IBM Director 4.1 Events Reference

Document Number: SC01-R054-20
Part Number: 01R0542

Note:

Before using this information and the product it supports, read the general information in Appendix F, “Notices”, on page 211.

First Edition (June 2003)

Contents

Figures

Tables

Preface

This book provides information about IBM® Director 4.1 events. Depending on the event, this information can include:

- Event type
- Description
- Severity
- Whether it is an alert or resolution
- Extended attributes
- Whether it is new for IBM Director 4.1

This book also provides planning and implementation information for event management.

How this book is organized

Chapter 1, “Introduction”, on page 18 contains an overview of events and event action plans in IBM Director.

Chapter 2, “Event management”, on page 30 contains information about planning, designing, and building event action plan implementations.

Chapter 3, “Active PCI Manager events”, on page 49 contains information about the Active™ PCI Manager events.

Chapter 4, “Alert Standard Format (ASF) events”, on page 52 contains information about the Alert Standard Format (ASF) events.

Chapter 5, “BladeCenter Assistant events”, on page 58 contains information about the BladeCenter® Assistant events.

Chapter 6, “Capacity Manager events”, on page 60 contains information about the Capacity Manager events.

Chapter 7, “Common Information Model (CIM) events”, on page 62 contains information about the Common Information Model (CIM) events.

Chapter 8, “IBM Director events”, on page 71 contains information about IBM Director events.

Chapter 9, “Mass Configuration events”, on page 81 contains information about Mass Configuration events.

Chapter 10, “Management Processor Assistant (MPA) events”, on page 82 contains information about the Management Processor Assistant events.

Chapter 11, “SNMP events”, on page 109 contains information about IBM Director-specific SNMP events.

Chapter 12, “Software Rejuvenation events”, on page 111 contains information about Software Rejuvenation events.

Appendix A, “SNMP information”, on page 119 contains information that is helpful for working with SNMP devices and upward integration modules (UIMs).

Appendix B, “CIM events”, on page 192 contains information for working with the CIM events.

Appendix C, “IBM Director Agent events found in the Windows event log”, on page 196 contains information about the events found in the Microsoft® Windows® event log.

Appendix D, “Terminology summary and abbreviation list”, on page 203, contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

Appendix E, “Getting help and technical assistance”, on page 209, contains information about accessing IBM Support Web sites for help and technical assistance.

Appendix F, “Notices”, on page 211, contains product notices and trademarks.

The “Glossary” on page 214 provides definitions for terms used in IBM Director publications.

Notices that are used in this book

This book contains the following notice designed to highlight key information:

- **Notes**: These notices provide important tips guidance or advice.
- **Important**: These notices provide information or advice that might help you avoid inconvenient or difficult situations.
- **Attention**: These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.

IBM Director publications

The following publications are available in Portable Document Format (PDF) from the IBM Support Web site:

- *IBM Director 4.1 Installation and Configuration Guide* (dir41_install.pdf)
- *IBM Director 4.1 Systems Management Guide* (dir41_sysmgt.pdf)
- *IBM Director 4.1 Events Reference* (dir41_events.pdf)
- *IBM Director 4.1 Upward Integration Modules Installation Guide* (dir41_uim.pdf)

Check this Web site regularly for new or updated IBM Director publications. For additional information about downloading materials from the IBM Support Web site, see “IBM Director resources on the World Wide Web” on page 15.

For planning purposes, the following IBM xSeries™ publications might be of interest:

- *IBM @server BladeCenter Type 8677 Planning and Installation Guide*
- *Advanced System Management PCI Adapter, Software User’s Guide*
- *Advanced System Management PCI Adapter, Installation Instructions*
- *Remote Supervisor Adapter, User’s Guide*
- *Remote Supervisor Adapter, Installation Guide*
- *Remote Supervisor Adapter II, User’s Guide*
- *Remote Supervisor Adapter II, Installation Guide*

For the integrated system management processor (ISMP), see the documentation that came with the server. You can obtain these publications from the IBM Support Web site.

In addition, the following IBM Redbooks™ publications might be of interest:

- *Implementing Systems Management Solutions using IBM Director* (SG24-6188)
- *IBM @server BladeCenter Systems Management* (REDP3582)
- *The Cutting Edge: IBM @server BladeCenter* (REDP3581)
- *IBM @server xSeries 440 Planning and Installation Guide* (SG24-6196)
- *Server Consolidation with the IBM @server xSeries 440 and VMware ESX Server* (SG24-6852)
- *Managing IBM TotalStorage NAS with IBM Director* (SG24-6830)
- *IBM Director Security* (REDPO417)
- *Integrating IBM Director with Enterprise Management Solutions* (SG24-5388)
- *Using Active PCI Manager* (REDP0446)
- *Implementing Asset ID* (SG24-6165)

You can download these books from the IBM Web site at http://www.ibm.com/redbooks/.

Note: Some of the Redbooks publications contain outdated information. Be sure to note the date of publication and to determine the level of IBM Director software to which the Redbooks publication refers.

IBM Director resources on the World Wide Web

The following Web pages provide resources for understanding, using, and troubleshooting IBM Director and systems-management tools.

IBM Online Assistant and e-Mail

http://www.ibm.com/pc/qtechinfo/MIGR-4Z7HJX.html

This Web page offers a quick resource to help solve your technical questions. Follow the instructions on this page to find additional solutions for your systems-management tools.

If you do not find an acceptable solution, or if you just want to bypass looking for your own solution, you can submit an electronic question. From any page within the IBM Online Assistant, click **None of the above** to submit an electronic inquiry. Response times vary between 24 and 48 hours.

IBM Universal Manageability Discussion Forum
http://www7.pc.ibm.com/~ums/

IBM forums put you in contact with other IBM customers. The forums are monitored by IBM technicians.

IBM Systems Management Software: Download/Electronic Support page
http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html

Use this Web page to download IBM systems-management software, including IBM Director.

IBM xSeries Systems Management page
http://www.ibm.com/pc/ww/eserver/xseries/systems_management/index.html

This Web page presents an overview of IBM systems management and IBM Director. Click **IBM Director 4.1** for the latest information and publications.

IBM Universal Manageability page
http://www.ibm.com/pc/us/pc/um/index.html

This Web page links to an IBM portfolio of advanced management tools that help lower costs and increase availability throughout the life cycle of a product.

IBM ServerProven® page
http://www.ibm.com/pc/us/compat/index.html

This Web page provides information about IBM hardware compatibility, as well as supported operating systems.

IBM Director Agent page
http://www.ibm.com/pc/ww/eserver/xseries/systems_management/nfdir/agent.html

This Web page includes the compatibility document for IBM Director 4.1. It lists all the supported operating systems and is updated every 6 to 8 weeks.

IBM Support page

http://www.ibm.com/pc/support/

This is the IBM Support Web site for IBM hardware and systems-management software. For systems-management software support, click **Systems management**.

Chapter 1. Introduction

This Events Reference is for system administrators that want to create IBM Director event action plans so they can be notified of events that they consider important in their systems-management environment.

Note: If you are new to IBM Director, read the *IBM Director 4.1 Systems Management Guide* first. If you are not familiar with IBM Director terminology, be sure to read Appendix D, “Terminology summary and abbreviation list”, on page 203.

This chapter provides an introduction to events, alerts, and event action plans, as well as the basics of setting up an event action plan in the Event Action Plan Builder. If you are familiar with this information, continue to Chapter 2, “Event management”, on page 30 for detailed information about planning, designing, and implementing event action plans. If you already understand these concepts, use the remaining chapters in this book as a reference to available events, their descriptions and severity, and other information, such as any extended attributes, that you use when creating your event action plans.

Note: Starting with Chapter 3, “Active PCI Manager events”, on page 49, each chapter represents a top-level node, or root option, in the tree that is displayed on the Event Type page of the “Event Filter Builder” window.

If you are not using IBM Director, but are using an IBM Director 4.1 Upward Integration Module (UIM) with other systems-management enterprise software, Appendix A, “SNMP information”, on page 119 provides useful information about events in a UIM implementation.

Events and alerts

Understanding the difference between an event and an alert is important. An event is an occurrence of a predefined (in IBM Director) condition relating to a specific managed object. An alert, on the other hand, notifies you of an event occurrence and relates specifically to an event action plan. That is, if an event action plan is configured to filter a specific event, when that event occurs an alert is generated in response to that event.

Event action plans

By creating event action plans and applying them to specific managed systems, you can be notified by e-mail or pager, for example, when a specified threshold is reached or a specified event occurs. Or, you can configure an event action plan to start a program on a managed system and change a managed system variable when a specific event occurs. You can use process-monitor events and resource-monitor events to build an event action plan. For more information see, Chapter 8, “IBM Director events”, on page 71.

Successful implementation of event action plans requires planning and consideration of how you will implement them. In particular, developing and following strict naming conventions is important, so you can easily identify what a specific plan does. For more tips on creating event action plans, see Chapter 2, “Event management”, on page 30.

The following steps are an overview for implementing an event action plan:

1. Create a new event action plan.
2. Create an event filter or filters.
3. Customize an event action or actions.
4. Assign the event filter or filters and event action or actions to the new event action plan.
5. Activate the event action plan by applying it to a single managed system, more than one managed system, or a group.

Note: When you first start IBM Director, the Event Action Plan wizard opens. You can use this wizard to create an event action plan also. See the *IBM Director 4.1 Installation and Configuration Guide* for more information.

