explanation: The temperature for the specified I/O module has exceeded the fault threshold.

Severity: Error

Alert Category: I/O Modules (Critical) - mmTrapIOC

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Make sure the fan modules are working properly.
2. Make sure the ambient temperature is within the operating requirements for the chassis.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays.
4. Check to see if there is a firmware update for the advanced management module that is related to over temperature conditions. If so, update the firmware for the advanced management module.
5. Update the firmware for the I/O module.
6. Replace the I/O module.

0x0EA1D401 I/O module 01 over recommended temperature

Related messages:
- 0x0EA1D402 : I/O module 02 over recommended temperature
- 0x0EA1D403 : I/O module 03 over recommended temperature
- 0x0EA1D404 : I/O module 04 over recommended temperature
- 0x0EA1D405 : I/O module 05 over recommended temperature
- 0x0EA1D406 : I/O module 06 over recommended temperature
- 0x0EA1D407 : I/O module 07 over recommended temperature
- 0x0EA1D408 : I/O module 08 over recommended temperature
- 0x0EA1D409 : I/O module 09 over recommended temperature
- 0x0EA1D40A : I/O module 10 over recommended temperature

Explanation: The temperature for the specified I/O module exceeds the recommended temperature.

Severity: Warning

Alert Category: I/O Modules (Warning) - mmTrapION

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the room temperature to ensure that it is within the operating specifications for the chassis.
2. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
4. Make sure that there is nothing covering the chassis (that will obstruct airflow through the chassis).

0x0EC00001   BEM 01 fault

Explanation: A fault has occurred in either the BladeCenter Storage Expansion (BSE) Unit or the Peripheral Component Interconnect(PCI) Expansion Unit.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: From the advanced management module Web interface, view the hardware VPD page to determine if a BladeCenter Storage Expansion Unit or a Peripheral Component Interconnect (PCI) Expansion Unit is installed.
- If a BladeCenter Storage Expansion Unit is installed, perform these steps:
  1. Update the blade server service processor firmware, the blade server BIOS, and ServeRAID firmware, drivers, and manager, if applicable.
  2. Reseat these components:
     a. ServeRAID SAS controller
     b. RAID battery
     c. BladeCenter Storage Expansion Unit
  3. Replace the BladeCenter Storage Expansion Unit.
- If a Peripheral Component Interconnect (PCI) Expansion Unit is installed, perform these steps:
  1. Verify that the PCI adapters are supported in the expansion unit as listed on the IBM ServerProven Web site.
  2. Reseat the PCI adapters and the PCI expansion unit. Test one at a time of two are installed.
  3. Replace the PCI expansion unit.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about the BladeCenter Storage Expansion Unit and the Peripheral Component Interconnect (PCI) Expansion Unit. The Problem Determination and Service Guide is available on the Web.

0x0EC00002   BEM 02 fault

Explanation: A fault has occurred in the Peripheral Component Interconnect (PCI) Expansion Unit.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Verify that the PCI adapters are supported in the expansion unit, as listed on the IBM ServerProven Web site.
2. Reseat the PCI adapters and the PCI expansion unit. Test one at a time if two are installed.
3. Replace the PCI expansion unit.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about the Peripheral Component Interconnect (PCI) Expansion Unit. The Problem Determination and Service Guide is available on the Web.

0x0EE00000   BSE RAID fault

Explanation: A RAID fault has occurred in the BladeCenter Storage Expansion Unit in the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Update the ServeRAID-related code (including driver, BIOS and service processor firmware, and the ServeRAID application) for the blade server.
2. Update the hard drive firmware.
3. Reseat the ServeRAID SAS controller in the BladeCenter Storage Expansion Unit.
4. Replace the following components one at a time, in the order shown, restarting the blade server each time:
   a. ServeRAID SAS controller.
   b. BladeCenter Storage Expansion Unit.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about the BladeCenter Storage Expansion Unit. The Problem Determination and Service Guide is available on the Web.

0x0EE18000   BSE RAID battery failure

Explanation: The battery for the BladeCenter Storage Expansion Unit has failed.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Make sure the battery is connected.
2. Update the service processor firmware, the BIOS, and the ServeRAID application for the blade server.
3. Replace the battery.

Refer to the Problem Determination and Service Guide for the specified blade server type for information about reseating and replacing the battery.

0x0F00A001   AMM failed to set the Open Fabric Manager configuration for blade 01. Blade power permissions denied.

Related messages:
- 0x0F00A002 : AMM failed to set the Open Fabric Manager configuration for blade 02. Blade power permissions denied.
- 0x0F00A003 : AMM failed to set the Open Fabric Manager configuration for blade 03. Blade power permissions denied.
- 0x0F00A004 : AMM failed to set the Open Fabric Manager configuration for blade 04. Blade power permissions denied.
- 0x0F00A005 : AMM failed to set the Open Fabric Manager configuration for blade 05. Blade power permissions denied.

- 0x0F00A006 : AMM failed to set the Open Fabric Manager configuration for blade 06. Blade power permissions denied.
- 0x0F00A007 : AMM failed to set the Open Fabric Manager configuration for blade 07. Blade power permissions denied.
- 0x0F00A008 : AMM failed to set the Open Fabric Manager configuration for blade 08. Blade power permissions denied.
- 0x0F00A009 : AMM failed to set the Open Fabric Manager configuration for blade 09. Blade power permissions denied.
- 0x0F00A00A : AMM failed to set the Open Fabric Manager configuration for blade 10. Blade power permissions denied.
- 0x0F00A00B : AMM failed to set the Open Fabric Manager configuration for blade 11. Blade power permissions denied.
- 0x0F00A00C : AMM failed to set the Open Fabric Manager configuration for blade 12. Blade power permissions denied.
- 0x0F00A00D : AMM failed to set the Open Fabric Manager configuration for blade 13. Blade power permissions denied.
- 0x0F00A00E : AMM failed to set the Open Fabric Manager configuration for blade 14. Blade power permissions denied.

Explanation: The advanced management module cannot set the Open Fabric Manager configuration for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Power off the blade server, and then power it on again.
2. Reseat the blade server.
3. Update the firmware for the service processor on the blade server. You can find firmware on the IBM BladeCenter software and device drivers Web page.

0x0F00B001   Unable to apply Open Fabric Manager configuration to one or more devices at blade 01

Related messages:
- 0x0F00B002 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 02
- 0x0F00B003 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 03
- 0x0F00B004 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 04
- 0x0F00B005 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 05
- 0x0F00B006 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 06
- 0x0F00B007 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 07
- 0x0F00B008 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 08
- 0x0F00B009 : Unable to apply Open Fabric Manager configuration to one or more devices at blade 09
- 0x0F00B00A : Unable to apply Open Fabric Manager configuration to one or more devices at blade 10
- 0x0F00B00B : Unable to apply Open Fabric Manager configuration to one or more devices at blade 11
- 0x0F00B00C : Unable to apply Open Fabric Manager configuration to one or more devices at blade 12
- 0x0F00B00D : Unable to apply Open Fabric Manager configuration to one or more devices at blade 13
- 0x0F00B00E : Unable to apply Open Fabric Manager configuration to one or more devices at blade 14

0x0F00C001

Explanation: The Open Fabric Manager configuration cannot be applied to the specific blade server because the firmware does not support Open Fabric Manager.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform this steps:

1. From the advanced management module Web interface, go to the Open Fabric Manager page to determine which action is failing.
2. See the IBM BladeCenter Open Fabric Manager Installation and User's Guide to verify that the specified blade server type and the expansion card options within the blade server support Open Fabric Manager. The guide is available on the Web.
3. Upgrade the firmware for the blade server and all expansion card options. See the IBM BladeCenter Open Fabric Manager Installation and User's Guide for more information. The guide is available on the Web.

0x0F00C001   Blade 01 not allowed to power on; constrained by power budget.

Related messages:
- 0x0F00C002 : Blade 02 not allowed to power on; constrained by power budget.
- 0x0F00C003 : Blade 03 not allowed to power on; constrained by power budget.
- 0x0F00C004 : Blade 04 not allowed to power on; constrained by power budget.
- 0x0F00C005 : Blade 05 not allowed to power on; constrained by power budget.
- 0x0F00C006 : Blade 06 not allowed to power on; constrained by power budget.
- 0x0F00C007 : Blade 07 not allowed to power on; constrained by power budget.
- 0x0F00C008 : Blade 08 not allowed to power on; constrained by power budget.
- 0x0F00C009 : Blade 09 not allowed to power on; constrained by power budget.
- 0x0F00C00A : Blade 10 not allowed to power on; constrained by power budget.
- 0x0F00C00B : Blade 11 not allowed to power on; constrained by power budget.
- 0x0F00C00C : Blade 12 not allowed to power on; constrained by power budget.
- 0x0F00C00D : Blade 13 not allowed to power on; constrained by power budget.
- 0x0F00C00E : Blade 14 not allowed to power on; constrained by power budget.

Explanation: While the specified blade server is being powered on, the management module has detected that there is no longer enough power capacity in the power budget to allow the blade server to continue powering on.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Select a different power management policy to increase the power budget.
2. Add additional power modules to increase power capacity.
3. Shut down other devices in the chassis.

0x0F00D001   FW/BIOS for blade 01 does not support Open Fabric Manager

Related messages:

- 0x0F00D002 : FW/BIOS for blade 02 does not support Open Fabric Manager
- 0x0F00D003 : FW/BIOS for blade 03 does not support Open Fabric Manager
- 0x0F00D004 : FW/BIOS for blade 04 does not support Open Fabric Manager
- 0x0F00D005 : FW/BIOS for blade 05 does not support Open Fabric Manager
- 0x0F00D006 : FW/BIOS for blade 06 does not support Open Fabric Manager
- 0x0F00D007 : FW/BIOS for blade 07 does not support Open Fabric Manager
- 0x0F00D008 : FW/BIOS for blade 08 does not support Open Fabric Manager
- 0x0F00D009 : FW/BIOS for blade 09 does not support Open Fabric Manager
- 0x0F00D00A : FW/BIOS for blade 10 does not support Open Fabric Manager
- 0x0F00D00B : FW/BIOS for blade 11 does not support Open Fabric Manager
- 0x0F00D00C : FW/BIOS for blade 12 does not support Open Fabric Manager
- 0x0F00D00D : FW/BIOS for blade 13 does not support Open Fabric Manager
- 0x0F00D00E : FW/BIOS for blade 14 does not support Open Fabric Manager

Explanation: The BIOS firmware on the specified blade server does not support Open Fabric Manager

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT):   Minor

User response: Upgrade the BIOS firmware for the specified blade server. See the BladeCenter Open Fabric Manager Installation and User's Guide for more information. The guide is available on the Web.

0x0F00E001   A device on blade 01 does not support Open Fabric Manager

Related messages:

- 0x0F00E002 : A device on blade 02 does not support Open Fabric Manager
- 0x0F00E003 : A device on blade 03 does not support Open Fabric Manager
- 0x0F00E004 : A device on blade 04 does not support Open Fabric Manager
- 0x0F00E005 : A device on blade 05 does not support Open Fabric Manager
- 0x0F00E006 : A device on blade 06 does not support Open Fabric Manager
- 0x0F00E007 : A device on blade 07 does not support Open Fabric Manager
- 0x0F00E008 : A device on blade 08 does not support Open Fabric Manager
- 0x0F00E009 : A device on blade 09 does not support Open Fabric Manager
- 0x0F00E00A : A device on blade 10 does not support Open Fabric Manager
- 0x0F00E00B : A device on blade 11 does not support Open Fabric Manager
- 0x0F00E00C : A device on blade 12 does not support Open Fabric Manager
- 0x0F00E00D : A device on blade 13 does not support Open Fabric Manager
- 0x0F00E00E : A device on blade 14 does not support Open Fabric Manager

Explanation: A expansion card option on the specified blade server does not support Open Fabric Manager.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

0x0F00F001 • 0x0F010001

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: See the BladeCenter Installation and User's Guide to determine which expansion card options support Open Fabric Manager. If the expansion card option is supported, update the firmware for the expansion card option.

The Installation and User's Guide is available on the Web.

0x0F00F001   Communication problems between an Open Fabric Manager device and a storage target at blade 01

Related messages:
- 0x0F00F002 : Communication problems between an Open Fabric Manager device and a storage target at blade 02
- 0x0F00F003 : Communication problems between an Open Fabric Manager device and a storage target at blade 03
- 0x0F00F004 : Communication problems between an Open Fabric Manager device and a storage target at blade 04
- 0x0F00F005 : Communication problems between an Open Fabric Manager device and a storage target at blade 05
- 0x0F00F006 : Communication problems between an Open Fabric Manager device and a storage target at blade 06
- 0x0F00F007 : Communication problems between an Open Fabric Manager device and a storage target at blade 07
- 0x0F00F008 : Communication problems between an Open Fabric Manager device and a storage target at blade 08
- 0x0F00F009 : Communication problems between an Open Fabric Manager device and a storage target at blade 09
- 0x0F00F00A : Communication problems between an Open Fabric Manager device and a storage target at blade 10
- 0x0F00F00B : Communication problems between an Open Fabric Manager device and a storage target at blade 11
- 0x0F00F00C : Communication problems between an Open Fabric Manager device and a storage target at blade 12
- 0x0F00F00D : Communication problems between an Open Fabric Manager device and a storage target at blade 13
- 0x0F00F00E : Communication problems between an Open Fabric Manager device and a storage target at blade 14

Explanation: After applying Open Fabric Manager settings on the blade server, the blade server cannot access the target storage device.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the zoning configuration for the blade server and target storage device.
2. Verify the path from the blade server to the target storage device.
3. Update any configuration settings, if needed, and apply Open Fabric Manager again.