Implementing an event action plan

Complete the following steps to implement an event action plan:

1. In IBM Director Console, click **Tasks** → **Event Action Plan Builder**. The “Event Action Plan Builder” window opens.

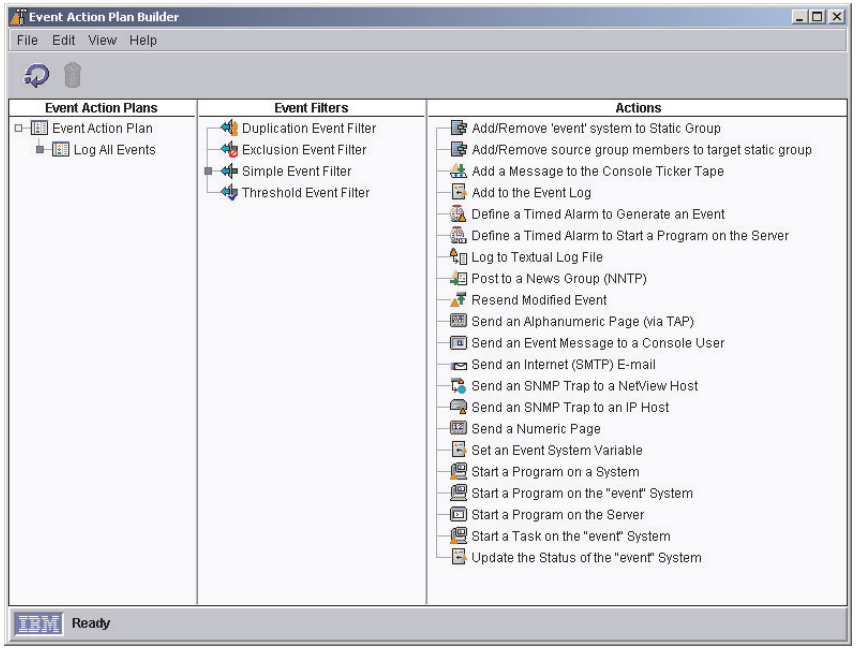

Figure 1. "Event Action Plan Builder" window

The Event Action Plan Builder interface contains three panes:

Event Action Plans pane

Lists event action plans. One default event action plan, Log All Events, is included with IBM Director. Also, if you used the Event Action Plan wizard to create an event action plan, that plan is listed.

Event Filters pane

Lists event filter types, with customized filters displayed under the applicable filter types. Expanding the Simple Event Filter tree displays, in addition to any customized simple event filters created, the preconfigured event type filters, such as Hardware Predictive Failure Events, and the preconfigured event severity event types, such as Critical Events. The preconfigured event filters are read only. Using one of these preconfigured event filters ensures that the correct event type or severity is preselected.

Actions pane
Lists event action types, with customized actions displayed under the event action types.

2. In the Event Action Plans pane, right-click **Event Action Plan**; then, click **New**. The “Create Event Action Plan” window opens.
3. Type a name for the plan and click **OK** to save it. The event action plan is displayed in the Event Action Plans pane.
4. In the Event Filters pane, double-click an event filter type:

   Simple Event Filter
   This is a general-purpose filter. Expanding this tree displays, in addition to any customized simple event filters created, the preconfigured, read-only event filters, such as Hardware Predictive Failure Events and Critical Events. Using one of these pre-configured event filters ensures that the correct event type or event severity is preselected.

   Duplication Event Filter
   Ignores duplicate events, in addition to the simple event filter options.

   Exclusion Event Filter
   Excludes certain event types, in addition to the simple event filter options.

   Threshold Event Filter
   Meets a specified interval or count threshold, in addition to the simple event filter options.

   Alternatively, you can create an event filter for an event that has already occurred. In the IBM Director Tasks pane, double-click the **Event Log** task. In the Events pane, right-click an event; then, click **Create** and select one of the four event filter types.

   The applicable “Event Filter Builder” window opens.

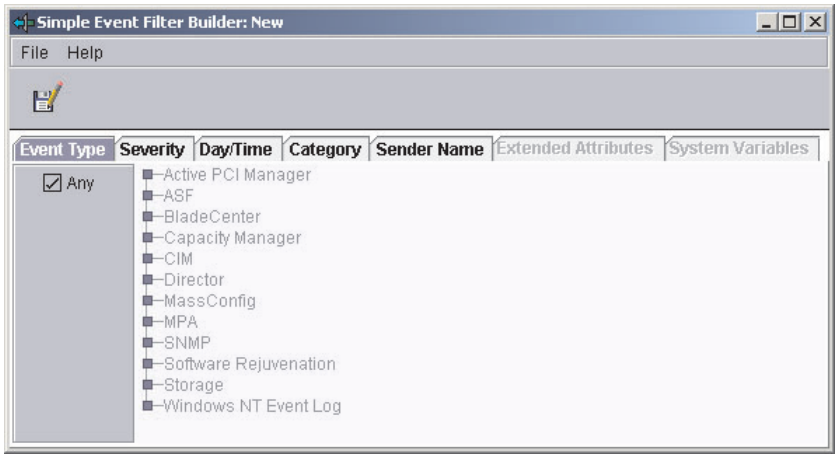

Figure 2. "Simple Event Filter Builder" window

5. Depending on the event filter type that you selected, the "Event Filter Builder" window contains different tabs. The following tabs are displayed for all event filters:

   Event Type
   Specifies the source or sources of the events to be processed. This list is created dynamically; entries are added by tasks and as new alerts are received. The event types for BladeCenter hardware-specific events are found under **MPA**, and BladeCenter Assistant-specific events are found under **BladeCenter**.

   Severity
   Specifies the urgency of events that are received.

   Day/Time
   Specifies days and times that the filter is set to ignore or accept events.

   Category
   Specifies the status of an event (alert or resolution) as a filtering criteria.

   Sender Name
   Specifies the managed system to which the filter applies.

Extended Attributes

Qualifies the filtering criteria using additional keywords and keyword values you can associate with some categories of events, such as SNMP.

System Variables

Specifies user-defined pairings of a keyword and value that are known only to the local management server. The **System Variables** tab is available only if one or more system variables exist. See “Viewing and changing system variables” on page 26 for more information.

By default, the **Any** check box is selected for all filtering categories, indicating that no filtering criteria apply.

Complete the fields as appropriate for the event filter you want to create.

6. Click **File** → **Save As**. The “Save Event Filter” window opens.
7. Name the filter and click **OK** to save the filter. The new filter is displayed in the Event Filters pane under the applicable filter type.
8. (Optional) You can create additional event filters for use in a single event action plan. Repeat step 4 on page 21 through step 7.
9. In the Actions pane of the Event Action Plan Builder, double-click an event action type. The “Customize Action” window opens. The example shown in Figure 3 on page 24 is for ticker-tape alerts.

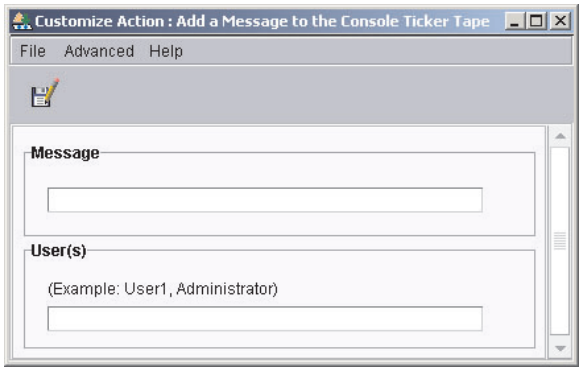

Figure 3. "Customize Action" window for ticker-tape alert

10. Complete the fields for the action type. You can use event data substitution variables to provide specific event information (see "Event data substitution variables" on page 46 for more information).
11. Click **File** → **Save As**. The "Save Event Action" window opens.
12. Name the action and click **OK** to save the action. The new action is displayed in the Actions pane under the applicable action type.
13. (Optional) Test the event action to verify that it works as you intended. For example, you can create a message using the Add a Message to the Console Ticker Tape action type and specify * in the **User** field to indicate all users. When you test this action, the ticker tape displays the message on your IBM Director Console.

    Complete the following steps to test an event action:

    a. Locate the event action under the corresponding event action type in the Actions pane of the "Event Action Plan Builder" window.
    b. Right-click the event action, then click **Test**. The action occurs.
14. (Optional) You can customize additional event actions for use in a single event action plan. Repeat step 9 on page 23 through step 13.
15. In the Event Filters pane, drag the event filter onto the event action plan (located in the Event Action Plans pane) that you created in steps 2 through 3 on page 21. The event filter is displayed under the event action plan.

16. If you have created additional event filters you want to use in this event action plan, repeat step 15 on page 24.
17. From the Actions pane, drag the event action onto the applicable event filter in the Event Action Plans pane. The event action is displayed under the event filter.
18. If you have created additional event actions you want to use in this event action plan, repeat step 17.

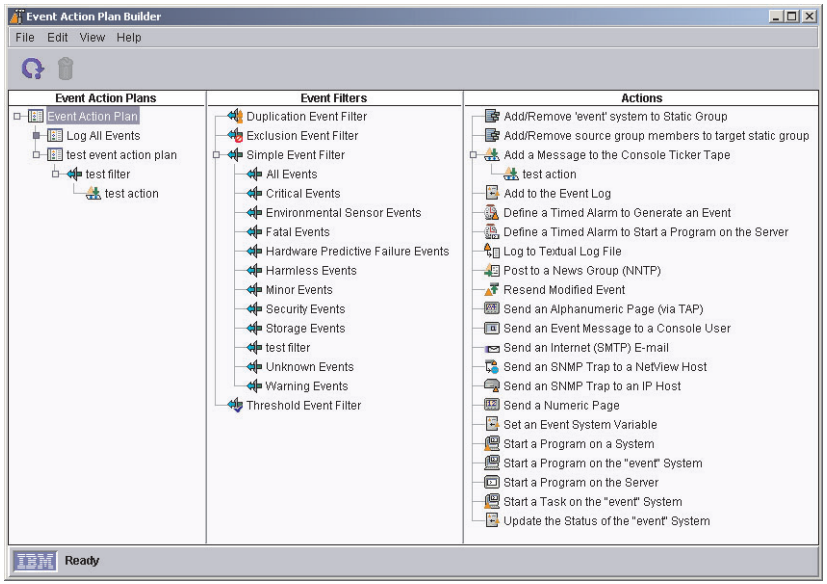

Figure 4. Example of an event action plan with an event filter and event action assigned to it

Click **File** → **Close** to close the Event Action Plan Builder.

19. In the IBM Director Console Tasks pane, expand the **Event Action Plan** task. The event action plan you created is displayed in the Event Action Plan tree.
20. Drag the event action plan from the Tasks pane onto the appropriate managed system or systems, or managed group. A confirmation message is displayed indicating that you have successfully applied the event action plan to the target system or group.

Viewing and changing system variables

You can use system variables in an event action plan to help you test and track the status of network resources. For example, you can create an event action plan that has:

- An event filter for an SNMP event that indicates network congestion
- An event action of Set Event System Variable, where you have specified:
  - `NetStatus` in the **Variable Name** field
  - `Congested` in the **New Value** field
  - `Normal` in the **Value to Reset to if Server is Restarted** field
  - `10` in the **Time until Automatic Value Reset** field

Then, if 10 seconds elapse before IBM Director Server receives the event that triggers this event action or before the management server stops and restarts, the NetStatus system variable is reset to Normal. You can reference system variable names and values wherever event data substitution is allowed. See “System Variables page” on page 40 for more information about system variables and how they can be used in event action plans.

To set a system variable, you must use the Set Event System Variable event action. However, in the Event Action Plan Builder, you can view existing system variables and their values by clicking **View** → **System Variables**. The “View System Variables” window opens. To change the value of an existing system variable, click the system variable. In the **Value** field, type the new value and click **Update**.

Enabling and viewing an event action history

By default, the event action history is disabled. To enable the event action history, in the Event Action Plan Builder Actions pane, right-click the customized event action and click **Enable**. Then, to view the event action history, right-click the event action again and click **Show**.

Viewing event action plan associations

You can view which event action plans are applied to which managed systems and groups. In IBM Director Console, click **Associations** → **Event Action Plans**. If a managed system or group has an event action plan assigned to it, you can expand the managed system or group and expand the Event Action Plan folder to view the specific event action plans that are applied to the managed system or group.

To view which managed systems have an event action plan applied to them, click **All Systems and Devices** in the Groups pane. If a managed system has an event action plan applied to it, you can expand the managed system in the Group Contents pane and expand the Event Action Plan folder to view the plans applied to the managed system.

To view which groups have event action plans applied to them, click **All Groups** in the Groups pane. If a group has an event action plan applied to it, you can expand the group in the Group Category Contents pane and expand the Event Action Plan folder to view the plans applied to the group.

Restricting event action plans

You can restrict whether an event action plan applies to both events received by all managed systems in a group and events received by one or more managed system in the group, or just the events received by all managed systems in the group. If an event action plan is restricted, all managed systems in a group to which the plan is applied must receive the event for the event action to occur. The default setting is unrestricted.

Complete the following steps to restrict an event action plan:

1. In IBM Director Console, click **Associations** → **Event Action Plans**.
2. Expand the tree for the managed system or group that has the event action plan you want to restrict applied to it.
3. Right-click the event action plan and click **Restricted**.

Exporting event action plans

With the Event Action Plan Builder, you can import and export event action plans to files. You can export event action plans from IBM Director Server to three types of files:

Archive
: Copies the selected event action plan to a file that you can import to any IBM Director Server.

HTML
: Creates a detailed listing of the selected event action plans, including their filters and actions, in an HTML format.

XML

Creates a detailed listing of the selected event action plans, including their filters and actions, in an XML format.

You would want to import and export event action plans in archive format generally for two reasons:

- To move event action plans from one IBM Director Server to another
- To back up event action plans on an IBM Director Server

Complete the following steps to export an event action plan:

1. In IBM Director Console, click **Tasks** → **Event Action Plan Builder**. The “Event Action Plan Builder” window opens.
2. In the Event Action Plan pane, click the event action plan you want to export.
3. Click **File** → **Export**, and select the type of file to which you want to export. Depending on which type of file you chose, the applicable window opens (for example, if you chose `Archive`, the “Select Archive File for Export” window opens).
4. Type a file name and, if necessary, change the location where you want to save the file. Click **OK** to export.

Importing event action plans

You can import event action plans from an Archive export of an event action plan from another IBM Director Server.

Complete the following steps to import an event action plan:

1. Transfer the archive file that you want to import to a drive on the management server.
2. In IBM Director Console, click **Tasks** → **Event Action Plan Builder**. The “Event Action Plan Builder” window opens.
3. Click **File** → **Import** → **Archive**. The “Select File for Import” window opens.
4. Select the archive file from step 1.
5. Click **OK** to begin the import process. The “Import Action Plan” window opens, displaying the event action plan to import.

6. Click **Import** to complete the import process. If the event action plan had previously been assigned to managed systems or groups, you have the option to preserve those assignments during the import process.

Chapter 2. Event management

One way to manage events is through event action plans. You can use event action plans to specify actions that occur as a result of events generated by a managed system. Event action plans are composed of two components:

- One or more event filters, which specify an event type and any related parameters
- One or more event actions, which occur in response to a filtered event

You can apply an event action plan to an individual managed system, several managed systems, or a group of managed systems.

Events can be generated from sources other than IBM Director Agent, such as the Microsoft Windows event log or Windows Management Instrumentation (WMI). You can use these events when working with managed objects. To monitor these events, you must create an event filter that contains an event type from one of these sources, use it as part of an event action plan and then apply the event action plan to a managed object. Events from the Windows event log or WMI are displayed under the Windows event log and Common Information Model (CIM) trees respectively on the Event Type Filter Builder.

When you create an event filter using an event from the Windows event log or CIM tree and apply it to a managed object as part of an event action plan, a process occurs on the managed node, twgescli.exe, and subscribes to the event type that translates the specific event type. This translates to an IBM Director event type, and then forwards it to the management server from which the event action plan was applied.

It is useful to understand how a typical event message flows through IBM Director. A basic understanding of this process will help you build and troubleshoot event action plans more efficiently.

IBM Director performs the following steps to determine which actions must be taken:

1. The managed system generates an event and forwards the event to all the management servers that have discovered the managed system (except for some events such as those generated through meeting or exceeding a Resource Monitor threshold, which are sent only to the management server where the thresholds are configured and applied, and the events in the Director tree and the CIM.Director.Agent Events tree).

Additional events are SNMP traps, ASF Platform Event Types (PETs), and management processors that have been configured to send events that are out-of-band to the management server.

2. IBM Director Server processes the message and determines which managed system generated the event and which group or groups the managed system belongs to.
3. IBM Director determines whether any event action plans are applied to the managed system or to any of the groups of which the managed system is a member.
4. If an event action plan has been applied, IBM Director Server determines whether any event filters match the event that was generated.
5. The management server performs any event actions for each matching event filter.

Planning and designing event action plan implementations

You must determine what the goal of the event action plan is. You should consider which managed systems you intend to target with the event action plan. You can target all managed systems, a subgroup of managed systems, or a specific managed system.

You can structure event filters and event actions in a number of ways. This section discusses some of the possible structures that you can use. Remember that many event action plans might include each of the elements of each of the structures discussed.

When designing your event action plan structure, consider all the managed systems in groups. Start by designing an event action plan that contains events that apply to the largest number of systems. Then, create event action plans that cover the next largest group of managed systems and continue to group them until you reach the individual managed-system level. When doing this, remember that each managed system can be a member of multiple groups.

When planning an event action plan structure, consider the following issues:

- Consider all the managed systems of the same type as a whole. What would you want to monitor on most or all of these systems? This answer determines the grouping and event filters for your first event action plan.
- Consider your managed systems as smaller groups. Decide how you would group them based on the additional events for which you would want to monitor. The smaller groups are usually based on the following criteria:

  - Managed-system manufacturer, for vendor-specific events
  - Function of the managed system, for services and resources specific to that function
- What type of managed systems are you monitoring?
- What is the function of the managed system?
- What are the key monitors for the managed system?
- Are there other managed systems for which the same monitors are desirable?

Grouping managed systems

Event action plans are best implemented by grouping all of your managed systems into both larger and smaller groups. The following criteria for these groupings are examples:

Type of managed system (servers, desktop computers, workstations, mobile computers, and network equipment)

Each type of managed system has its own event action plans.

By manufacturer

Each managed-system manufacturer has its own event action plans. Many organizations have managed systems from multiple manufacturers. In this case, if manufacturer-specific event monitors are required, you might want to have manufacturer-specific event action plans for each type of managed system.