0x0F010001   Open Fabric Manager converted configuration for bay 01

Related messages:
- 0x0F010002 : Open Fabric Manager converted configuration for bay 02
- 0x0F010003 : Open Fabric Manager converted configuration for bay 03
- 0x0F010004 : Open Fabric Manager converted configuration for bay 04
- 0x0F010005 : Open Fabric Manager converted configuration for bay 05
- 0x0F010006 : Open Fabric Manager converted configuration for bay 06
- 0x0F010007 : Open Fabric Manager converted configuration for bay 07
- 0x0F010008 : Open Fabric Manager converted configuration for bay 08
- 0x0F010009 : Open Fabric Manager converted configuration for bay 09
- 0x0F01000A : Open Fabric Manager converted configuration for bay 10

- 0x0F01000B : Open Fabric Manager converted configuration for bay 11
- 0x0F01000C : Open Fabric Manager converted configuration for bay 12
- 0x0F01000D : Open Fabric Manager converted configuration for bay 13
- 0x0F01000E : Open Fabric Manager converted configuration for bay 14

Explanation: Open Fabric Manager protocol supports 2 versions. Version 1 is the original version. Version 2 added virtual ethernet support for cards that support vNic. The blade noted in message supports only version 1, so the Open Fabric Manager configuration was downgraded from version 2 to version 1 which removes virtual ethernet configuration data, 4 boot target support, and use of offset 2 and offset 3.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Information only; no action is required.

0x0F010101   Blade 01 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.

Related messages:
- 0x0F010102 : Blade 02 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F010103 : Blade 03 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F010104 : Blade 04 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F010105 : Blade 05 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F010106 : Blade 06 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F010107 : Blade 07 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F010108 : Blade 08 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F010109 : Blade 09 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F01010A : Blade 10 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F01010B : Blade 11 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F01010C : Blade 12 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F01010D : Blade 13 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.
- 0x0F01010E : Blade 14 firmware unable to support Open Fabric Manager version 2. Blade configuration downgraded to OFM version 1.

Explanation: The specified blade server IMM and UEFI firmware are unable to support Open Fabric Manager version 2. The advanced management module has downgraded the configuration of this blade server to Open Fabric Manager version 1.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

0x10016000 • 0x1C000003

Automatically notify service: No

Recoverable: Yes

User response: Update the specified blade server to the latest IMM and UEFI levels to restore Open Fabric Manager version 2 capability.

0x10016000   No sensor information or invalid sensor repository.

Explanation: The sensor data records for the specified blade server have been updated.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Information only; no action is required. MM will load the new sensor data records.

0x1C000001   Blade powered off

Explanation: The specified blade server has powered off.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x1C000002   Blade powered on

Explanation: The specified blade server has powered on.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x1C000003   Blade in standby power state

Explanation: The specified blade server is in standby power state.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x1C000004   Blade in hibernate power state

Explanation: The specified blade server is in hibernate power state.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x1E00D001   Open Fabric Manager configuration for bay 01 was changed

Related messages:
- 0x1E00D002 : Open Fabric Manager configuration for bay 02 was changed
- 0x1E00D003 : Open Fabric Manager configuration for bay 03 was changed
- 0x1E00D004 : Open Fabric Manager configuration for bay 04 was changed
- 0x1E00D005 : Open Fabric Manager configuration for bay 05 was changed
- 0x1E00D006 : Open Fabric Manager configuration for bay 06 was changed
- 0x1E00D007 : Open Fabric Manager configuration for bay 07 was changed
- 0x1E00D008 : Open Fabric Manager configuration for bay 08 was changed
- 0x1E00D009 : Open Fabric Manager configuration for bay 09 was changed
- 0x1E00D00A : Open Fabric Manager configuration for bay 10 was changed
- 0x1E00D00B : Open Fabric Manager configuration for bay 11 was changed
- 0x1E00D00C : Open Fabric Manager configuration for bay 12 was changed
- 0x1E00D00D : Open Fabric Manager configuration for bay 13 was changed
- 0x1E00D00E : Open Fabric Manager configuration for bay 14 was changed

Explanation: The Open Fabric Manager configuration for the specified blade server was changed.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x1E00E001   Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 01. Expected configuration will take affect when blade restarted.

Related messages:
- 0x1E00E002 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 02. Expected configuration will take affect when blade restarted.
- 0x1E00E003 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 03. Expected configuration will take affect when blade restarted.
- 0x1E00E004 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 04. Expected configuration will take affect when blade restarted.
- 0x1E00E005 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 05. Expected configuration will take affect when blade restarted.
- 0x1E00E006 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 06. Expected configuration will take affect when blade restarted.

0x1E00F001

- 0x1E00E007 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 07. Expected configuration will take affect when blade restarted.
- 0x1E00E008 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 08. Expected configuration will take affect when blade restarted.
- 0x1E00E009 : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 09. Expected configuration will take affect when blade restarted.
- 0x1E00E00A : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 10. Expected configuration will take affect when blade restarted.
- 0x1E00E00B : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 11. Expected configuration will take affect when blade restarted.
- 0x1E00E00C : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 12. Expected configuration will take affect when blade restarted.
- 0x1E00E00D : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 13. Expected configuration will take affect when blade restarted.
- 0x1E00E00E : Open Fabric Manager configuration mismatch detected between expected configuration and the actual configuration for blade 14. Expected configuration will take affect when blade restarted.

Explanation: The Open Fabric Manager configuration detected by the advanced management module does not match the action Open Fabric Manager configuration for the specified blade server. The active configuration from the specified blade server will be used.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Power off the specified blade server.
2. Attempt to apply the Open Fabric Manager configuration again.

See the BladeCenter Open Fabric Manager Installation and User's Guide for more information. The guide is available on the Web.

0x1E00F001   Blade 01 system management processor does not support Open Fabric Manager

Related messages:
- 0x1E00F002 : Blade 02 system management processor does not support Open Fabric Manager
- 0x1E00F003 : Blade 03 system management processor does not support Open Fabric Manager
- 0x1E00F004 : Blade 04 system management processor does not support Open Fabric Manager
- 0x1E00F005 : Blade 05 system management processor does not support Open Fabric Manager
- 0x1E00F006 : Blade 06 system management processor does not support Open Fabric Manager
- 0x1E00F007 : Blade 07 system management processor does not support Open Fabric Manager
- 0x1E00F008 : Blade 08 system management processor does not support Open Fabric Manager
- 0x1E00F009 : Blade 09 system management processor does not support Open Fabric Manager
- 0x1E00F00A : Blade 10 system management processor does not support Open Fabric Manager
- 0x1E00F00B : Blade 11 system management processor does not support Open Fabric Manager
- 0x1E00F00C : Blade 12 system management processor does not support Open Fabric Manager
- 0x1E00F00D : Blade 13 system management processor does not support Open Fabric Manager
- 0x1E00F00E : Blade 14 system management processor does not support Open Fabric Manager

Explanation: The service processor on the specified blade server does not support Open Fabric Manager.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Verify that the blade server supports Open Fabric Manager. If so, update the firmware for the service processor on the blade server. See the BladeCenter Open Fabric Manager Installation and User's Guide for more information about supported blade servers and updating firmware.

0x1E00F00F **Open Fabric Manager configuration was cleared, because the AMM was moved to a new chassis or restored to default**

Explanation: The Open Fabric Manager configuration was cleared because the advanced management module was moved to another chassis or restored to the default settings.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Apply the Open Fabric configuration again.

0x1E010012 **The 'Save Configuration to Chassis' operation was unable to save all the data to the chassis.**

Explanation: The advanced management module is unable to save all configuration data to the chassis.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Save the configuration data to a file. See the Advanced Management Module User's Guide or the Advanced Management Module Command-Line Interface Reference Guide for more information about saving configuration data. These documents are available from the Web.

0x40000010 **DNS is enabled**

Explanation: Domain Name System (DNS) has been enabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40000011   DNS is disabled

Explanation: Domain Name System (DNS) has been disabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40000012   DNS server priority setting is configured as

Explanation: The Domain Name System (DNS) IPv4 and IPv6 priority configuration has been changed on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40000013   DNS server IP

Explanation: The Domain Name System (DNS) IPv4 and IPv6 server address configuration has been changed on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40000014   Dynamic DNS is enabled

Explanation: Dynamic Domain Name System (DNS) has been enabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40000015   Dynamic DNS is disabled

Explanation: Dynamic Domain Name System (DNS) has been disabled on the advanced management module by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40000016   %s AMM domain name has been changed %s

Explanation: The valueadvanced management module domain name has been changed by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Primary AMM domain name has been changed from 'domainname.net' to 'domain.net' by user 'USERID' from '10.12.200.35 (Web)'

User response: Information only; no action required.

0x40000020   initiated hard reset of service processor on blade

Explanation: The specified user reset the service processor on the specified blade server. The Blade Service Management Processor (BSMP) has been hard reset by the specified user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: 'USERID' initiated hard reset of service processor on blade 1

User response: Information only; no action is required.

0x40000022   User

Explanation: The specified user performed a power operation on the specified blade server.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: User 'USERID' powered on BLADE 11

User response: Information only; no action is required.

0x40000030   Remote Presence port number

Explanation: The remote presence port number has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Remote presence port number successfully disabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.
- Remote presence port number successfully enabled by 'USERID' from '192.168.0.1 (TCP Cmd)'.

User response: Information only; no action is required.

0x40001001   License added

Explanation: An advanced management module license was added to the system that allows access to the specified feature.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: License added for <feature name> by <username> at <ip address> (<access protocol>)
- License added for Open Fabric Manager by USERID at 10.11.20.66 (Web)

User response: Information only; no action is required.

0x40001002   License removed

Explanation: An advanced management module license was removed from the system. Access to the specified feature is no longer allowed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40001003   License serial number modified

Explanation: The chassis serial number for an advanced management module license has been modified.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40001004   License Machine Type/Model number modified

Explanation: The Machine Type/Model for an advanced management module license has been modified.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40001005   License

Related messages:
- 0x40001007 : License
- 0x40001008 : License
- 0x4000100A : License

Explanation: The license for the specified feature has expired.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: To continue using the specified feature, upgrade the license to a full version from the IBM Website.

0x40001006   Transitional license has been issued.

Explanation: The Basic Open Fabric Manager license transitional period has timed out.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Transitional license is in use. Please upgrade IBM BladeCenter Open Fabric Manager to a full license.

User response: Information only. You can register to upgrade to a full license from the IBM Website.

0x40001009   Your trial license for

Explanation: Your trial period for the specified license is about to end.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only. You can register to upgrade to a full license from the IBM website.

0x40001020   IPSEC IKEv2 enabled

Explanation: The IPSEC IKEv2 service has been enabled by a user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC IKEv2 enabled by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40001021   IPSEC IKEv2 disabled

Explanation: The IPSEC IKEv2 service has been disabled by a user. All security policy database (SPD) entries and security association database (SA) entries are permanently removed.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC IKEv2 disabled by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40001022   IPSEC secure port modified

Explanation: The port number of the IPSEC secure port has been changed by a user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC secure port modified by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40001023   IPSEC secure protocol modified

Explanation: The IPSEC secure protocol value has been changed by a user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC secure protocol modified by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40001024   IPSEC esp algorithms modified

Explanation: The IPSEC esp algorithms have been modified by a user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC esp algorithms modified by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40001025   IPSEC IKEv2 algorithms modified

Explanation: The IPSEC IKEv2 algorithms have been modified by a user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC IKEv2 algorithms modified by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40001026   IPSEC pre-shared key modified

Explanation: The IPSEC pre-shared key has been modified by a user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC pre-shared key modified by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40001027   IPSEC configuration reset to defaults

Explanation: A user has reset the IPSEC configuration to default values. IKEv2 is disabled.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: IPSEC configuration reset to defaults by USERID at 192.168.10.10 (SSH)

User response: Information only; no action is required.

0x40015070   The Build ID List was modified successfully

Explanation: The Firmware Build ID List from Blade Firmware Level Management User Interface has been changed by the specified user account.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40015080   The Build ID List was imported successfully

Explanation: The Firmware Build ID List from Blade Firmware Level Management User Interface was imported successfully by the specified user account.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40015090   SMTP Email Domain modified

Explanation: The Simple Mail Transfer Protocol (SMTP) Email Domain configuration has been changed by a user.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: SMTP Email Domain successfully changed to 'xyz.net' by 'USERID' from '192.168.0.1 (Web)'

User response: Information only; no action is required.

0x4001711E   Standby MM failed to synchronize with primary MM. Standby network interface is disabled.

Explanation: The standby advanced management module failed to synchronize with the primary advanced management module. Therefore, the network interface for the standby advanced management module is disabled. This log entry can be seen only after a failover has occurred and the standby advanced management module becomes the primary.

Severity: Warning

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT):   Minor

User response: Perform these steps:

1. If the firmware configuration has not changed recently, reseat the standby advanced management module. Otherwise, reseat the primary advanced management module.
2. Check the IBM Support Web page for any service bulletins that might be related to this problem.
3. Restore system defaults to factory settings. Then attempt to apply the configuration again.

0x40110001   Management Module IP address configuration changed.