By function

Each function of the managed system has its own event action plans. Each group of managed systems performing specific roles has different events for which to monitor. For example, on all of your print servers, you might want to monitor the printer spools and printers.

By resources

Event action plans based on specific resources. Typically, these event action plans monitor a specific resource outside of those in the managed system type event action plan. These resource event action plans might apply to managed systems with more than one system function, but not to all managed systems of the same type.

By management technology

If you have many devices that send SNMP traps, you can design event action plans to act on those events.

Structuring event action plans

You should determine the overall structure of your event action plans before you create them. A little planning in advance can prevent wasted time and duplication of effort.

Consider the following examples of event action plan structures:

A structure based on the areas of responsibility of each administrator
Typically, servers are maintained and managed by one group of personnel, and desktop computers and mobile computers are maintained by another group of personnel.

A structure based on administrator expertise
Some organizations have personnel that are specialized in the types of technology with which they work. These individuals might be responsible for complete managed systems, or only certain software running on these managed systems.

A structure based on managed-system function
Servers performing different functions need to be managed differently.

A structure based on the type of event
Examples are monitoring a specific process, monitoring for hardware events, and monitoring nearly anything else.

A structure based on work-day shifts
Because you can set up the event filters to be active only during certain parts of certain days, it is possible to structure your event action plans and event filters based on the shift (for example, first, second, and third shift) that will be affected by the events that are occurring.

Structuring event filters

You can use an event filter to capture a single event or multiple events. The following list includes some of the criteria you can use to determine whether to include an event with other events:

- All managed systems targeted for the filter are able to generate all events included in the filter. If the managed system does not generate the event for which the filter is defined, the filter is not going to be effective on that managed system.

- The event actions that will be used to respond to the event are the same for all targeted systems.
- The other event filter options besides the event type are common for all targeted systems. These settings include the times the event filter is active, the severity of the event, and other attributes.

Event action plans can include event filters with event types that will not be generated by all managed systems. In such instances, the event action plan can still be applied to those systems; it will just have no effect. For example, if an event filter is based on a ServeRAID™ event and that event action plan is applied to managed systems that do not have a ServeRAID adapter installed, the event filter has no events to filter, and therefore, no actions are performed. If you understand this concept you can create more complex event action plans and will reduce the number of event action plans you need to build and maintain.

Building an event action plan

There are five main steps to building and implementing event action plans:

1. Using the Event Action Plan Builder, create a new event action plan.
2. Using the Event Action Plan Builder, create an event filter or filters, then drag the filter or filters onto the event action plan.
3. Using the Event Action Plan Builder, customize an event action or actions, then drag the action or actions onto the applicable event filter.
4. Activate the event action plan by applying it to a single managed system, more than one managed system, or a group.

When you install IBM Director, a single event action plan is already defined, in addition to any you created using the Event Action Plan wizard. The Log All Events event action plan has the following characteristics:

- It uses the filter named All Events, a simple event filter that processes all events from all managed systems.
- It performs the action Add to the Event Log, a standard event action that adds an entry to the IBM Director Server event log.

To build a new event action plan, use the Event Action Plan Builder. In IBM Director Console, click **Tasks** → **Event Action Plan Builder** to open the “Event Action Plan Builder” window.

Successful implementation of event action plans requires planning and consideration of how they will be used. Developing and following strict naming standards is very important.

Event filters

In the “Event Action Plan Builder” window, the Event Filters pane displays all the event filters. The purpose of an event filter is to process only the events specified by the filter. All other events are ignored by the filter.

When naming an event filter, it is best if the name indicates the type of events for which the filter is targeted. The name also should indicate any special options that you have configured for the filter, including the time the filter is active and event severity. For example, an event filter for fatal storage events that occur on the weekend should be named to reflect that.

There are four types of event filters:

Simple event filter

The general-purpose filter type. Most event filters are of this type.

Eleven filters of this type are predefined:

- All Events
- Critical Events
- Environmental Sensor Events
- Fatal Events
- Hardware Predictive Failure Events
- Harmless Events
- Minor Events
- Security Events
- Storage Events
- Unknown Events
- Warning Events

Some of these filters use the severity of events to determine which events they will allow to pass through; others target a specific type of event. For example, the Critical Events filter processes only those events that have a Critical severity. The All Events filter processes any events that occur on any managed system.

Duplication event filter

Duplicate events are ignored, in addition to the options available in the Simple Event Filters.

An event meeting the criteria defined for this filter triggers the associated actions only the first time the criteria are met within a specified frequency range, interval, or frequency range within an interval. To trigger the associated event actions again, one of the following conditions must be met:

- The value specified in the **Count** field must occur.
- The time range specified in the **Interval** field must elapse.
- The value specified in the **Count** field must occur within the time range specified in the **Interval** field.

For example, you can define a duplication event filter to filter on the occurrence of an offline event and define a corresponding event action to forward the event to IBM Director Server. Depending on the criteria you define, only the first event announcing that the system is offline is processed, and all other instances in which an event meets the filtering criteria are discarded until the Count value is met during the specified interval.

Threshold event filter

In addition to the simple event filter options, threshold filters process an event after it occurs a specified number of times within a specified interval.

An event meeting the criteria defined in this filter triggers associated actions only after an event meets the criteria for the number of times specified in the **Count** field or only after the number of times specified in the **Count** field within the time range specified in the **Interval** field.

For example, you can define a threshold event filter to monitor frequently occurring heartbeat events and forward the event to IBM Director Server only when the heartbeat event is received for the 100th time during a specified amount of time.

Exclusion event filter

In addition to the simple event filter options, you can define event filtering criteria using the Event Type page and correlate another set of criteria using the Excluded Event Type page. The Excluded Event Type

excludes specified types of events from the criteria. That is, you can filter on a specified group of events but exclude certain events that might occur within that group.

Creating an event filter

To create a simple event filter, in the “Event Action Plan Builder” window, right-click **Simple Event Filter** and click **New**. The “Simple Event Builder” window opens.

Event Type page

Most event filters are created using only this page. It specifies the source or sources of the events that are to be processed by this filter.

By default, the **Any** check box is selected, meaning that all events listed are filtered. If you want to specify certain events on which to filter, clear the **Any** check box. You can highlight more than one event by pressing the Ctrl or Shift keys.

For example, a simple event filter based on all hardware-related events from BladeCenter units corresponds to the entry **MPA**.

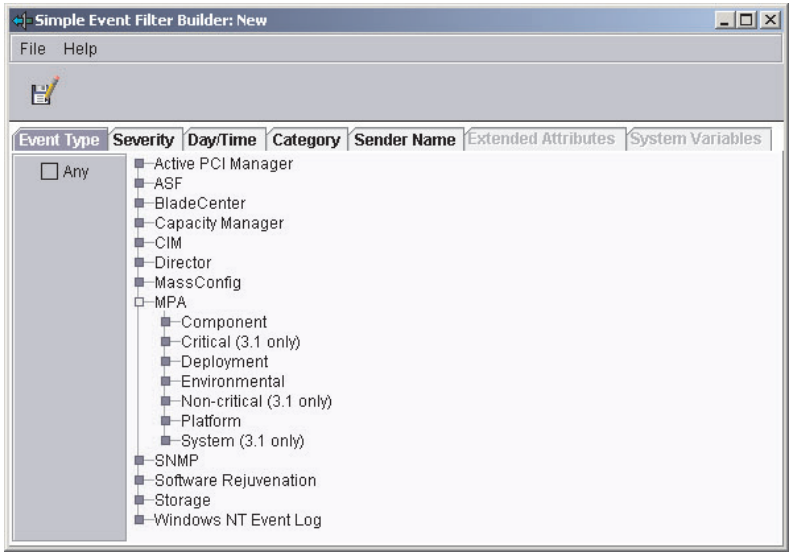

Figure 5. "Simple Event Filter Builder" window

Note: When you select a root option, all suboptions are selected as well. For example, selecting **MPA** in the "Simple Event Filter Builder" window also selects all Component, Deployment, Environmental, and Platform events listed as suboptions.

Severity page

Use the Severity page to indicate the urgency of the events that are filtered. If an event is received whose severity level is not included in the event filter, the filter will not process that event. By default, the **Any** check box is selected, indicating that all event severities are processed by the filter.

When you select more than one severity, they are joined together using logical OR. The source of the event should determine what severity the event is. Generally, the severity levels have the following meanings:

Fatal

The event caused a failure and should be resolved before the program or component is restarted.

Critical

The event might cause a failure and should be resolved immediately.

Minor
The event is not likely to cause immediate program failure but should be resolved.

Warning
The event is not necessarily problematic but might warrant investigation.

Harmless
The event is for information only; no potential problems are likely to occur as a result of this event.

Unknown
The application that generated the event did not assign a severity level.

Day/Time page

Use the Day/Time page to set the filter to accept and ignore events on certain days and at certain times of the day. By default, the **Any** check box is selected, indicating that events that occur at any time are processed by the event filter.

The time zone that applies to the specified time is the time zone in which the management server is located. If your management console is not in the same time zone as the management server, the difference in time zones is displayed above the Selections pane as an aid to determining the correct time.

By default, all events are passed through all filters. This includes events that were queued by IBM Director Agent because the link between the managed system or device and the management server was unavailable. However, you can prevent these queued events from being processed by a filter by selecting the **Block queued events** check box. This option can be useful if the timing of the event is important or if you want to avoid filtering on multiple queued events that are sent all at once when IBM Director Server becomes accessible. However, you can block queued events only if you filter events at a specified time. To block queued events, you must clear the **Any** check box.

Category page

Use the Category page to specify an event filter based on the alerting or resolution of a problem. However, not all events have resolutions.

Sender Name page

Use the Sender Name page to specify the managed system or device to which the event filter will apply. Events generated by all other managed systems or devices will be ignored. By default, the **Any** check box is selected, indicating that events from all managed systems and devices (including IBM Director Server) are processed by the event filter.

Initially, only IBM Director Server is listed in the list. As other managed systems generate events, such as when a threshold is exceeded, this list is added to dynamically. If you anticipate that other managed systems will generate events, you also can manually type managed-system or managed-device names into the field and click **Add** to add them.

Extended Attributes page

Use the Extended Attributes page to specify additional event-filter criteria. This page is available only when you clear the **Any** check box on the Event Type page and select certain entries from that page.

If the Extended Attributes page is available for a specific event type but no keywords are listed, IBM Director Server is not aware of any keywords that can be used for filtering.

To view the extended attributes of specific event types, expand the Event Log task in the IBM Director Console Tasks pane and select an event of that type from the list. The extended attributes of the event, if any, are displayed at the bottom of the Event Details pane, under the Sender Name category.

System Variables page

This page is available only if there are one or more system variables. A system variable consists of a user-defined keyword and value that are stored in IBM Director Server. You can create a system variable using the Set Event System Variable event action. For more details about this event action, see “Event data substitution variables” on page 46.

You can further qualify the filtering criteria by specifying a system variable.

Note: These user-defined system variables are not associated with the system variables of the Windows operating system.

Modifying an event action plan

You can modify an existing event action plan, even one already applied to managed systems or groups, using the Event Action Plan Builder.

If you modify an event filter or an event action used in an existing event action plan, the changes are applied automatically to any event action plans that use those filters or actions.

If you add or delete a filter or an action used in an existing event action plan, you will see the following prompt:

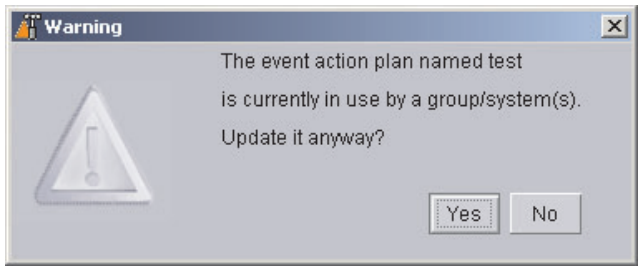

Figure 6. Prompt when modifying an existing event action plan

If you click **Yes**, the addition or deletion will affect all managed systems and groups that use that event action plan.

Event actions

You must customize an event action type to specify which action or actions you want IBM Director to take as a result of the occurrence of an event. Two examples of how to customize event action types to create event actions are described in the following sections.

The Actions pane lists the predefined event action types. With the exception of **Add Event to Event Log**, each event action type must be customized.

Event action names should be as descriptive as possible to reflect the action that will take place. The Event Action Plan Builder sorts all event actions alphabetically. For example, if the event action involves sending a message to

a pager, start the event action name with `Pager`; if the event action involves sending a message to a phone, start the event action name with `Phone`. Using such a naming convention ensures entries are grouped conveniently in the “Event Action Plan Builder” window.

Creating a pop-up message notification event action

An example of customizing an event action type is using the NET SEND command to display a pop-up message to a specific system on the network.

IBM Director has a standard event action that displays a message on the screen of any managed system currently running the management console. However, because you cannot always be sure that the person who needs to receive the message will have IBM Director Console running on the managed system he is using, you can use the NET SEND method to send a pop-up message. In this example, C3PO is the managed system to which the pop-up message will be sent.

Complete the following steps to configure a NET SEND command to send a pop-up message to a managed system named C3PO:

1. Determine the IP address or host name of the managed system on which you want the pop-up message to be displayed. In this case, the host name is C3PO.
2. In the “Event Action Plan Builder” window, right-click **Start a Program on the Server** in the Actions pane and click **Customize**. The “Customize Action” window opens.
3. Type the following command in the **Program Specification** field:

   ```
   cmd /c net send C3PO "IBM Director: &system generated a &severity &category"
   ```

   where

   - `cmd /c` is part of the command line that indicates to the Windows operating system on the management server to close the window automatically when the command is completed.
   - *C3PO* is the managed system on which you want the message to be displayed.
   - `&system` is an event data substitution variable that in the message is substituted with the name of the managed system that generated the event. See “Event data substitution variables” on page 46 for more information.
   - `&severity` is an event data substitution variable that in the message is substituted with the event severity.

- `&category` is an event data substitution variable that in the message is substituted with the event category (either Alert or Resolution).

Leave the working directory blank, as cmd.exe is in the Windows path.

4. Click **File** → **Save As** to save the action. The Save Event Action window opens.
5. Type the name of the action. In this example, `Net send popup to C3PO` is used. The new event action is displayed in the Actions pane as a subentry under the **Start a Program on the Server** event action type.

Creating an e-mail notification event action

Another example of an event action type is sending an e-mail notification. Typically, this is the first type of event action that IBM Director administrators set up. This event action is flexible because you can use it to generate standard e-mail messages and to send messages to most pagers and mobile phones.

Complete the following steps to create an event action for e-mail notification:

1. In the Actions pane, right-click **Send an Internet (SMTP) E-mail** and click **Customize**.
2. Complete the fields. See Figure 7 on page 44 for example values.

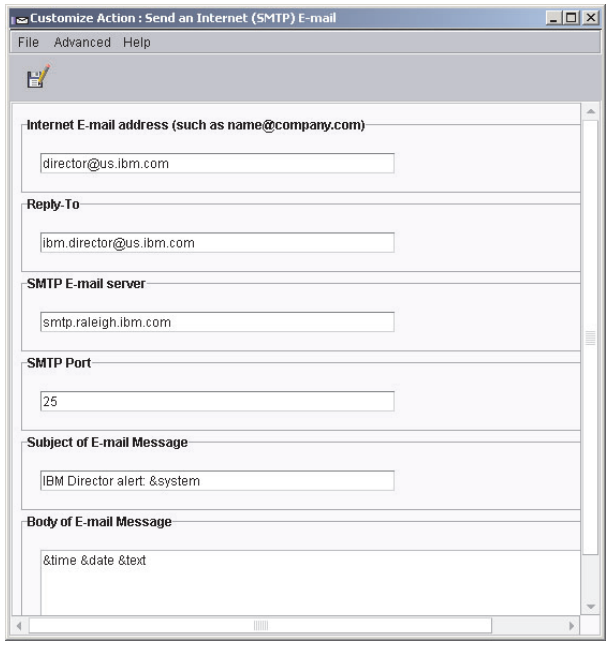

Figure 7. "Customize Action" window displaying example values

Note: Many pager and phone services that support SMTP messages limit the number of characters that can be sent in a given message. For this reason, it is recommended that you keep the text of the message brief.

3. Click **File** → **Save As** to save the event action. The "Save Event Action" window opens.
4. Type a name for the event action. In this example, `E-mail: director@us.ibm.com generic` is used.

   If you are sending the message to a pager, start the event action name with `Pager`; if you are sending the message to a phone, start the event action name with `Phone`. Using such a naming convention ensures entries are grouped conveniently in the "Event Action Plan Builder" window.
5. Click **OK**. The new event action is displayed in the Actions pane as a subentry under the **Send an Internet (SMTP) E-mail** event action type.

Available event action types

The following table describes all the available event action types.

Table 1. Event action types

Event	Description
Add/Remove “event” system to Static Group	Adds a managed system to or removes a managed system from a specified static group when the managed system logs a specific event.
Add/Remove source group members to a target static group	Adds all specified managed systems in a source group to a target group or removes all specified managed systems from the target group.
Add a Message to the Console Ticker Tape	Displays a message in red type that scrolls from right to left at the bottom of IBM Director Console.
Add to the Event Log	Adds a description of the event to the event log.
Define a Timed Alarm to Generate an Event	Generates an event only if IBM Director does not receive an associated event within the specified interval.
Define a Timed Alarm to Start a Program on the Server	Starts a program on the management server if IBM Director does not receive an associated event within the specified interval.
Log to Textual Log File	Generates a text log file for the event that triggers this action.
Post a News Group (NNTP)	Sends a message to a newsgroup using the NNTP protocol.
Resend Modified Event	Creates or changes an event action that modifies and resends an original event.
Send an Alphanumeric Page (through TAP)	Sends a message to a pager using the Telocator Alphanumeric Protocol (TAP).
Send an Event Message to a Console User	Displays a pop-up message on the management console of one or more specified users.
Send an Internet (SMTP) E-mail	Sends an e-mail message.
Send an SNMP Trap to a NetView Host	Generates an SNMP trap and sends it to a specified NetView® host using a TCP/IP connection to the host. If delivery of the SNMP trap fails, a message is posted in the history log of the managed system.

Table 1. Event action types (continued)

Event	Description
Send an SNMP Trap to an IP Host	Generates an SNMP trap and sends it to a specified IP address or host name.
Send a Numeric Page	Sends a numeric-only message to the specified pager.
Set an Event System Variable	Sets the managed system variable to a new value or resets the value of an existing system variable.
Start a Program on a System	Starts a program on any managed systems on which IBM Director Agent is installed.
Start a Program on the “event” System	Starts a program on the managed system that generated the event.
Start a Program on the Server	In response to an event, starts a program on the management server that received the event.
Start a Task on the “event” System	In response to an event, starts a noninteractive task on the managed system that generated the event.
Update the Status of the “event” System	When the selected resource status generates an event, the status of the managed system associated with the resource is set or cleared according to your specification.