Explanation: The IP address configuration for the advanced management module has been changed by the specified user account.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40110002   %s AMM IPv6 static configuration: %s

Explanation: The specified IPv6 static configuration for the advanced management module external network interface has been applied.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Primary AMM IPv6 static configuration: IP=2001::1234, Prefix=64, Gateway=2001::3456.

User response: Information only; no action is required.

0x40217006   Logical uplink failover IPv4 address setting

Explanation: The setting "Failover IPv4 address for logical link loss" has been changed by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Logical uplink failover IPv4 address changed by 'USERID' from '192.168.0.1 (Web)

User response: Information only; no action is required.

0x40217007   Logical uplink failover IPv6 address setting

Explanation: The setting "Failover IPv6 address for logical link loss" has been changed by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

0x40217008 • 0x40324101

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Logical uplink failover IPv6 address changed by 'USERID' from '192.168.0.1 (Web)

User response: Information only; no action is required.

0x40217008   Logical uplink failover policy setting

Explanation: The setting "Failover policy for logical link loss" has been changed by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Logical uplink failover policy changed by 'USERID' from '192.168.0.1 (Web)

User response: Information only; no action is required.

0x40324001   IPv6 was enabled for IOM 01 by user %s from %s

Related messages:
- 0x40324002 : IPv6 was enabled for IOM 02 by user %s from %s
- 0x40324003 : IPv6 was enabled for IOM 03 by user %s from %s
- 0x40324004 : IPv6 was enabled for IOM 04 by user %s from %s
- 0x40324005 : IPv6 was enabled for IOM 05 by user %s from %s
- 0x40324006 : IPv6 was enabled for IOM 06 by user %s from %s
- 0x40324007 : IPv6 was enabled for IOM 07 by user %s from %s
- 0x40324008 : IPv6 was enabled for IOM 08 by user %s from %s
- 0x40324009 : IPv6 was enabled for IOM 09 by user %s from %s
- 0x4032400A : IPv6 was enabled for IOM 10 by user %s from %s

Explanation: The specified user account requested that IPv6 be enabled for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 is enabled for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324101   IPv6 was disabled for IOM 01 by user %s from %s

Related messages:
- 0x40324102 : IPv6 was disabled for IOM 02 by user %s from %s
- 0x40324103 : IPv6 was disabled for IOM 03 by user %s from %s

- 0x40324104 : IPv6 was disabled for IOM 04 by user %s from %s
- 0x40324105 : IPv6 was disabled for IOM 05 by user %s from %s
- 0x40324106 : IPv6 was disabled for IOM 06 by user %s from %s
- 0x40324107 : IPv6 was disabled for IOM 07 by user %s from %s
- 0x40324108 : IPv6 was disabled for IOM 08 by user %s from %s
- 0x40324109 : IPv6 was disabled for IOM 09 by user %s from %s
- 0x4032410A : IPv6 was disabled for IOM 10 by user %s from %s

Explanation: The specified user account requested that IPv6 be disabled for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 is disabled for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324201   IPv6 static configuration was %s for IOM 01 by user %s from %s

Related messages:
- 0x40324202 : IPv6 static configuration was %s for IOM 02 by user %s from %s
- 0x40324203 : IPv6 static configuration was %s for IOM 03 by user %s from %s
- 0x40324204 : IPv6 static configuration was %s for IOM 04 by user %s from %s
- 0x40324205 : IPv6 static configuration was %s for IOM 05 by user %s from %s
- 0x40324206 : IPv6 static configuration was %s for IOM 06 by user %s from %s
- 0x40324207 : IPv6 static configuration was %s for IOM 07 by user %s from %s
- 0x40324208 : IPv6 static configuration was %s for IOM 08 by user %s from %s
- 0x40324209 : IPv6 static configuration was %s for IOM 09 by user %s from %s
- 0x4032420A : IPv6 static configuration was %s for IOM 10 by user %s from %s

Explanation: The specified user account requested that IPv6 static configuration be enabled or disabled for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 static configuration is enabled for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324301   IPv6 DHCP configuration was %s for IOM 01 by user %s from %s

Related messages:
- 0x40324302 : IPv6 DHCP configuration was %s for IOM 02 by user %s from %s
- 0x40324303 : IPv6 DHCP configuration was %s for IOM 03 by user %s from %s
- 0x40324304 : IPv6 DHCP configuration was %s for IOM 04 by user %s from %s

- 0x40324305 : IPv6 DHCP configuration was %s for IOM 05 by user %s from %s
- 0x40324306 : IPv6 DHCP configuration was %s for IOM 06 by user %s from %s
- 0x40324307 : IPv6 DHCP configuration was %s for IOM 07 by user %s from %s
- 0x40324308 : IPv6 DHCP configuration was %s for IOM 08 by user %s from %s
- 0x40324309 : IPv6 DHCP configuration was %s for IOM 09 by user %s from %s
- 0x4032430A : IPv6 DHCP configuration was %s for IOM 10 by user %s from %s

Explanation: The specified user account requested that IPv6 DHCP configuration be enabled or disabled for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 dhcp configuration is disabled for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324401   IPv6 stateless auto-configuration was %s for IOM 01 by user %s from %s

Related messages:
- 0x40324402 : IPv6 stateless auto-configuration was %s for IOM 02 by user %s from %s
- 0x40324403 : IPv6 stateless auto-configuration was %s for IOM 03 by user %s from %s
- 0x40324404 : IPv6 stateless auto-configuration was %s for IOM 04 by user %s from %s
- 0x40324405 : IPv6 stateless auto-configuration was %s for IOM 05 by user %s from %s
- 0x40324406 : IPv6 stateless auto-configuration was %s for IOM 06 by user %s from %s
- 0x40324407 : IPv6 stateless auto-configuration was %s for IOM 07 by user %s from %s
- 0x40324408 : IPv6 stateless auto-configuration was %s for IOM 08 by user %s from %s
- 0x40324409 : IPv6 stateless auto-configuration was %s for IOM 09 by user %s from %s
- 0x4032440A : IPv6 stateless auto-configuration was %s for IOM 10 by user %s from %s

Explanation: The specified user account requested that IPv6 stateless automatic configuration be enabled or disabled for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 stateless auto-configuration is disabled for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324501   IPv6 static address was changed to %s for IOM 01 by user %s from %s

Related messages:
- 0x40324502 : IPv6 static address was changed to %s for IOM 02 by user %s from %s
- 0x40324503 : IPv6 static address was changed to %s for IOM 03 by user %s from %s
- 0x40324504 : IPv6 static address was changed to %s for IOM 04 by user %s from %s
- 0x40324505 : IPv6 static address was changed to %s for IOM 05 by user %s from %s

- 0x40324506 : IPv6 static address was changed to %s for IOM 06 by user %s from %s
- 0x40324507 : IPv6 static address was changed to %s for IOM 07 by user %s from %s
- 0x40324508 : IPv6 static address was changed to %s for IOM 08 by user %s from %s
- 0x40324509 : IPv6 static address was changed to %s for IOM 09 by user %s from %s
- 0x4032450A : IPv6 static address was changed to %s for IOM 10 by user %s from %s

Explanation: The specified user account changed the IPv6 static address for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 static address is changed to 2000::1 for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324601   IPv6 gateway address was changed to %s for IOM 01 by user %s from %s

Related messages:
- 0x40324602 : IPv6 gateway address was changed to %s for IOM 02 by user %s from %s
- 0x40324603 : IPv6 gateway address was changed to %s for IOM 03 by user %s from %s
- 0x40324604 : IPv6 gateway address was changed to %s for IOM 04 by user %s from %s
- 0x40324605 : IPv6 gateway address was changed to %s for IOM 05 by user %s from %s
- 0x40324606 : IPv6 gateway address was changed to %s for IOM 06 by user %s from %s
- 0x40324607 : IPv6 gateway address was changed to %s for IOM 07 by user %s from %s
- 0x40324608 : IPv6 gateway address was changed to %s for IOM 08 by user %s from %s
- 0x40324609 : IPv6 gateway address was changed to %s for IOM 09 by user %s from %s
- 0x4032460A : IPv6 gateway address was changed to %s for IOM 10 by user %s from %s

Explanation: The specified user account changed the IPv6 gateway address for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 gateway address is changed to 2000::1 for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324701   IPv6 prefix length was changed to %s for IOM 01 by user %s from %s

Related messages:
- 0x40324702 : IPv6 prefix length was changed to %s for IOM 02 by user %s from %s
- 0x40324703 : IPv6 prefix length was changed to %s for IOM 03 by user %s from %s
- 0x40324704 : IPv6 prefix length was changed to %s for IOM 04 by user %s from %s
- 0x40324705 : IPv6 prefix length was changed to %s for IOM 05 by user %s from %s
- 0x40324706 : IPv6 prefix length was changed to %s for IOM 06 by user %s from %s
- 0x40324707 : IPv6 prefix length was changed to %s for IOM 07 by user %s from %s

- 0x40324708 : IPv6 prefix length was changed to %s for IOM 08 by user %s from %s
- 0x40324709 : IPv6 prefix length was changed to %s for IOM 09 by user %s from %s
- 0x4032470A : IPv6 prefix length was changed to %s for IOM 10 by user %s from %s

Explanation: The specified user account changed the IPv6 prefix length for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- IPv6 prefix length is changed to 64 for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324801   Configuration request succeeded for IOM 01 by user %s from %s

Related messages:
- 0x40324802 : Configuration request succeeded for IOM 02 by user %s from %s
- 0x40324803 : Configuration request succeeded for IOM 03 by user %s from %s
- 0x40324804 : Configuration request succeeded for IOM 04 by user %s from %s
- 0x40324805 : Configuration request succeeded for IOM 05 by user %s from %s
- 0x40324806 : Configuration request succeeded for IOM 06 by user %s from %s
- 0x40324807 : Configuration request succeeded for IOM 07 by user %s from %s
- 0x40324808 : Configuration request succeeded for IOM 08 by user %s from %s
- 0x40324809 : Configuration request succeeded for IOM 09 by user %s from %s
- 0x4032480A : Configuration request succeeded for IOM 10 by user %s from %s

Explanation: The specified user account successfully changed the configuration for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- "Configuration request succeeded for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Information only; no action is required.

0x40324901   Configuration request failed for IOM 01 by user %s from %s

Related messages:
- 0x40324902 : Configuration request failed for IOM 02 by user %s from %s
- 0x40324903 : Configuration request failed for IOM 03 by user %s from %s
- 0x40324904 : Configuration request failed for IOM 04 by user %s from %s
- 0x40324905 : Configuration request failed for IOM 05 by user %s from %s
- 0x40324906 : Configuration request failed for IOM 06 by user %s from %s
- 0x40324907 : Configuration request failed for IOM 07 by user %s from %s
- 0x40324908 : Configuration request failed for IOM 08 by user %s from %s
- 0x40324909 : Configuration request failed for IOM 09 by user %s from %s

- 0x4032490A : Configuration request failed for IOM 10 by user %s from %s

Explanation: The specified user account was not able to change the IPv6 configuration for the specified I/O module.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:

- "Configuration request failed for IOM 2 by user USERID from 192.168.1.1 (Web).

User response: Perform these steps:

1. Verify that the I/O module is capable of IPv6 configuration. See the documentation that was provided with the I/O module.
2. Reseat the I/O module.
3. Update the firmware for the I/O module.

0x40324A01   DHCP configuration timeout for IOM 01

Related messages:

- 0x40324A02 : DHCP configuration timeout for IOM 02
- 0x40324A03 : DHCP configuration timeout for IOM 03
- 0x40324A04 : DHCP configuration timeout for IOM 04
- 0x40324A05 : DHCP configuration timeout for IOM 05
- 0x40324A06 : DHCP configuration timeout for IOM 06
- 0x40324A07 : DHCP configuration timeout for IOM 07
- 0x40324A08 : DHCP configuration timeout for IOM 08
- 0x40324A09 : DHCP configuration timeout for IOM 09
- 0x40324A0A : DHCP configuration timeout for IOM 10

Explanation: The specified I/O module DHCP configuration timeout.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:

- "IOM 2 IPv6 DHCP address configuration timeout (Web).

User response: Perform these steps:

1. Verify that the DHCP server is functional.
2. Verify that the I/O module is capable of IPv6 configuration. See the documentation that was provided with the I/O module.
3. Reseat the I/O module.
4. Update the firmware for the I/O module.

0x40524901   POST timeout for I/O module 01 has occurred and a retry is being attempted

Related messages:
- 0x40524902 : POST timeout for I/O module 02 has occurred and a retry is being attempted
- 0x40524903 : POST timeout for I/O module 03 has occurred and a retry is being attempted
- 0x40524904 : POST timeout for I/O module 04 has occurred and a retry is being attempted
- 0x40524905 : POST timeout for I/O module 05 has occurred and a retry is being attempted
- 0x40524906 : POST timeout for I/O module 06 has occurred and a retry is being attempted
- 0x40524907 : POST timeout for I/O module 07 has occurred and a retry is being attempted
- 0x40524908 : POST timeout for I/O module 08 has occurred and a retry is being attempted
- 0x40524909 : POST timeout for I/O module 09 has occurred and a retry is being attempted
- 0x4052490A : POST timeout for I/O module 10 has occurred and a retry is being attempted

Explanation: The specified I/O module did not complete POST. The advanced management module is restarting the I/O module.

Severity: Informational

Alert Category: I/O Modules (Informational) - mmTrapIOS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

User response: Information only; no action is required.

0x40624901   I/O module fast POST was disabled.

Explanation: The fast POST for the specified I/O module has been disabled by a user.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x40624902   I/O module fast POST was enabled.

Explanation: The fast POST for the specified I/O module has been enabled by a user.

Severity: Informational

Alert Category: Network change (Informational) - mmTrapNwChangeS

Log Source: IOMod_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x43000101   Complex %04X (blades %s): Power Off Partition 01 (blades %s) by %s at %s

Explanation: The specified user requested that the specified partition be stopped.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Power Off Partition 1 (blades 4,5) request by USERID at 10.10.10.50 (Web)

User response: If the partition is not stopped, perform these steps:

1. Check the event log for other events related to the specified blade servers and resolve those events.
2. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
3. Reseat the scalable blade complex.
4. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000102   Complex %04X (blades %s): Power On Partition 02 (blades %s) by %s at %s

Explanation: The specified user requested that the specified partition be started.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Power On Partition 2 (blades 6,7) request by USERID at 10.10.10.50 (Web)

User response: If the partition is not started, perform these steps:

1. Check the event log for other events related to the specified blade servers and resolve those events.
2. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
3. Reseat the scalable blade complex.
4. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000103   Complex %04X (blades %s): Power Cycle Partition 03 (blades %s) by %s at %s

Explanation: The specified user requested that the partition in the specified scalable blade complex be reset. If the partition is off, it will turn on. If the partition is on, it will turn off than then turn on.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Power Cycle Partition 1 (blades 4,5) request by USERID at 10.10.10.50 (Web)

User response: If the partition is not reset, perform these steps:

1. Check the event log for other events related to the specified blade servers and resolve those events.

2. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.

3. Reseat the scalable blade complex.

4. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000104   Complex %04X (blades %s): Reset Partition 04 (blades %s) by %s at %s

Explanation: The specified user requested that the partition in the specified scalable blade complex be reset. If the partition is off, it will turn on. If the partition is on, it will turn off than then turn on.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Reset Partition 1 (blades 4,5) request by USERID at 10.10.10.50 (Web)

User response: This event only reports a requested action from a user for auditing purposes. If the requested action does not appear to have the desired effect, perform the following:

1. Check the event log for other events related to the specified blade servers and resolve those events.

2. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.

3. Reseat the scalable blade complex.

4. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000105   Complex %04X (blades %s): Pulse Interrupt Partition 05 (blades %s) by %s at %s

Explanation: The specified user requested a partition interrupt for the specified partition.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Interrupt Partition 1 (blades 4,5,6) request by USERID at 10.10.10.50 (Web)

User response: This event only reports a requested action from a user for auditing purposes. The product may not support the operation. If the product does support the operation and the requested action does not appear to have the desired effect, perform the following:

1. Check the event log for other events related to the specified blade servers and resolve those events.

2. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.

3. Reseat the scalable blade complex.

4. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000106   Complex %04X (blades %s): Soft Shutdown Partition 06 (blades %s) by %s at %s

Explanation: The specified user requested a soft shudown of the specified partition.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Soft Shutdown Partition 1 (blades 4,5) request by USERID at 10.10.10.50 (Web)

User response: This event only reports a requested action from a user for auditing purposes. The product may not support the operation. If the product does support the operation and the requested action does not appear to have the desired effect, perform the following:

1. Check the event log for other events related to the specified blade servers and resolve those events.
2. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
3. Reseat the scalable blade complex.
4. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000108   Complex %04X (blades %s): Add/Write Partition 08 (blades %s) by %s at %s

Explanation: The specified user performed a Partition Write/Add Configuration operation for the specified scalable blade complex.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Add/Write Partition 1 (blades 4,5) by USERID at 10.10.10.50 (Web)

User response: If the requested action does not appear to have the desired effect, perform these steps:

1. Ensure that all the blade servers in the scalable blade complex are powered off.
2. Check the event log for other events related to the specified blade servers and resolve those events.
3. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
4. Reseat the scalable blade complex.
5. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000109   Complex %04X (blades %s): Delete Partition 09 (blades %s) by %s at %s

Explanation: The specified user requested that the partition be removed for the specified scalable blade complex. As a result, all blade servers in the scalable blade complex will operate independently until a new partition has been created.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

0x4300010A • 0x4300010B

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Delete Partition 1 by USERID at 10.10.10.50 (Web)

User response: If the blade servers in the scalable blade complex are not operating independently, perform these steps:

1. Ensure that all the blade servers in the scalable blade complex are powered off.
2. Check the event log for other events related to the specified blade servers and resolve those events.
3. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
4. Reseat the scalable blade complex.
5. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x4300010A   Complex %04X (blades %s): Create Auto Partition by %s at %s

Explanation: The specified user performed a Set Auto Partition Configuration operation. This request should result in having all the blade/nodes in a complex be configured into a single partition.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Create Auto Partition by USERID at 10.10.10.50 (Web)

User response: If the requested action does not appear to have the desired effect, perform these steps:

1. Ensure that all the blade servers in the scalable blade complex are powered off.
2. Check the event log for other events related to the specified blade servers and resolve those events.
3. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
4. Reseat the scalable blade complex.
5. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x4300010B   Complex %04X (blades %s): Clear all Partition Configuration by %s at %s

Explanation: The specified user requested that the partition be removed for the specified scalable blade complex. As a result, all blade servers in the scalable blade complex will operate independently until a new partition has been created.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Clear all Partition Configuration by USERID at 10.10.10.50 (Web)

User response: If the blade servers in the scalable blade complex are not operating independently, perform these steps:

1. Ensure that all the blade servers in the scalable blade complex are powered off.

2. Check the event log for other events related to the specified blade servers and resolve those events.

3. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.

4. Reseat the scalable blade complex.

5. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x4300010C   Complex %04X (blades %s): Set Partition 12 (blades %s) to Partition Mode by %s at %s

Explanation: The specified user requested that the blade servers in a scalable blade complex operate in partition mode.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Request to set Partition 1 (blades 4,5) to Partition Mode by USERID at 10.10.10.50 (Web)

User response: If the blade servers are not operating in partition mode, perform these steps:

1. Ensure that all the blade servers in the scalable blade complex are powered off.

2. Check the event log for other events related to the specified blade servers and resolve those events.

3. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.

4. Reseat the scalable blade complex.

5. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and Device Drivers Web page.

0x4300010D   Complex %04X (blades %s): Set Partition 13 (blades %s) to Stand-Alone Mode by %s at %s

Explanation: The specified user requested requested that the blade servers in a scalable blade complex operate in stand-alone mode.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message: Complex A01C (blades 4,5,6,7): Request to set Partition 1 (blades 4,5) to Stand-alone Mode by USERID at 10.10.10.50 (Web)

User response: This event only reports a requested action from a user for auditing purposes. If the blade servers are not operating in stand-alone mode, perform these steps:

1. Ensure that all the blade servers in the scalable blade complex are powered off.

2. Check the event log for other events related to the specified blade servers and resolve those events.

3. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.

4. Reseat the scalable blade complex.

5. Update the firmware for the service processor on the blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x4300010E   Complex Descriptor is corrupted. Partition configuration and control not available.

Explanation: The blade server provided a complex descriptor that is not valid. The advanced management module cannot perform partition configuration or control until a valid complex descriptor is provided by the target scalable blade complex.

Severity: Warning

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Reset the blade system management processor on all blade servers in the scalable blade complex. You can reset the service processor through the advanced management module Web interface from the Blade Power/Restart page.
2. Reseat the scalable blade complex.
3. Update the firmware for the service processor on the specified blade server. You can find the appropriate firmware on the IBM BladeCenter software and device drivers Web page.

0x43000500   Management network auto-discovery

Explanation: Management channel auto-discovery (MCAD) has been enabled or disabled by the specified user account.

Severity: Informational

Alert Category: User activity (Informational) - mmTrapRemoteLoginS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Management network auto-discovery enabled by 'USERID' from '192.168.0.1 (Web)'.
- Management network auto-discovery disabled by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x48008401   Power allocated is higher than the power domain 01 capacity

Related messages:
- 0x48008402 : Power allocated is higher than the power domain 02 capacity

Explanation: The power allocated for the components in the domain is higher than the power capacity available in the domain. The power domain may go down.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Make sure there are working power modules in the domain. Replace any power modules that have been removed or have failed.

0x4800A400   Blade power policy on chassis restart

Explanation: The power policy for blade servers in the chassis has changed. The new policy will take affect when the advanced management module is restarted .

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: Audit

Automatically notify service: No

Recoverable: No

Example Message:
- Blade power policy on chassis restart was successfully changed to 'restore last power state' by 'USERID' from '192.168.0.1 (Web)'.
- Blade power policy on chassis restart was successfully changed to 'automatic power on' by 'USERID' from '192.168.0.1 (Web)'.
- Blade power policy on chassis restart was successfully changed to 'manual power on' by 'USERID' from '192.168.0.1 (Web)'.

User response: Information only; no action is required.

0x64001000   Cable on add-in card not connected to system board

Explanation: A cable on an expansion card is not connected to system board for the specified blade server.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Reseat the expansion card, ensuring the cable is connected to the system board.
2. Replace the cable.

0x6E000001   I/O and Graphics Adapter problem detected.

Explanation: A problem with the I/O and Graphics Adapter has been detected for the specified blade.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. If this is occurring on an HC10, reseat the graphics adapter and video controller.
2. If this is occurring on any other blade server, reseat the blade server.
3. Update the firmware for the video adapter.

4. Update BIOS for the blade server.
5. Replace the compression card.
6. Generate a call home using Service Advisor:
   - If this is occurring on an HC10 blade workstation, replace the graphics adapter. Be ready to provide part number for the adapter.
   - If this is occurring on any other blade server, replace the system board.

0x6F100000   The air filter needs service immediately

Explanation: The air filter needs service immediately.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Service the air filter. Check the IBM Support Web page for any service bulletins related to servicing the air filter.

0x6F100001   Routine air filter service check is needed.

Explanation: It is time to perform a routine check on the air filter.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Perform these steps:
1. Check the air filter.
2. Acknowledge the event from the advanced management module interface to set the air filter service timer. See the Advanced Management Module User's Guide for information about setting the air filter server timer. The guide is available on the Web.

0x6F200000   The air filter needs service.

Explanation: The air filter needs service.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Major

User response: Service the air filter. Check the IBM Support Web page for any service bulletins related to servicing the air filter.

0x6F300000   The air filter may need service.

Explanation: The air filter needs service.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Service the air filter. Check the IBM Support Web page for any service bulletins related to servicing the air filter.

0x6F500000   Routine air filter service check is needed.

Explanation: The air filter needs routine service.

Severity: Warning

Alert Category: Chassis/System Management (Warning) - mmTrapChassisN

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: Service the air filter. Check the IBM Support Web page for any service bulletins related to servicing the air filter.

0x6F600001   Management Module interposer 01 installed.

Related messages:
- 0x6F600002 : Management Module interposer 02 installed.

Explanation: The specified management-module interposer has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F600101   Management Module secondary interposer 01 installed.

Related messages:
- 0x6F600102 : Management Module secondary interposer 02 installed.

Explanation: The specified secondary management-module interposer has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F601001   Management Module interposer 01 removed.

Related messages:

• 0x6F601002 : Management Module interposer 02 removed.

Explanation: The specified management-module interposer has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F601101   Management Module secondary interposer 01 removed.

Related messages:

• 0x6F601102 : Management Module secondary interposer 02 removed.

Explanation: The specified secondary management-module interposer has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F602001   I/O Module interposer 01 installed.

Related messages:

• 0x6F602002 : I/O Module interposer 02 installed.
• 0x6F602003 : I/O Module interposer 03 installed.
• 0x6F602004 : I/O Module interposer 04 installed.
• 0x6F602005 : I/O Module interposer 05 installed.
• 0x6F602006 : I/O Module interposer 06 installed.
• 0x6F602007 : I/O Module interposer 07 installed.
• 0x6F602008 : I/O Module interposer 08 installed.
• 0x6F602009 : I/O Module interposer 09 installed.
• 0x6F60200A : I/O Module interposer 10 installed.

Explanation: The specified I/O-module interposer has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F602101   I/O Module secondary interposer 01 installed.

Related messages:
- 0x6F602102 : I/O Module secondary interposer 02 installed.
- 0x6F602103 : I/O Module secondary interposer 03 installed.
- 0x6F602104 : I/O Module secondary interposer 04 installed.
- 0x6F602105 : I/O Module secondary interposer 05 installed.
- 0x6F602106 : I/O Module secondary interposer 06 installed.
- 0x6F602107 : I/O Module secondary interposer 07 installed.
- 0x6F602108 : I/O Module secondary interposer 08 installed.
- 0x6F602109 : I/O Module secondary interposer 09 installed.
- 0x6F60210A : I/O Module secondary interposer 10 installed.

Explanation: The specified secondary I/O-module interposer has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F603001   I/O Module interposer 01 removed.

Related messages:
- 0x6F603002 : I/O Module interposer 02 removed.
- 0x6F603003 : I/O Module interposer 03 removed.
- 0x6F603004 : I/O Module interposer 04 removed.
- 0x6F603005 : I/O Module interposer 05 removed.
- 0x6F603006 : I/O Module interposer 06 removed.
- 0x6F603007 : I/O Module interposer 07 removed.
- 0x6F603008 : I/O Module interposer 08 removed.
- 0x6F603009 : I/O Module interposer 09 removed.
- 0x6F60300A : I/O Module interposer 10 removed.

Explanation: The specified I/O-module interposer has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F603101   I/O Module secondary interposer 01 removed.