Event data substitution variables

When you create some types of event actions, you can include event-specific information as part of the text message. Including event information is referred to as event data substitution. You can use event data substitution variables to customize event actions. The following table describes the event data substitution variables.

Table 2. Event data substitution variables

Variable	Description
&date	Provides the date the event occurred.
&time	Provides the time the event occurred.

Table 2. Event data substitution variables (continued)

Variable	Description
&text	Provides the event details, if supplied by the event.
&type	Provides the event-type criteria used to trigger the event. For example, the event generated when a managed system goes offline is of type Director.Topology.Offline. This corresponds to the entry on the Event Type page.
&severity	Provides the severity level of the event.
&system	Provides the name of the managed system for which the event was generated. The system name is either the name of IBM Director Agent, or in the case of an SNMP device, the TCP/IP address.
&sender	Provides the name of the managed system from which the event was sent. This keyword returns null if unavailable.
&group	Provides the group to which the target system belongs and is being monitored. This keyword returns null if unavailable.
&category	Provides the category of the event, either Alert or Resolution. For example, if the managed system goes offline, the category is Alert. If the managed system goes online, the category is Resolution.
&pgmtype	Provides a dotted representation of the event type using internal type strings.
&timestamp	Provides the coordinated time of the event.
&rawsev	Provides the nonlocalized string of event severity (Fatal, Critical, Minor, Warning, Harmless, Unknown).
&rawcat	Provides the nonlocalized string of event category (Alert, Resolution).
&corr	Provides the correlator string of the event. Related events, such as those from the same monitor-threshold activation, will match this.
&snduid	Provides the unique ID of the event sender.
&sysuid	Provides the unique ID of the managed system associated with the event.

Table 2. Event data substitution variables (continued)

Variable	Description
&prop:*filename*#*propname*	Provides the value of the property string *propname* from property file *filename* (relative to IBM\Director\classes).
&sysvar:*varname*	Provides the event system variable *varname*. This keyword returns null if a value is unavailable.
&slotid:*slot-id*	Provides the value of the event detail slot with the nonlocalized ID *slot-id*.
&md5hash	Provides the MD5 (message digest 5) hash code (CRC) of the event data (good event-specific unique ID).
&hashtxt	Provides a full replacement for the field with an MD5 hash code (32-character hex code) of the event text.
&hashtxt16	Provides a full replacement for the field with a short MD5 hash code (16-character hex code) of the event text.
&otherstring	Provides the value of the detail slot with the localized label that matches otherstring. This keyword returns OTHERSTRING if unavailable.

Chapter 3. Active PCI Manager events

Active PCI Manager event types are displayed in the “Event Filter Builder” window if you have installed the IBM Director Server Plus Pack and have selected to install Active PCI Manager. Active PCI Manager events notify you of changes to PCI or PCI-X adapters. That is, you can use Active PCI Manager events to monitor changes to these types of devices on supported systems. Examples of when these events can occur are:

- When the adapter-retention latch is raised or lowered (such as in the case of hot-plug add or eject operations or the surprise removal of an adapter)
- When the operating system requests an eject operation

For more information about which xSeries servers are supported with Active PCI Manager, see http://www.ibm.com/pc/us/compat/.

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or resolution.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Table 3. Active PCI Manager events

Tree node	Event type	Description	Severity	Resolution or alert	Generated by OS or by IBM Director
1	Slot events				
2	Adapter add complete	The operating system detects that a previously empty slot has a powered on adapter; occurs after a successful hot-add operation.	Harmless	Alert	OS
2	Adapter ejected complete	User requests that the operating system eject an adapter, which causes the eject operation to unload the device driver from the adapter and powers off its slot in preparation for removing the adapter while the system is powered on.	Harmless	Alert	OS
2	Power fault	An adapter has a power fault.	Harmless	Alert	OS
2	Surprise removal of an adapter	The adapter-retention latch on a slot was lifted manually without first ejecting the adapter in that slot through the operating system. This action is never recommended.	Harmless	Alert	OS

Table 4. Events that are published only if they occur

Event type	Description	Severity	Resolution or alert	Generated by OS or by IBM Director
Locator Stop	The locator LED on the slot has been turned on or off by Slot Manager.	Harmless	Alert	IBM Director (Slot Manager subtask)
BusDataChanged	Slot Manager needs to update its data.	Harmless	Alert	IBM Director (Slot Manager subtask)

Table 4. Events that are published only if they occur (continued)

Event type	Description	Severity	Resolution or alert	Generated by OS or by IBM Director
BusSpeedMismatch	Hot add blocked; adding an adapter might cause a bus speed mismatch. The adapter is not capable of running at the current bus speed.	Harmless	Alert	IBM Director (Slot Manager subtask)
Too many adapters	Hot add blocked; adding an adapter limit has been reached for current bus speed.	Harmless	Alert	IBM Director (Slot Manager subtask)
Slot Unavailable	Hot add blocked; slot is not operational at current bus speed.	Harmless	Alert	IBM Director (Slot Manager subtask)

Chapter 4. Alert Standard Format (ASF) events

Alert Standard Format (ASF) defines remote control and alerting interfaces in an environment without an operating system, on servers with ASF-capable network interface cards (NICs) such as the xSeries 255, xSeries 235, and xSeries 345. Alert Standard Format events provide advanced warning of a possible system failure. System failure notifications are generated from the management server.

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Table 5. ASF events

Tree node	Event type	Description	Severity	Resolution or alert	Generated by OS or by IBM Director
1	Environmental				
2	Sensor				
3	Case Intrusion	Case intrusion event.	Critical	Alert	IBM Director
3	Fan	Fan event [Device X (ENTITYINSTANCE)]	Critical	Alert	IBM Director
	Fan	Device X (ENTITYINSTANCE) inserted.	Harmless	Resolution	IBM Director
3	Fan	Device X (ENTITYINSTANCE) removed.	Warning	Alert	IBM Director
3	Power Supply	Redundancy has been lost or redundancy has been degraded.	Critical	Alert	IBM Director

Table 5. ASF events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Generated by OS or by IBM Director
	Power Supply	Power supply has failed.	Critical	Alert	IBM Director
	Power Supply	Redundancy has been regained.	Harmless	Resolution	IBM Director
3	Temperature	Temperature event.	Critical	Alert	IBM Director
3	Voltage	Voltage event Device X (ENTITY INSTANCE)	Critical	Alert	IBM Director
2	Firmware				
3	BIOS				
4	Progress	System firmware progress	Harmless	Resolution	IBM Director
	Progress	System firmware error	Critical	Alert	IBM Director
	Progress	System boot initiated	Harmless	Resolution	IBM Director
	Progress	System firmware hang	Critical	Alert	IBM Director
2	Hardware				
3	Cable/Interconnect	Device is absent.	Warning	Alert	IBM Director
	Cable/Interconnect	Device is present.	Harmless	Resolution	IBM Director
3	Drivebay	Device X (ENTITY INSTANCE) removed.	Warning	Alert	IBM Director
	Drivebay	Transition to critical.	Warning	Alert	IBM Director
2	Drivebay	Device X (ENTITY INSTANCE) inserted.	Harmless	Resolution	IBM Director
2	Drivebay	Transition to OK.	Harmless	Resolution	IBM Director
3	Module/Board	Device is absent.	Warning	Alert	IBM Director
	Module/Board	Device is present.	Harmless	Resolution	IBM Director
3	Monitor ASIC/ IC	System management module is too critical.	Critical	Alert	IBM Director

Table 5. ASF events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Generated by OS or by IBM Director
3	Network	Network connection is offline.	Harmless	Resolution	IBM Director
4	Network	Network connection is degraded.	Harmless	Resolution	IBM Director
5	Network	Network connection is online.	Harmless	Resolution	IBM Director
3	Watchdog 1	Watchdog has expired.	Critical	Alert	IBM Director
3	Watchdog 2	Timer has expired.	Critical	Alert	IBM Director
2	System				
3	OS				
4	Boot	No bootable media or device.	Critical	Alert	IBM Director
4	Operation				
	Heartbeat	Heartbeat	Harmless	Resolution	IBM Director

The event qualifier information in the following table can be helpful when working with managed systems with ASF-capable NICs. These NICs send certain events, and enable you to monitor environmental sensors without having a Remote Supervisor Adapter or other event generating hardware. After you enable the configuration in the management console, use IBM Director Server to monitor these events.