Related messages:
- 0x6F603102 : I/O Module secondary interposer 02 removed.
- 0x6F603103 : I/O Module secondary interposer 03 removed.
- 0x6F603104 : I/O Module secondary interposer 04 removed.
- 0x6F603105 : I/O Module secondary interposer 05 removed.

- 0x6F603106 : I/O Module secondary interposer 06 removed.
- 0x6F603107 : I/O Module secondary interposer 07 removed.
- 0x6F603108 : I/O Module secondary interposer 08 removed.
- 0x6F603109 : I/O Module secondary interposer 09 removed.
- 0x6F60310A : I/O Module secondary interposer 10 removed.

Explanation: The specified secondary I/O-module interposer has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F608001   Multiplexer Expansion module 01 installed.

Related messages:
- 0x6F608002 : Multiplexer Expansion module 02 installed.

Explanation: The specified multiplexer expansion module has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required. Now the module can be removed.

0x6F609001   Multiplexer Expansion module 01 removed.

Related messages:
- 0x6F609002 : Multiplexer Expansion module 02 removed.

Explanation: The specified multiplexer expansion module has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required. Now the module can be removed.

0x6F609101   Multiplexer Expansion module 01 can now be removed safely.

Related messages:
- 0x6F609102 : Multiplexer Expansion module 02 can now be removed safely.

Explanation: The specified multiplexer expansion module can now be removed. The FFR (FRU ready for removal) LED should be lit.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required. Now the module can be removed.

0x6F60A001   **Alarm Panel module installed.**

Explanation: The alarm panel module has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F60A002   **Alarm Panel module removed.**

Explanation: The alarm panel module has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F60A003   **Alarm Panel module can now be removed safely.**

Explanation: The alarm panel module can now be removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F60A101   **Alarm Panel module hardware failure.**

Explanation: The alarm panel module (LED panel on the front of the chassis) has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:

1. Reseat the alarm panel.
2. Replace the alarm panel.

0x6F60A201   Alarm Panel module is now powered on.

Explanation: The alarm panel module has been powered on.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F60A401   Alarm Panel module is now powered off.

Explanation: The alarm panel module has powered off.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F60B001   Air filter installed.

Explanation: The bezel filter on the chassis has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F60B101   Air filter removed.

Explanation: The bezel filter on the chassis has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F60C001   Media Tray 01 hardware failure.

Related messages:

• 0x6F60C002 : Media Tray 02 hardware failure.

Explanation: Communication over the I2C bus between the advanced management module and the specified media tray has been lost. The advanced management module cannot determine the state of the media tray.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the media tray.
2. Replace the media tray.

0x6F60C101   Media tray 01 firmware update will take effect after restarting the AMM.

Related messages:

• 0x6F60C102 : Media tray 02 firmware update will take effect after restarting the AMM.

Explanation: The firmware for the specified media tray was updated.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Restart the advanced management module.

0x6F60C201   Media Tray 01 has unrecognized VPD.

Related messages:

• 0x6F60C202 : Media Tray 02 has unrecognized VPD.

Explanation: The vital product data (VPD) for the specified media tray is not recognized as valid by the advanced management module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Continue to monitor the event log for other events related to the media tray and resolve those events if they occur.

0x6F60D001   Multiplexer Expansion module 01 communication failed.

Related messages:

• 0x6F60D002 : Multiplexer Expansion module 02 communication failed.

Explanation: Communication on the I2C bus between the advanced management module and the specified multiplexer expansion module has failed.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the multiplexer expansion module.
2. Replace the multiplexer expansion module.

0x6F60F001   Multiplexer Card 01 controller firmware was not updated.

Related messages:

• 0x6F60F002 : Multiplexer Card 02 controller firmware was not updated.

Explanation: The firmware for the specified media tray was not updated. Existing firmware will continue to be used.

Severity: Error

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Reseat the media tray.
2. Check the event log for other errors related to the management module and resolve them.
3. Attempt to update the management module firmware again.

0x6F700001   Begin formatting

Explanation: File system formatting has started on the CompactFlash module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Begin formatting top mediatray's Compact Flash device at /dev/sdc1

User response: Information only; no action is required. However, anything currently stored in the compact flash card will be lost.

0x6F700002   End formatting

Explanation: File system formatting has completed on the CompactFlash module.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: End formatting top mediatray's Compact Flash device at /dev/sdc1

User response: Information only; no action is required.

0x6F700003   Empty log message or generated at run-time

Explanation: An active volume is selected for CompactFlash module. This log message is empty or generated at run-time.

Severity: Informational

Alert Category: Chassis/System Management (Informational) - mmTrapChassisS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Example Message: Top mediatray's compact flash card is active

User response: Information only; no action is required.

0x6F700004   Active volume is inoperable

Explanation: The active volume on the CompactFlash module cannot be read.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Perform these steps:
1. Reseat the CompactFlash module.
2. Replace the CompactFlash module.

0x6F700005   Image file on active volume failed size check and is deleted

Explanation: The image on the active volume of the CompactFlash module is corrupt; it has been deleted.

Severity: Error

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

0x6F800001 • 0x6F800301

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Attempt to load the image to the CompactFlash module again.
2. Reset the CompactFlash module.
3. Replace the CompactFlash module.

0x6F800001   Storage Module 01 installed

Related messages:
- 0x6F800002 : Storage Module 02 installed

Explanation: The specified storage module was installed.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

User response: Perform these steps:
1. If you installed a storage module, this event is informational; no action is required.
2. If you did not install a storage module, check the IBM Support Web page for any service bulletins that might be related to this problem.

0x6F800101   Storage Module 01 removed

Related messages:
- 0x6F800102 : Storage Module 02 removed

Explanation: The specified storage module was removed.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT): Minor

User response: If you removed the storage module, this event is informational only; no action is required. If you did not remove the storage module:
1. Look in the event log for other events related to this storage module and resolve those events.
2. Continue monitoring the event log for additional messages. At your earliest convenience, reseat the storage module.
3. If problem persists, check the IBM Support Web page for any service bulletins that might be related to this problem.

0x6F800301   No compatible I/O Module installed for use with Storage Module 01.

Related messages:
- 0x6F800302 : No compatible I/O Module installed for use with Storage Module 02.

Explanation: No compatible I/O Module installed for use with certain Storage Module. Either there is no I/O module installed in I/O module bays 3 and 4, or the I/O modules installed in I/O module bays 3 and 4 are not SAS I/O modules.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: If you are using the integrated, shared storage, you must install a SAS I/O module in I/O module bay 3 (a SAS I/O module may also be required in I/O module bay 4).

0x6F800401   Storage Module 01 was powered on.

Related messages:

- 0x6F800402 : Storage Module 02 was powered on.

Explanation: The advanced management module detected that the specified power module was powered on.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F800501   Unable to read VPD for Storage Module 01.

Related messages:

- 0x6F800502 : Unable to read VPD for Storage Module 02.

Explanation: The advanced management module is unable to read the vital product data (VPD) for the specified storage module.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Verify that the storage module LED is not lit. If it is not lit, continue monitoring the event log for additional messages. At your earliest convenience, reseat the storage module.
2. If the storage module LED is lit, reseat the storage module. Before reseating the storage module, make sure that the blade servers are not actively working with the hard disk drives (the hard disk drive LEDs are lit when drive activity is occurring).
3. If the problem persists, check the IBM Support Web page for any service bulletins that might be related to this problem.

0x6F800601   Storage Module 01 may power down due to multiple cooling device failures.

Related messages:

- 0x6F800602 : Storage Module 02 may power down due to multiple cooling device failures.

0x6F801001 • 0x6F801101

Explanation: There is insufficient cooling available for the storage module. It will power down in five minutes if no action is taken.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:
1. Check the event log for errors related to power modules.
2. Resolve any errors that you find.

0x6F801001   Storage Module 1 Drive 01 installed

Related messages:
- 0x6F801002 : Storage Module 1 Drive 02 installed
- 0x6F801003 : Storage Module 1 Drive 03 installed
- 0x6F801004 : Storage Module 1 Drive 04 installed
- 0x6F801005 : Storage Module 1 Drive 05 installed
- 0x6F801006 : Storage Module 1 Drive 06 installed
- 0x6F801007 : Storage Module 1 Drive 07 installed
- 0x6F801008 : Storage Module 1 Drive 08 installed
- 0x6F801009 : Storage Module 1 Drive 09 installed
- 0x6F80100A : Storage Module 1 Drive 10 installed
- 0x6F80100B : Storage Module 1 Drive 11 installed
- 0x6F80100C : Storage Module 1 Drive 12 installed

Explanation: The specified hard disk drive was installed in storage module 1.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F801101   Storage Module 1 Drive 01 removed

Related messages:
- 0x6F801102 : Storage Module 1 Drive 02 removed
- 0x6F801103 : Storage Module 1 Drive 03 removed
- 0x6F801104 : Storage Module 1 Drive 04 removed
- 0x6F801105 : Storage Module 1 Drive 05 removed
- 0x6F801106 : Storage Module 1 Drive 06 removed
- 0x6F801107 : Storage Module 1 Drive 07 removed
- 0x6F801108 : Storage Module 1 Drive 08 removed
- 0x6F801109 : Storage Module 1 Drive 09 removed
- 0x6F80110A : Storage Module 1 Drive 10 removed
- 0x6F80110B : Storage Module 1 Drive 11 removed

- 0x6F80110C : Storage Module 1 Drive 12 removed

Explanation: The specified hard disk drive has been removed from storage module 1 or the storage module has been removed from the chassis.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

User response: If you removed a hard drive, this event is for your information only; no action is required. If you did not remove a hard disk drive, perform these steps:

1. Verify that the specified hard disk drive is installed in the storage module.
2. If you are in the same location as the chassis, verify that the fault LED on the hard disk drive is not lit. If it is lit, replace the hard disk drive.
3. Determine if the hard drive is operational:
   a. Use Storage Configuration Manager*, if installed, to determine if the hard disk drive is available. *Storage Configuration Manager is not supported when configured with 12 disks storage module.
   b. Log into the blade server that is assigned to that hard disk drive to see if the blade server can still see that drive.
4. If the hard disk drive is not operational, replace the hard disk drive.
5. If the hard disk drive is operational, check the IBM Support Web page for any service bulletins that might be related to this problem.

0x6F801201   Storage Module 1 Drive 01 fault

Related messages:
- 0x6F801202 : Storage Module 1 Drive 02 fault
- 0x6F801203 : Storage Module 1 Drive 03 fault
- 0x6F801204 : Storage Module 1 Drive 04 fault
- 0x6F801205 : Storage Module 1 Drive 05 fault
- 0x6F801206 : Storage Module 1 Drive 06 fault
- 0x6F801207 : Storage Module 1 Drive 07 fault
- 0x6F801208 : Storage Module 1 Drive 08 fault
- 0x6F801209 : Storage Module 1 Drive 09 fault
- 0x6F80120A : Storage Module 1 Drive 10 fault
- 0x6F80120B : Storage Module 1 Drive 11 fault
- 0x6F80120C : Storage Module 1 Drive 12 fault

Explanation: There is a fault with the specified hard disk drive that is installed in storage module 1.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: Stor_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Replace the hard disk drive.
2. Check the IBM Support Web page for related service bulletins.

3. Update the firmware for the storage module, the SAS expansion card options in the blade servers, the SAS I/O modules, and hard drives if applicable.

0x6F801301   Storage Module 2 Drive 01 installed

Related messages:
- 0x6F801302 : Storage Module 2 Drive 02 installed
- 0x6F801303 : Storage Module 2 Drive 03 installed
- 0x6F801304 : Storage Module 2 Drive 04 installed
- 0x6F801305 : Storage Module 2 Drive 05 installed
- 0x6F801306 : Storage Module 2 Drive 06 installed
- 0x6F801307 : Storage Module 2 Drive 07 installed
- 0x6F801308 : Storage Module 2 Drive 08 installed
- 0x6F801309 : Storage Module 2 Drive 09 installed
- 0x6F80130A : Storage Module 2 Drive 10 installed
- 0x6F80130B : Storage Module 2 Drive 11 installed
- 0x6F80130C : Storage Module 2 Drive 12 installed

Explanation: The specified hard disk drive was installed in storage module 2.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F801401   Storage Module 2 Drive 01 removed

Related messages:
- 0x6F801402 : Storage Module 2 Drive 02 removed
- 0x6F801403 : Storage Module 2 Drive 03 removed
- 0x6F801404 : Storage Module 2 Drive 04 removed
- 0x6F801405 : Storage Module 2 Drive 05 removed
- 0x6F801406 : Storage Module 2 Drive 06 removed
- 0x6F801407 : Storage Module 2 Drive 07 removed
- 0x6F801408 : Storage Module 2 Drive 08 removed
- 0x6F801409 : Storage Module 2 Drive 09 removed
- 0x6F80140A : Storage Module 2 Drive 10 removed
- 0x6F80140B : Storage Module 2 Drive 11 removed
- 0x6F80140C : Storage Module 2 Drive 12 removed

Explanation: The specified hard disk drive has been removed from storage module 2 or the storage module has been removed from the chassis.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

User response: If you removed a hard drive, this event is for your information only; no action is required. If you did not remove a hard disk drive, perform these steps:

1. Verify that the specified hard disk drive is installed in the storage module.
2. If you are in the same location as the chassis, verify that the fault LED on the hard disk drive is not lit. If it is lit, replace the hard disk drive.
3. Determine if the hard drive is operational:
   a. Use Storage Configuration Manager*, if installed, to determine if the hard disk drive is available. *Storage Configuration Manager is not supported when configured with 12 disks storage module.
   b. Log into the blade server that is assigned to that hard disk drive to see if the blade server can still see that drive.
4. If the hard disk drive is not operational, replace the hard disk drive.
5. If the hard disk drive is operational, check the IBM Support Web page for any service bulletins that might be related to this problem.

0x6F801501   Storage Module 2 Drive 01 fault

Related messages:
- 0x6F801502 : Storage Module 2 Drive 02 fault
- 0x6F801503 : Storage Module 2 Drive 03 fault
- 0x6F801504 : Storage Module 2 Drive 04 fault
- 0x6F801505 : Storage Module 2 Drive 05 fault
- 0x6F801506 : Storage Module 2 Drive 06 fault
- 0x6F801507 : Storage Module 2 Drive 07 fault
- 0x6F801508 : Storage Module 2 Drive 08 fault
- 0x6F801509 : Storage Module 2 Drive 09 fault
- 0x6F80150A : Storage Module 2 Drive 10 fault
- 0x6F80150B : Storage Module 2 Drive 11 fault
- 0x6F80150C : Storage Module 2 Drive 12 fault

Explanation: There is a fault with the specified hard disk drive that is installed in storage module 2.

Severity: Error

Alert Category: Storage Modules (Critical) - mmTrapStorageC

Log Source: Stor_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Critical

User response: Perform these steps:
1. Replace the hard disk drive.
2. Check the IBM Support Web page for related service bulletins.
3. Update the firmware for the storage module, the SAS expansion card options in the blade servers, the SAS I/O modules, and hard drives if applicable.

0x6F801601   Storage Module 1 Drive 01 PFA

Related messages:
- 0x6F801602 : Storage Module 1 Drive 02 PFA
- 0x6F801603 : Storage Module 1 Drive 03 PFA
- 0x6F801604 : Storage Module 1 Drive 04 PFA
- 0x6F801605 : Storage Module 1 Drive 05 PFA

0x6F801701

- 0x6F801606 : Storage Module 1 Drive 06 PFA
- 0x6F801607 : Storage Module 1 Drive 07 PFA
- 0x6F801608 : Storage Module 1 Drive 08 PFA
- 0x6F801609 : Storage Module 1 Drive 09 PFA
- 0x6F80160A : Storage Module 1 Drive 10 PFA
- 0x6F80160B : Storage Module 1 Drive 11 PFA
- 0x6F80160C : Storage Module 1 Drive 12 PFA

Explanation: A Predictive Failure Analysis (PFA) fault was detected with the specified hard disk drive that is installed in storage module 1.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Replace the hard disk drive. See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for information about predictive failure analysis conditions and replacing hard disk drives. The guide is available from the Web.
2. Check the IBM Support Web page for related service bulletins.

0x6F801701   Storage Module 2 Drive 01 PFA

Related messages:
- 0x6F801702 : Storage Module 2 Drive 02 PFA
- 0x6F801703 : Storage Module 2 Drive 03 PFA
- 0x6F801704 : Storage Module 2 Drive 04 PFA
- 0x6F801705 : Storage Module 2 Drive 05 PFA
- 0x6F801706 : Storage Module 2 Drive 06 PFA
- 0x6F801707 : Storage Module 2 Drive 07 PFA
- 0x6F801708 : Storage Module 2 Drive 08 PFA
- 0x6F801709 : Storage Module 2 Drive 09 PFA
- 0x6F80170A : Storage Module 2 Drive 10 PFA
- 0x6F80170B : Storage Module 2 Drive 11 PFA
- 0x6F80170C : Storage Module 2 Drive 12 PFA

Explanation: A Predictive Failure Analysis (PFA) fault was detected with the specified hard disk drive that is installed in storage module 2.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT): Minor

User response: Perform these steps:

1. Replace the hard disk drive. See the IBM BladeCenter SAS RAID Controller Module Installation and User's Guide for information about predictive failure analysis conditions and replacing hard disk drives. The guide is available from the Web.

2. Check the IBM Support Web page for related service bulletins.

0x6F802001   Battery Backup Unit 01 installed

Related messages:

- 0x6F802002 : Battery Backup Unit 02 installed

Explanation: The specified battery backup unit has been installed.

Severity: Informational

Alert Category: Storage Modules (Informational) - mmTrapStorageS

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F802101   Battery Backup Unit 01 removed

Related messages:

- 0x6F802102 : Battery Backup Unit 02 removed

Explanation: The specified battery backup unit has been removed.

Severity: Warning

Alert Category: Storage Modules (Warning) - mmTrapStorageN

Log Source: Stor_##

Automatically notify service: No

Recoverable: No

Alarm Panel LED (BC T and BC HT):   Minor

User response: Information only; no action is required.

0x6F803001   Direct Serial Attach module installed

Explanation: The serial pass-thru module has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F803002   Direct Serial Attach module removed

Explanation: The serial pass-thru module has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

0x6F900001 • 0x6FA00001

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F900001   I/O Flex Cable 01 installed

Related messages:
- 0x6F900002 : I/O Flex Cable 02 installed
- 0x6F900003 : I/O Flex Cable 03 installed
- 0x6F900004 : I/O Flex Cable 04 installed

Explanation: The specified I/O-module Flex Cable has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6F901001   I/O Flex Cable 01 removed

Related messages:
- 0x6F901002 : I/O Flex Cable 02 removed
- 0x6F901003 : I/O Flex Cable 03 removed
- 0x6F901004 : I/O Flex Cable 04 removed

Explanation: The specified I/O-module Flex Cable has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6FA00001   KVM module installed

Explanation: A KVM module has been installed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6FA01001   KVM module removed

Explanation: A KVM module has been removed.

Severity: Informational

Alert Category: Inventory change (Informational) - mmTrapSysInvS

Log Source: SERVPROC

Automatically notify service: No

Recoverable: No

User response: Information only; no action is required.

0x6FA02001   KVM module unavailable

Explanation: The KVM module installed in the chassis is unavailable or unreadable. The chassis keyboard and mouse functions will not be available.

Severity: Warning

Alert Category: Chassis/System Management (Critical) - mmTrapChassisC

Log Source: SERVPROC

Automatically notify service: Yes

Recoverable: Yes

Chassis LED: Error

Alarm Panel LED (BC T and BC HT):   Major

User response: Perform these steps:
1. Make sure that there is a KVM module installed in the chassis.
2. If a KVM module is installed, replace it.
3. If a KVM module is not installed, install one. The chassis needs a KVM module to operate.

0x800000FF   Blade Specific Message

Explanation: The meaning of this event depends on the blade server that generates the event.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x80010000   under warning threshold.

Explanation: The service processor on the specified blade server has detected that the specified component has reached or is below the specified warning threshold (such as under voltage).

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

0x80010200 • 0x80010400

Recoverable: Yes

Example Message: System board (VBATT Sense) voltage under warning threshold. Reading: 6.10 Threshold: 7.00

Alarm Panel LED (BC T and BC HT): Minor

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Continue to monitor the event log to additional messages related to this condition.

2. If the event is an under voltage problem and it is occurring on all blade servers, look for other events in the log related to power and resolve those events.

0x80010200   **under critical threshold.**

Explanation: The service processor on the specified blade server has detected that the specified component has reached or is below the specified critical threshold (such as under voltage).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Expansion Module 2 (PEU2 3.3V Sense) voltage under critical threshold. Reading: 6.10, Threshold: 7.00.
- System board (Planar 12V) voltage under critical threshold. Reading: 6.10, Threshold: 7.00.
- Recovery Expansion Module 1 (BPE3 3.3V Sense) voltage under critical threshold.

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

0x80010400   **under non-recoverable threshold.**

Explanation: The service processor on the specified blade server has detected that the specified component has reached or is below the specified nonrecoverable critical threshold (such as under voltage).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: System board (5V Sense) voltage under nonrecoverable threshold. Reading: 6.10, Threshold: 7.00

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the under voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

0x80010700   over warning threshold.

Explanation: The service processor on the specified blade server has detected that the specified component has reached or exceeded the specified warning threshold (such as over temperature or over voltage).

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Processor 4 (CPU 4 Temp) temperature over warning threshold. Reading: 6.10, Threshold: 7.00.
- System board (Inlet Temp) temperature over warning threshold. Reading: 6.10, Threshold: 7.00.
- Recovery System board (Inlet Temp) temperature over warning threshold.

Alarm Panel LED (BC T and BC HT): Minor

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
   c. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
2. If the event is related to an over voltage condition:
   a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x80010701   %s %s (%s) %s recommended %s.

Related messages:
- 0x80010702 : %s %s (%s) %s recommended %s.
- 0x80010002 : %s %s (%s) %s recommended %s.

Explanation: The service processor on the specified blade server has detected that the specified component has reached or exceeded the specified fault threshold (such as over temperature or over voltage).

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

0x80010900

- System board (Planar 3.3V) over recommended voltage
- Processor (CPU 1 Temp) over recommended temperature

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Minor

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
   c. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
2. If the event is related to an over voltage condition:
   a. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
   b. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x80010900   over critical threshold.

Explanation: The service processor on the specified blade server has detected that the specified component has reached or exceeded the specified critical threshold (such as over temperature or over voltage).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Battery 1 (Planar VBAT) voltage over critical threshold. Reading: 6.10, Threshold: 7.00.
- Expansion Module 1 (BPE3 12V Sense) voltage over critical threshold. Reading: 6.10, Threshold: 7.00.
- Recovery System board (Inlet Temp) temperature over critical threshold.

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. If an air filter is installed, make sure that it is cleaned or replaced.
   c. Make sure that all fan/blower modules are running. Replace fan modules if necessary.

d. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

2. If the event is related to an over voltage condition:

a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

b. If no other blade server has this same problem, the issue is specific to the blade as a hardware or firmware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.

3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x80010901   %s %s (%s) %s critical %s.

Related messages:

- 0x80010902 : %s %s (%s) %s critical %s.
- 0x80010202 : %s %s (%s) %s critical %s.

Explanation: The service processor on the specified blade server has detected that the specified component has reached or exceeded the specified fault threshold (such as over temperature or over voltage).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

- System board (Planar 3.3V) over critical voltage
- Processor (CPU 1 Temp) over critical temperature

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:

a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.

b. Make sure that all fan/blower modules are running. Replace fan modules if necessary.

c. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

2. If the event is related to an over voltage condition:

a. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.

b. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

   Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x80010B00   over non-recoverable threshold.

Explanation: The service processor on the specified blade server has detected that the specified component has reached or exceeded the specified nonrecoverable threshold (such as over temperature or over voltage).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
*   Memory bank 2 (BANK2 TEMP) temperature over nonrecoverable threshold. Reading: 6.10, Threshold: 7.00.
*   System board (Inlet Temp) temperature over non-recoverable threshold. Reading: 6.10, Threshold: 7.00.

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
    a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
    b. If an air filter is installed, make sure that it is cleaned or replaced.
    c. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
    d. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

2. If the event is related to an over voltage condition:
    a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
    b. If no other blade server has this same problem, the issue is specific to the blade as a hardware or firmware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.

3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x80010B01   %s %s (%s) %s non-recoverable %s fault.

Related messages:
*   0x80010B02 : %s %s (%s) %s non-recoverable %s fault.
*   0x80010402 : %s %s (%s) %s non-recoverable %s fault.

Explanation: The service processor on the specified blade server has detected that the specified component has reached or exceeded the specified fault threshold (such as over temperature or over voltage).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

- System board (Planar 3.3V) over non-recoverable voltage fault
- Processor (CPU 1 Temp) over non-recoverable temperature fault

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
   c. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

2. If the event is related to an over voltage condition:
   a. Refer to the Problem Determination and Service Guide for the blade server or the documentation that came with the specified component for information about over voltage conditions.
   b. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events.

      Note: If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

0x80030100   occurred

Explanation: The specified sensor type event of the specified component on the specified blade server has occurred.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: System board, voltage (Out of Range) occurred.

User response: Information only; no action is required.

0x80070000   normal

Explanation: The specified sensor type of the specified component on the specified blade server is in a normal state.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 2, temperature (CPU 2 Overtemp) normal

User response: Information only; no action is required.

0x80070100   warning

Explanation: The specified sensor type of the specified component on the specified blade server is in a warning state.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
• Processor 1, temperature (CPU 1 Overtemp) warning
• Memory device 9, temperature (DIMM 9 Temp) warning
• Recovery Memory device 12, temperature (DIMM 12 Temp) warning

Alarm Panel LED (BC T and BC HT):   Minor

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. If an air filter is installed, make sure that it is cleaned or replaced.
   c. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
   d. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
2. If the event is related to an over voltage condition:
   a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
   b. If no other blade server has this same problem, the issue is specific to the blade as a hardware or firmware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.
3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x80070200   critical

Explanation: The specified sensor type of the specified component on the specified blade server is in a critical state.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
• Processor 2, temperature (CPU 2 Overtemp) critical
• Expansion Card 1 (HSDC Fault) critical
• System board, chip set (Sys Board Fault) critical

- Recovery Memory device 8, temperature (DIMM 8 Temp) critical
- Unsupported blade/blower combination

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. If an air filter is installed, make sure that it is cleaned or replaced.
   c. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
   d. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

2. If the event is related to an over voltage condition:
   a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
   b. If no other blade server has this same problem, the issue is specific to the blade as a hardware or firmware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.