Table 6. ASF events technical information

Tree node	Event type	Event qualifier	Extended attributes
1	Environmental		See the list of internal string information following this table.
2	Sensor		
3	Case Intrusion	ASF.Environmental.Sensor.Case Intrusion	
3	Fan	ASF.Environmental.Sensor.Fan	
3	Power Supply	ASF.Environmental.Sensor.Power Supply	
3	Temperature	ASF.Environmental.Sensor.Temperature	
3	Voltage	ASF.Environmental.Sensor.Voltage	
2	Firmware		
3	BIOS		
4	Progress	ASF.Firmware.BIOS.Progress	
2	Hardware		
3	Cable/ Interconnect	ASF.Hardware.Cable/Interconnect	
3	Drivebay	ASF.Hardware.Drivebay	

Table 6. ASF events technical information (continued)

Tree node	Event type	Event qualifier	Extended attributes
3	Module/Board	ASF.Hardware.Module/Board	
3	Monitor ASIC/ IC	ASF.Hardware.Monitor ASIC/IC	
3	Network	ASF.Hardware.Network	
3	Watchdog 1	ASF.Hardware.Watchdog1	
3	Watchdog 2	ASF.Hardware.Watchdog2	
2	System		
3	OS		
4	Boot		
4	Operation		
5	Heartbeat	ASF.System.OS.Operation.Heartbeat	

Note: All ASF PETs use the same extended attributes. These attributes are per the Intel IPMI Platform Event Trap specification Version 1.0, dated Dec 7, 1998. Event Type: Size = Integer: Bits 18 through 8 have a code indicating what type of transition or state triggered a trap. For example:

The following list provides the internal string names of the extended attributes for the event types.

- ALLVARBIND
- EVENTTYPE
- OFFSET
- GUID
- SEQUENCEID
- LOCALTIMESTAMP
- UTCOFFSET
- TRAPSOURCETYPE

- EVENTSOURCETYPE
- EVENTSEVERITY
- SENSORDEVICE
- SENSORNUMBER
- ENTITY
- ENTITYINSTANCE
- EVENTDATA
- LANGUAGECODE
- MANUFACTURERID
- SYSTEMID
- OEMCUSTOMFIELD

Chapter 5. BladeCenter Assistant events

You can use these events for the BladeCenter Assistant task.

Note: These are not the hardware-related events that are sent from the management module; those events are found in the MPA section of the Event Filter Builder. See Chapter 10, “Management Processor Assistant (MPA) events”, on page 82.

Only one IBM Director Server can be used to manage a BladeCenter chassis. An event might occur if more than one IBM Director Server is attempting to manage the chassis. Also, a failure might occur when IBM Director cannot identify the correct login for the management module.

Note: When using these tables, be sure to remember the following information:

- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.
- The “Extended attribute” column provides the extended attributes that can be used for this event filter.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Table 7. BladeCenter Assistant events

Event type	Description	Severity	Resolution or alert	Extended attributes	Generated by OS or by IBM Director
Component	Deployment wizard failed to connect or log in: possible invalid username or password.	Critical	Alert	String - Profile Name	IBM Director
Deployment wizard	Connection lost to chassis during deployment.	Critical	Alert	String - Profile Name	IBM Director

Chapter 6. Capacity Manager events

You can use Capacity Manager events to receive events for system capacity. To receive Capacity Manager events, you must select the **Generate Bottleneck Events** check box in the Capacity Manager report definition. For more information, see “Capacity Manager” in the *IBM Director 4.1 Systems Management Guide*.

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.
- The “Extended attributes” column provides the extended attributes that you can use for filtering with this event.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Table 8. Capacity Manager events

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes	Generated by OS or by IBM Director
1	Bottleneck	A system bottleneck has been detected.	Critical	Alert	String-cmrFile, String-txtfile, String-htmlFile, Boolean-Involves memory, Boolean-Involves disk, Boolean-Involves LAN, Boolean-ClusterNode	IBM Director
2	Recommendation	An event-enabled Capacity Manager report has been run and a system bottleneck was detected during performance analysis.	Critical	Alert	startTime, stopTime, minutesSinceStart, MinutesSinceStop, hoursSinceStart, hoursSinceStop, daysSinceStart, daysSinceStop, hoursThis	IBM Director
1	No Response		Minor	Alert	None	IBM Director
2	No Monitors	No systems responded with monitor data when an event-enabled report was run.	Minor	Alert	None	IBM Director

Chapter 7. Common Information Model (CIM) events

You can use CIM events when working with hardware related events.

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.
- The “Extended attributes” column provides information about the extended attributes for the CIM events.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.
- The “New in IBM Director 4.1″ column indicates if an event type is available for the first time in the IBM Director 4.1 release.

Table 9. IBM Director Agent events

Tree node	Event type	Description	Severity	Resolution or Alert	Extended attributes	New in IBM Director 4.1
	Common Information Model (CIM)	Organizes data and all hardware alerts				No
1	DASD Backplane	Sent through the subsystem on a managed system from the Remote Supervisor Adapter when an error condition is detected in the drive backplane of servers with a Remote Supervisor Adapter installed. The event description specifies the SCSI ID or drive number of the problematic hard disk drive.	Critical	Alert	See Table 10 on page 66 for more information.	Yes

Table 9. IBM Director Agent events (continued)

Tree node	Event type	Description	Severity	Resolution or Alert	Extended attributes	New in IBM Director 4.1
1	Disk Space Low	A warning event is sent when a the total used space on a volume exceeds 95%. A critical event is sent when a the total used space on a volume exceeds 98%.	Normal, Warning, Critical	Alert and Resolution	See Table 10 on page 66 for more information.	No
1	Error Log	Sent from systems with the Remote Supervisor Adapter installed only to indicate when the log for the adapter is 75% or 100% full.	Warning	Alert	See Table 10 on page 66 for more information.	No
1	Fan	If a Remote Supervisor Adapter is installed on a system, this event is sent when a fan stops, is removed, or is not performing optimally. If a Remote Supervisor Adapter is not installed, an event is sent when the fan stops or is removed.	Warning, Critical, Normal	Alert, Resolution	See Table 10 on page 66 for more information.	No
1	LAN Leash	Systems with Alert on LAN™ hardware. The system has been removed from the network.	Critical	Alert	See Table 10 on page 66 for more information.	No
1	Lease Expiration	Monitors the IBMPSG_Lease.EndDate CIM property. If the date is less than the current date, a warning event is sent.	Warning	Alert	Asset ID™ task	No
		If the date is in the future or null (not set), a normal event is sent. Indications are only sent when the system CIM Object Manager (CIMOM) starts and when a state change is detected (relative to a internal poll interval).	Normal	Resolution		

Table 9. IBM Director Agent events (continued)

Tree node	Event type	Description	Severity	Resolution or Alert	Extended attributes	New in IBM Director 4.1
1	Memory PFA	A memory error has been detected.	Critical, Normal	Alert, Resolution	See Table 10 on page 66 for more information.	No
1	Network Adapter				See Table 10 on page 66 and Table 11 on page 67 for more information.	Yes
2	Failed	The network adapter failed.	Critical	Alert		Yes
2	Offline	The network adapter is offline.	Warning	Alert		Yes
2	Online	The network adapter is online.	Normal	Resolution		Yes
1	PFA	This event is sent on behalf of the Remote Supervisor Adapter when a monitored subsystem is experiencing an imminent failure.	Critical	Alert	See Table 10 on page 66 for more information.	No
1	Processor PFA	The processor is experiencing an imminent failure.	Critical, Normal	Alert, Resolution	See Table 10 on page 66 for more information.	No
1	Redundant Network Adapter Failover	A network interface card (NIC) failover has occurred. This requires a teamed configuration.	Warning	Alert	See Table 10 on page 66 for more information.	No
1	Redundant Network Adapter Switchback	A NIC switchback has occurred. This requires a teamed configuration.	Warning	Alert	See Table 10 on page 66 for more information.	No

Table 9. IBM Director Agent events (continued)

Tree node	Event type	Description	Severity	Resolution or Alert	Extended attributes	New in IBM Director 4.1
1	Redundant Network Adapter Switchover	A NIC switch over has occurred. This requires a teamed configuration.	Normal	Alert	See Table 10 on page 66 for more information.	No
1	Remote Login	Sent for the Remote Supervisor Adapter. This indicates that a user has logged in to the Web interface of the Remote Supervisor Adapter.	Warning	Alert	See Table 10 on page 66 for more information.	Disabled by default.
1	ServeRAID Health	Sent by the ServeRAID Agent for IBM Director; a change in status in the ServeRAID subsystem has occurred. The Event Text field of this event, documented in Table 12 on page 67, specifies the cause of the status change.	Warning, Normal	Alert, Resolution	See Table 10 on page 66 for more information.	No
1	Server Power Supply	A power supply failure or loss in redundancy has occurred.	Critical, Normal	Alert, Resolution	See Table 10 on page 66 for more information.	No
1	SMART Drive	Sends an event when a SMART capable drive determines that an imminent failure is predicted.	Critical, Normal	Alert, Resolution	See Table 10 on page 66 for more information.	No
1	System Enclosure	The cover has been removed from a system with a chassis intrusion sensor or from a desktop model.	Critical, Normal	Alert, Resolution	See Table 10 on page 66 for more information.	No

Table 9. IBM Director Agent events (continued)

Tree node	Event type	Description	Severity	Resolution or Alert	Extended attributes	New in IBM Director 4.1
1	Temperature	The warning or critical temperature threshold being measured by a temperature sensor has been exceeded.	Warning, Critical, Normal	Alert, Resolution	See Table 10 for more information.	No
1	Voltage	A system is over or under current.	Critical, Normal	Alert, Resolution	See Table 10 for more information.	
1	Warranty Expiration	Monitors the IBMPSG_Warranty.EndDate CIM property. If the date is earlier than the current date, a warning event is sent. If the date is in the future or not set, an event is sent. Events are sent only when the managed system (CIMOM) starts and when a state change is detected (relative to a internal poll interval).	Warning	Alert, Resolution	Asset ID task	No

The CIM.Director Agent events have the following extended attributes:

Table 10. CIM.Director Agent event extended attributes

Values	Extended attributes	Description
Environmental, Network, Storage, Security, and others.	String CATEGORY//	This is the hardware event category as defined by the Hardware Status task.
	String CLASSNAME //	This is the CIM class name for this event.
	String TARGET //	This is the standard CIM ObjectPath of the target for this event type.