3. If the event is related to Unsupported blade/blower:
   a. Check for the IBM Support Web page for any service bulletins related to Unsupported blade blower combinations
   b. Refer to the specific product interoperability guide for valid CPU / Power / Blower configurations and resolve

4. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x80070300   non-recoverable

Explanation: The specified sensor type of the specified component on the specified blade server is in a non-recoverable state.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 1, temperature (CPU 1 OverTemp) non-recoverable

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. If an air filter is installed, make sure that it is cleaned or replaced.
   c. Make sure that all fan/blower modules are running. Replace fan modules if necessary.

d. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

2. If the event is related to an over voltage condition:

a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

b. If no other blade server has this same problem, the issue is specific to the blade as a hardware or firmware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.

3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x80070500 critical

Explanation: The state of the specified sensor type on the specified component of the specified blade server has changed.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Recovery Processor 1, temperature (CPU 1 OverTemp) critical

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:

a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.

b. Make sure that all fan/blower modules are running. Replace fan modules if necessary.

c. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.

2. If the event is related to an over voltage condition:

a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.

b. If no other blade server has this same problem, the issue is specific to the blade as a hardware or firmware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.

3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x80070600 non-recoverable

Explanation: The specified sensor type of the specified component on the specified blade server is in a nonrecoverable state.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 2, temperature (CPU 2 OverTemp) non-recoverable

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the event is related to an over temperature condition:
   a. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
   b. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
   c. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
2. If the event is related to an over voltage condition:
   a. If the over voltage problem is occurring on all blade servers, look for other events in the log related to power and resolve those events. If the over voltage problem is occurring on all blade servers in the same power domain, the problem might be in one of the power modules that power that domain (log in to the advanced management module to see the power modules that are associated with each power domain). Replace the power modules, one at a time, to see if the problem is resolved.
   b. If no other blade server has this same problem, the issue is specific to the blade as a hardware or firmware problem. If the blade is still functioning the log can be ignored, but the blade should be monitored to see if the voltages get worse.
3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x80080000   absent

Explanation: The specified component on the specified blade server is either absent or present.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Blade bezel 1, cable (Front panel) absent

User response: Information only; no action is required.

0x80090000   disabled

Explanation: The service processor for the specified blade server has detected that the specified component or sensor type has been enabled or disabled.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

- System board, memory (Performance Mode) disabled

- System board, memory (Performance Mode) enabled

User response: If you disabled the device or sensor, no action is required. Otherwise, Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x800B0100 is not redundant

Explanation: Redundancy has been lost for the specified component on the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Memory device 0 (Bckup Mem Status) is not redundant
- Recovery Memory device 0 (Bckup Mem Status) is not redundant

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x800B0300 is not redundant and operational with minimal resources

Related messages:
- 0x800B0400 : is not redundant and operational with minimal resources

Explanation: The specified component on the specified blade server is not redundant,. However, it continues to function with the minimum resources required for normal operation.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Memory device 0 (Bckup Mem Status) is not redundant and operational with minimal resources

Alarm Panel LED (BC T and BC HT): Minor

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x800B0500 is not redundant and not operational

Explanation: The specified component on the specified blade server is not redundant and does not have sufficient resources available to maintain normal operation.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0007   internal error

Explanation: The CPU on the blade server has encountered an internal error.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 1 (CPU 1 Status) internal error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Check the IBM Support Web page for any service bulletins that might be related to this problem.
2. Restart the service processor for the specified blade server. You can restart the service processor from the advanced management module Web interface.
3. Reboot the blade server and press F1 to display the BIOS menu:
   a. Verify that both processors are being seen by BIOS.
   b. Load the default settings.
   c. Go to the advanced setup menu, select the CPU settings, and attempt to enable the CPU slot.
4. Swap processors on the blade server to determine if the problem is related to the CPU slot or the processor.

   Note: This step does not apply to JSxx blade servers.
5. Go to the IBM BladeCenter software and device drivers Web page for firmware updates.
6. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F0009   power off

Explanation: The service processor on the specified blade server has detected a power off or power on condition.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- System board (SysPwr Monitor) power off
- System board (Power Unit Stat) power on

User response: Information only; no action is required.

0x806F000D   removed

Related messages:

- 0x806F002C : removed

Explanation: The hot-swap hard disk drive for the specified blade server has been removed or replaced.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

- Hard drive 1 (Drive 1 Status) installed
- Hard drive 1 (Drive 1 Status) removed

User response: Information only; no action is required.

0x806F000F   error

Explanation: The service processor for the specified blade server has detected a system firmware error. The firmware will not be loaded.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

- FW/BIOS, firmware progress (Pri FW Corrupt) error
- FW/BIOS, firmware progress (ABR Status) error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Reboot the blade server.
2. Update the service processor firmware for the blade server through the advanced management module Web interface. Select Blade Tasks and then Firmware Update.
3. Reseat the blade server.
4. Update the system firmware for the blade server.
5. Replace the system board (trained service technician only).

0x806F0013   diagnostic interrupt

Explanation: The service processor for the specified blade server has detected a Non-Maskable Interrupt (NMI). This NMI was generated from a user request from the front panel of the blade server.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Chassis (NMI State) diagnostic interrupt

User response: Information only; no action is required.

0x806F001E   no bootable media

Explanation: Blade booting fails due to no bootable media.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F001F   boot completed

Related messages:
- 0x806F011F : boot completed
- 0x806F021F : boot completed
- 0x806F041F : boot completed

Explanation: The operating system for the specified blade server has completed the startup process.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0021   fault

Explanation: A fault was detected for the specified component in the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message:
- Expansion Card 1, connector (UIDC Diag) fault
- System board, connector (PCIe Status) fault
- FW/BIOS, connector (no Op ROM Space) fault

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine

0x806F0029 • 0x806F0107

the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If Problem relates to no Op ROM please refer to TIP H197144 and evaluate the use of UEFI boot mode to potentially eliminate, see uEFI white paper http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5089627

2. Reseat the specified component or connector (if the component has a socket).

3. Update the firmware for the specified component (if the component has firmware).

4. Replace the component or connector.

0x806F0029   low

Explanation: The battery for the specified blade server is low.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Battery 1 (Battery Status) low

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F002B   Hardware change detected

Explanation: The meaning of this event depends on the blade server that generates the event.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: cKVM (PSOC Mismatch) hardware changed detected

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0107   thermal trip

Explanation: The service processor has detected a thermal trip (overheating due to an overload).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 3 (CPU 3 Status) thermal trip

Chassis LED: Error, Temperature

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Check the room ambient temperature to ensure that it is within the operating specifications for the chassis.
2. If an air filter is installed, make sure that it is cleaned or replaced.
3. Make sure that all fan/blower modules are running. Replace fan modules if necessary.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that there is nothing covering the bays. Any missing components can cause a major reduction in airflow for the blade server.
5. Update the firmware for the advanced management module. You can find firmware on the IBM BladeCenter software and device drivers Web page.
6. Update the firmware for the blade server.
7. For all blade servers other than the JSxx blade servers, make sure the heat sink and CPU are secured on the system board.

   Note: Be careful when handling the heat sink and CPU, they may be extremely hot.
8. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F0108   failure

Explanation: A power failure has been detected for the specified component on the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message: Power Module 1 (VRD 1 Status) failure.

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Update the firmware for the service processor (BMC) and advanced management module, if applicable.
2. If there are failures for multiple blade servers, check the event log for power module failures and resolve those events.
3. Verify that you have a stable power input source.

0x806F0109   power cycle

Explanation: A blade server service processor detects that power to the blade server has been cycled.

Severity: Informational

Alert Category: Power On/Off (Informational) - mmTrapPwrDOS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: System board (SysPwr Monitor) power cycle.

User response: This is an informational event and no action is required, unless the cycling of power is unexplained. Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific

0x806F010C • 0x806F010F

actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F010C   uncorrectable ECC memory error

Explanation: An uncorrectable error has occurred on the specified DIMM (if provided) for the specified blade server. The system will reboot, and this DIMM will be disabled. Most likely, the DIMM will need to be replaced, but you should follow the steps in the User Response to be sure that this is the appropriate action.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message:
* Group 1 (All DIMMs) uncorrectable ECC memory error
* Group 1 (DIMM Group Status) uncorrectable ECC memory error
* Group 1 (DIMM Status) uncorrectable ECC memory error
* Group 1 (One of the DIMMs) uncorrectable ECC memory error
* Memory device 1 (DIMM 1 Status) uncorrectable ECC memory error
* Recovery Memory device 3 (DIMM 3 Status) uncorrectable ECC memory error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F010D   fault

Explanation: A fault has occurred for the specified hard disk drive for the specified blade server.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message: Hard drive 2 (SAS 2 Status) fault

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:
1. Replace the hard disk drive.
2. Check the IBM Support Web page for related service bulletins.
3. Update the associated firmware for the storage module, the blade server SAS expansion card options, the SAS I/O modules, and hard drives if applicable.

0x806F010F   hang

Explanation: The specified blade server has hung while loading BIOS.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: FW/BIOS, firmware progress (Pri FW Corrupt) hang

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:
1. Attempt to reboot the blade server.
2. Determine the type of blade server for which this error has occurred. You can find the blade server type from the advanced management module Hardware VPD information:
   a. From the advanced management module Web Interface, click Hardware VPD.
   b. From the command-line interface, enter the Info command).

0x806F0112   OEM system boot event

Explanation: The service processor for the specified blade server has detected a product-specific system boot event.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Processor 1 (CPU Fault Reboot) OEM system boot event
- Group 4 (CPU Fault Reboot) OEM system boot event

User response: Information only; no action is required. The Problem Determination and Service Guide for the specified blade server might have additional information about this event. The Problem Determination and Service Guide is available on the Web.

0x806F0113   bus timeout

Explanation: The service processor on the specified blade server has detected a bus timeout.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Chassis (NMI State) bus timeout

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:
1. Remove the blade server from the BladeCenter chassis; then, reinstall it.
2. Reseat all the options installed in the blade server one, restarting the blade server each time, at a time to determine where the problem is located.

0x806F011B • 0x806F0129

3. Remove options from the blade server one at a time to determine where the problem is located.
4. Replace the following components one at a time, in the order shown, restarting the blade server each time:
   a. All options installed in the blade server.
   b. System board assembly (trained service technician only).

0x806F011B   configuration error

Explanation: A cable plugged into the specified component on the specified blade server may be plugged incorrectly.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Expansion Card 2, cable (Switch Connect) configuration error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:
1. Make sure that you using the correct cable. Refer to the Problem Determination and Service Guide for the specified blade server type for more information about cabling. The Problem Determination and Service Guide is available on the Web.
2. Reseat the cable.

0x806F0120   run-time critical stop

Explanation: The service processor on detected an operating system run-time critical stop.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0129   failed

Explanation: The battery for the specified component on the specified blade server has failed.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Expansion Module 1, battery (BSE3 RAID BAT) failed

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Reseat the battery.
2. Replace the battery.

0x806F012B   software changed detected

Explanation: This event is issued when a software change is detected. For example, this event will be issued when UEFI starts an automatic ROM recovery.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: If this is a UEFI automatic ROM recovery software change, do not remove the blade or remove power from the chassis until an event is logged indicating the software update was successful or UEFI failed to boot. Refer to the Problem Determination and Service Guide for the specified blade server for more information. The Problem Determination and Service Guide is available on the Web.

0x806F0207   BIST failure

Explanation: The specified processor on the blade server has encountered a Built-In Self Test (BIST) failure.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 2 (CPU 2 Status) BIST failure.

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Reboot the blade server.
2. Make sure the heat sink and CPU are secured on the system board.

   Note: Be careful when handling the heat sink and CPU, they may be extremely hot.
3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F0208   predictive failure

Explanation: The service processor detected a predictive failure for the specified component. Although the component has not yet failed, it might do so soon.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

0x806F020D • 0x806F0212

Automatically notify service: No

Recoverable: Yes

Example Message:
- Hard drive 2 (Drive 2 Status) predictive failure
- Power Module 1 (VRD 1 Status) predictive failure

Alarm Panel LED (BC T and BC HT): Minor

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F020D drive predictive failure

Explanation: The service processor detected a predictive failure for the specified component. Although the component has not yet failed, it might do so soon.

Severity: Warning

Alert Category: Blades (Warning) - mmTrapBladeN

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message:
- Hard drive 2 (Drive 2 Status) predictive failure
- Power Module 1 (VRD 1 Status) predictive failure

Alarm Panel LED (BC T and BC HT): Minor

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F020F   progress

Explanation: The service processor has detected that the specified firmware is in the process of being started (such as when a device is being initialized).

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: FW/BIOS, firmware progress (Progress) progress

User response: Information only; no action is required.

0x806F0212   system hardware failure

Explanation: The service processor on the specified blade server has determined that a system hardware failure has occurred during the specified system event.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message: Processor 1 (CPU 1 Halted) system hardware failure

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0229   absent

Explanation: The battery for the specified component on the specified blade server is absent or present.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Battery 1 (Battery Status) absent

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F030C   memory scrub failed

Explanation: Memory scrub operation failed.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message: Memory device 12 (DIMM 12 Status) memory scrub failed

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0313   software NMI

Explanation: The service processor has detected a software Non-Maskable Interrupt (NMI).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Chassis (NMI State) software NMI

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F032B • 0x806F0407

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Check the operating system event log for any related errors and resolve those errors. If you cannot resolve those errors, contact the appropriate service provider for the software.

2. Check the application log for any related errors and resolve those errors. If you cannot resolve those errors, contact the appropriate service provider for the software.

3. If the problem persists, check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F032B   software incompatibility

Explanation: Software for the specified component has been changed, and the change is not valid.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Firmware (PSOC Mismatch) software incompatibility

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0407   initialization failure

Explanation: The specified processor on the specified blade server has failed to initialize.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 2 (CPU 2 Status) initialization failure

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Restart the service processor for the specified blade server. You can restart the service processor from the advanced management module Web interface.

2. Reboot the blade server and press F1 to display the Setup Utility:

   a. Verify that both processors are being seen by the system firmware.

   b. Load the default settings.

   c. Go to the advanced setup menu, select the CPU settings, and attempt to reenable the CPU slot.

3. Swap processors on the blade server to determine if the problem is related to the CPU slot or the processor.

   Note: This step does not apply to JSxx blade servers.

4. Go to the IBM BladeCenter software and device drivers Web page for firmware updates.

5. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F0409   AC lost

Explanation: The service processor for the specified blade server had detected a loss of AC power for the specified component.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: System board (Power Unit Stat) AC lost

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Inspect the blade servers to make sure that they are all running as expected.
2. Verify that the AC LED is lit on all power modules.
3. Look for other power module events (such as over current or over temperature events) in the event log and resolve them.
4. Reseat the blade server.

0x806F040C   memory disabled

Explanation: The specified DIMM for the specified blade server has been disabled. This is a result of a previous uncorrectable memory error.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

* Group 1 (All DIMMs) memory disabled
* Group 1 (One of the DIMMs) memory disabled
* Memory device 1 (DIMM 1 Status) memory disabled

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0413   PCI parity error

Explanation: The service processor on the specified blade server has detected a PCI parity error for the specified component. The blade server will reboot.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:

0x806F0507 • 0x806F0509

- System board (PCI Error) PCI parity error
- System board (Critical Int) PCI parity error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If you have a PCI adapter in your blade server:
   a. Verify that the PCI adapter is supported in the blade server. See the IBM ServerProven Web site to determine which PCI adapters are supported.
   b. Reseat the PCI adapter.
2. Refer to the Problem Determination and Service Guide for the specified blade server for information related to PCI adapters. You can find the Problem Determination and Service Guide on the Web.
3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F0507   configuration error

Explanation: The specified processor on the specified blade server has a configuration error due to a possible hardware incompatibility (for example, the processors may be running at different speeds).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 1 (CPU 1 Status) configuration error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0509   power unit did not respond to power on request

Explanation: The service processor on the specified blade server has detected a soft power control failure (the blade server did not respond to a power no request).

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: System board (Sys pwr monitor) power unit did not respond to power on request

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. From the advanced management module, use the Power Management page to ensure that there is sufficient power budget to enable this blade server to power on.
2. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F050C   correctable ECC memory error logging limit reached

Explanation: The correctable Error Correction Code (ECC) memory error logging threshold for the specified blade server was reached. The system will continue to run. Refer to the steps in the user response before replacing a DIMM.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message:
- Group 1 (All DIMMs) correctable ECC memory error logging limit reached
- Group 1 (DIMM Group Status) correctable ECC memory error logging limit reached
- Group 1 (DIMM Status) correctable ECC memory error logging limit reached
- Group 1 (One of the DIMMs) correctable ECC memory error logging limit reached
- Memory device 1 (DIMM 1 Status) correctable ECC memory error logging limit reached
- Recovery Memory device 1 (DIMM 1 Status) correctable ECC memory error logging limit reached

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F050D   in critical array

Explanation: The service processor on the specified blade server detected a problem with one of the hard disk drives in a RAID array, placing the array in a critical state. The loss of another hard disk drive in the array could cause the array to fail.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Hard drive 1 (Drive 1 Status) in critical array

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0513   PCI system error

Explanation: The service processor on the specified blade server has detected a PCI system error for the specified component. The blade server will reboot.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

0x806F0521 • 0x806F052B

Example Message:

- System board (Critical Int) PCI system error
- System board (PCI Error) PCI system error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If you have a PCI adapter in your blade server:
   a. Verify that the PCI adapter is supported in the blade server (go to the IBM ServerProven Web site).
   b. Reseat the PCI adapter.
2. Refer to the Problem Determination and Service Guide for the specified blade server for information related to PCI adapters. You can find the Problem Determination and Service Guide on the Web.
3. Check the IBM Support Web page for any service bulletins that might be related to this problem.

0x806F0521   power is off

Explanation: The meaning of this message is specific to the blade server that generated the event. The event is not recorded in the advanced management module event log. If configured for alert notifications, the message can be seen in SNMP traps and is forwarded to IBM Systems Director.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Expansion Card 1, connector (UIDC Diag) power is off

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F052B   unsupported software version

Explanation: BMC detects that certain entity contains an invalid or unsupported FW or SW version.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Firmware (PSOC Mismatch) unsupported software version

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0607   SM BIOS uncorrectable error

Explanation: The service processor on the specified blade server detected a system management BIOS error, and the error cannot be corrected.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: Processor 1 (CPU 1 Status) SM BIOS uncorrectable error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Check the BIOS auxiliary log (if it exists) and resolve any issues specified. You can find information about the BIOS auxiliary log, if it exists, in the Problem Determination and Service Guide and the User's Guide for the specified blade server type.
2. Reboot the blade server.
3. Reseat all option cards.
4. Update the firmware for the option cards and expansion board, if they exist.
5. Update the BIOS firmware for the blade server. Firmware is available at the IBM BladeCenter software and device drivers Web site.
6. Replace the specified component.

0x806F0609   power unit failure

Explanation: The system board power unit for the specified blade server has failed.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message: System board (Sys pwr monitor) power unit failure

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. Reseat the blade server.
2. Replace the system board (trained service technician only).

0x806F060C   memory absent

Explanation: The specified memory device is either present or absent.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

0x806F060D • 0x806F0707

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Memory device 1 (DIMM 1 Status) memory absent
- Memory device 1 (DIMM 1 Status) memory present

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F060D   in failed array

Explanation: The service processor on the specified blade server has detected a problem with one or more hard disk drives in a RAID array, resulting in a failure of the RAID array.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message: Hard drive 1 (Drive 1 Status) in failed array

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:

1. If the RAID array is external to the blade, verify that the array has power.
2. Go to the interface for your RAID management implementation and resolve any problems that are found. If hard disk drives are bad, note the part number and size of the hard disk drives for replacement.

0x806F0707   absent

Explanation: The specified processor on the specified blade server is either absent or present.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Processor 1 (CPU 1 Status) absent
- Processor 1 (CPU 1 Status) present

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F070C   memory configuration error

Explanation: The memory configuration for the specified blade server is not valid.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Group 1 (All DIMMs) memory configuration error
- Group 1 (DIMM Group Status) memory configuration error
- Group 1 (DIMM Status) memory configuration error
- Group 1 (One of the DIMMs) memory configuration error
- Memory device 1 (DIMM 1 Status) memory configuration error

Alarm Panel LED (BC T and BC HT):   Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F070D   rebuild in progress

Explanation: The specified hard drive is in the process of being rebuilt.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Hard drive 1 (Drive 1 Status) rebuild in progress

User response: Information only; no action is required.

0x806F0807   disabled

Explanation: The specified processor on the specified blade server has been enabled or disabled.

Severity: Informational

Alert Category: Blades (Informational) - mmTrapBladeS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message:
- Group 4, processor (One of CPUs) disabled
- Group 4, processor (all CPUs) enabled
- Processor 1 (CPU 1 Status) disabled
- Processor 1 (CPU 1 Status) enabled

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine

0x806F0813 • 0x806F0A13

the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0813   bus uncorrectable error

Explanation: The service processor on the specified blade server has detected a bus error for the specified component, and the error cannot be corrected.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: Yes

Recoverable: Yes

Example Message:
- System board (Critical Int) bus uncorrectable error
- Group 1 (Critical Int) bus uncorrectable error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

If you do not have access to the Problem Determination and Service Guide, perform these steps:
1. Update the firmware for the service processor (BMC), BIOS, and firmware for the advanced management module.
2. Reseat the memory DIMMs and any expansion cards.
3. Check ServeRAID-MR10ie Backup Battery Cable (p/n: 46C7172) to see if it is damaged or poorly connected to the ServeRAID-MR10ie Controller or ServeRAID-MR10ie Backup Battery.
4. Replace the system board (trained service technician only).

0x806F0A07   Blade CPU Auto Throttle

Explanation: Processor or memory in the blade has auto throttled.

Severity: Informational

Alert Category: N/A - mmTrapRemoteLoginS

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

0x806F0A13   fatal bus error

Explanation: The service processor on the specified blade server has detected an fatal bus error for the specified component.

Severity: Error

Alert Category: Blades (Critical) - mmTrapBladeC

Log Source: Blade_##

Automatically notify service: No

Recoverable: Yes

Example Message: System board (Critical Int) fatal bus error

Alarm Panel LED (BC T and BC HT): Critical

User response: Refer to the Problem Determination and Service Guide for the specified blade server to determine the device-specific actions to resolve this event. The Problem Determination and Service Guide is available on the Web.

Appendix. I2C buses in a BladeCenter chassis

The tables in this section provide additional information to help you resolve events 0x00020000 - 0x00020036. For each chassis type, these tables lists the I2C buses and the device or devices on that bus.

Redundant I2C buses are used to communicate between the management module and the media tray, blowers, power modules, and I/O switch modules. When the management module cannot communicate with a device, it generates an event in the event log that provides the device number on the bus.

Each BladeCenter chassis has a different number of I2C devices; therefore, the meaning of the event is specific to a chassis type. In some cases, there is a specific device on the bus. For example, bus 10 on a BladeCenter H chassis is I/O Module 1. In other cases, a group of devices are on a bus. For example, multiple I/O modules are on bus 5 on a BladeCenter E chassis.

Note: It takes from two to five minutes for the I2C bus to reset itself and clear any faults. Keep this time frame in mind when resetting or adding devices for the I2C bus.

I2C buses in a BladeCenter E or BladeCenter T chassis

This table provides the devices for each of the buses in a BladeCenter E or BladeCenter T chassis.

Table 3. Buses in a BladeCenter E or BladeCenter T chassis

Bus	Device
0	Advanced management module (internal)
1	Local advanced management module (internal)
2	Chassis presence detection
3	Power modules and blowers
4	Media tray
5	I/O modules

I2C buses in a BladeCenter H chassis

This table provides the devices for each of the buses in a BladeCenter H chassis.

Table 4. Buses in a BladeCenter H chassis

Bus	Device
0	Advanced management module (internal)
1	Local advanced management module (internal)
2	Not used
3	Not used
4	Not used
5	External buses 6-9 (Chassis)
6	Chassis presence detection
7	Media tray
8	External buses 10-17 (I/0 modules)
9	External buses 18-25 (Power, Blower, Bridge)

Table 4. Buses in a BladeCenter H chassis (continued)

Bus	Device
10	I/O module 1
11	I/O module 2
12	I/O module 3
13	I/O module 4
14	I/O module 7 (HSS 1)
15	I/O module 8 (HSS 2)
16	I/O module 9 (HSS 3)
17	I/O module 10 (HSS 4)
18	Power module 1
19	Power module 2
20	Power module 3
21	Power module 4
22	Blower 1
22	Blower 2
24	I/O module 5 (Bridge 1)
25	I/O module 6 (Bridge 2)

I2C buses in a BladeCenter HT chassis

This table provides the devices for each of the buses in a BladeCenter HT chassis.

Table 5. Buses in a BladeCenter HT chassis

Bus	Device
0	Advanced management module (internal)
1	Local advanced management module (internal)
2	Not used
3	Not used
4	Not used
5	External buses 6-13 (Chassis)
6	Chassis presence detection
7	Media tray
8	External buses 14-21 (I/0 modules)
9	External buses 22-25 (Power)
10	External buses 26–29 (Fans)
11	External buses 30–31 (Clocks)
12	Presence Detection (network, Media Tray)
13	Not used
14	I/O module 1
15	I/O module 2
16	I/O module 3
17	I/O module 4

Table 5. Buses in a BladeCenter HT chassis (continued)

Bus	Device
18	I/O module (HSS 1)
19	I/O module (HSS 2)
20	I/O module (HSS 3)
21	I/O module (HSS 4)
22	Power module 1
22	Power module 2
24	Power module 3
25	Power module 4
26	External Buses 32-33 (Fan 1)
27	External Buses 34-35 (Fan 2)
28	External Buses 36-37 (Fan 3)
29	External Buses 38-39 (Fan 4)
30	Clock 1
31	Clock 2
32	Fan 1
33	Fan 1
34	Fan 2
35	Fan 2
36	Fan 3
37	Fan 3
38	Fan 4
39	Fan 4

I2C buses in a BladeCenter S chassis

This table provides the devices for each of the buses in a BladeCenter S chassis.

Table 6. Buses in a BladeCenter S chassis

Bus	Device
0	Advanced management module (internal)
1	Local advanced management module (internal)
2	Not used
3	Not used
4	Not used
5	External buses 6-9 (Chassis)
6	Chassis presence detection
7	Media tray
8	External buses 10-17
9	External buses 18-25
10	I/O module 1
11	I/O module 2

Table 6. Buses in a BladeCenter S chassis (continued)

Bus	Device
12	I/O module 3 (SAS)
13	I/O module 4 (SAS)
14	Power module 1
15	Power module 2
16	Storage module 1
17	Not used
18	Fan 1
19	Fan 2
20	Fan 3
21	Fan 4
22	Power module 3
22	Power module 4
24	Storage module 2

IBM ®

Part Number: 00KC263

Printed in USA