The Network Adapter.Failed, Network Adapter.Offline, and Network Adapter.Online events have the following additional extended attributes:

Table 11. Network events

Extended attributes	Description
String RESOLUTION//	This can help to resolve a hardware problem in the server.
String DEVICEID //	This is the ID for the component if there are more than one of the same component and you are trying to fix a particular instance.

Table 12. ServeRAID Health event type text

Event text	Severity	Category
Defunct drive (FRU Part # + [number] + on controller “+ [number] +, channel “+ [number] +”, SCSI ID “+[number] +”.”	Warning	Alert
Commands not responding on Controller + [number] +”.”	Critical	Alert
The battery-backup cache device on Controller + [number]+” needs a new battery.	Critical	Alert
The battery-backup cache device on Controller +[number] +” is defective “+[number]+” “	Critical	Alert
Background polling commands not responding on Controller + [number] +” “+ [number] +” “	Critical	Alert
Cannot read controller configuration.	Critical	Alert
Controller + [number] +” failover detected. Passive controller is now active.”	Warning	Alert
Logical Drive + [number] +” is Critical on Controller “+ [number] +”.”	Critical	Alert
Logical Drive + [number] +” is Offline on Controller “+ [number] +”.”	Critical	Alert
Rebuild failed on Logical Drive + [number] +” of Controller “+ [number] +” “+ [number] +”.”	Critical	Alert

Table 12. ServeRAID Health event type text (continued)

Event text	Severity	Category
Synchronization failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +"."	Critical	Alert
Migration failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +"."	Critical	Alert
Compression failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +"."	Critical	Alert
Decompression failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +"."	Critical	Alert
Flashcube® failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +"."	Critical	Alert
Rebuild failed on Array + [number] +" of Controller "+ [number] +" "+ [number] +"."	Critical	Alert
Synchronization failed on Array + [number] +" of	Critical	Alert

FTMI events

Using FTMI events you can receive alerts if Active PCI Manager is installed.

Tree node	Event type	Description	Severity	Generated by OS or IBM Director	New in IBM Director 4.1
1	FTMI data has been modified	FTMI needs a data update.	Harmless	IBM Director (FTMI subtask)	Yes
1	FTMI refresh	The adapter software needs an FTMI data update.	Harmless	OS (adapter software)	Yes

FTMI queries

This FTMI event information is available when Active PCI Manager is installed.

Tree node	Event type	Description	Severity	Resolution or alert	Generated by OS or IBM Director	New in IBM Director 4.1
1	Network Adapter Failed	Adapter software determined the adapter failed or lost connection to the network. Error Text: Network Adapter has Failed, for <*Name*>, <*DeviceID*>.	Critical	Check the FTMI log, the OS, or the event log for any messages.	IBM Director	Yes
1	Network Adapter Offline	The adapter was placed in an offline state by the user or by the adapter software. Error Text: Network Adapter has gone Offline, for <*Name*>, <*DeviceID*>.	Warning	Check the FTMI log, the OS, or the event log for any messages.	IBM Director	Yes
1	Network Adapter Online	The adapter was placed in an online state by the user or by the adapter software. Error Text: Network Adapter has gone Online, for *<Name>, <DeviceID>*.	Warning	Check the FTMI log, the OS, or the event log for any messages.	IBM Director	Yes
1	Redundancy Group Change	The adapter software has determined the data in the redundancy group has changed. Error Text: Redundancy Group property has changed for <*Name*>.	Warning	Check the FTMI log, the OS, or the event log for any messages.	IBM Director	Yes

Chapter 8. IBM Director events

The IBM Director event types that are in the “Event Filter Builder” window are displayed under the Director node and under the CIM.Director Agent Events node. When any of these event types are issued by a managed system, they are automatically sent to all of the management servers that have discovered that system. These events are processed by the Log All Events event action plan. The Log All Events event action plan adds the event to the IBM Director event log, and can be modified to include additional event actions for these event types. In contrast, other event types on which you want to filter on must be added to an event action plan manually.

The event types displayed in the Director Agent Events tree under the CIM root node are generated when a status change occurs for a hardware component in a managed system. The CIM events for the hardware component status changes applies only for systems running Windows.

The event types displayed in the Director tree include a set of events for notifying the user of IBM Director Console logins, a set of test events for testing event flow, events that notify you when a managed system is offline, and the placeholder node named mib which is used as the root node for event types that are displayed as the result of the configuration of a Resource Monitor threshold against an SNMP device.

Resource Monitor, Process Monitor, and Scheduler event types are published, and then displayed dynamically in the “Event Filter Builder” window when you configure a process or resource monitor or schedule a job and specify alert generation. If you configure a resource monitor for an SNMP device, an event type is created using the path to the variable in its Management Information Base (MIB) file, and this type is displayed in place of the node named mib. The format of the event type displayed in the tree uses a different template depending on whether the variable is a string or numeric value.

If a Resource monitor is configured against the ipForwarding `string` variable that is defined in the SMI version 2 MIB file, the following is displayed under the IBM Director node:

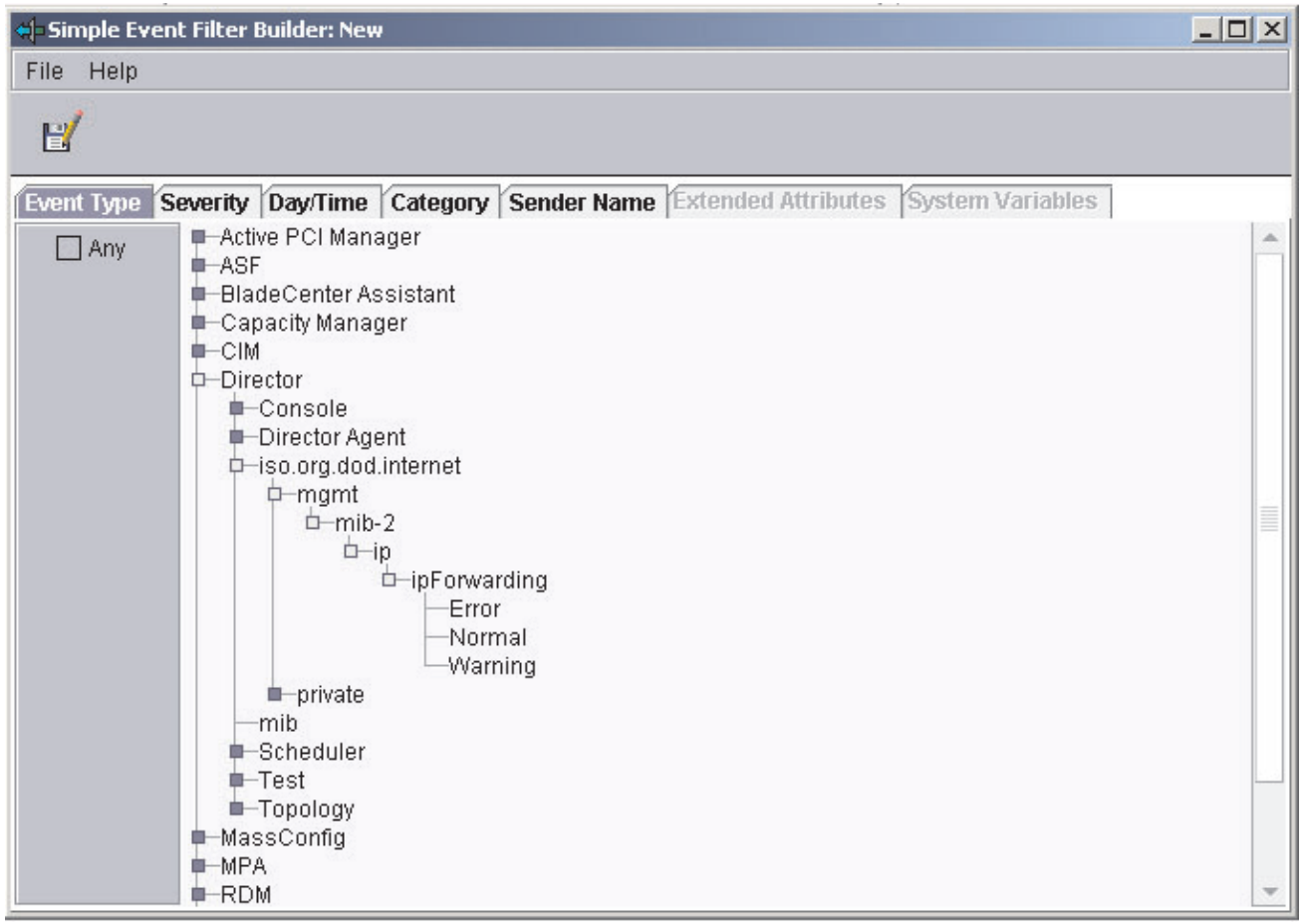

Figure 8. Resource monitor example for string variables

The string variables, Error, Normal, and Warning are displayed under the monitored variable.

The following example contains a resource monitor configured against the private Microsoft MIB. This MIB variable is an integer, not a string. The template for non-string variables (when configuring a resource monitor) is to put the

threshold levels that were defined in the monitor underneath the variable along with the state. This example is configured for a high-error and high-warning threshold.

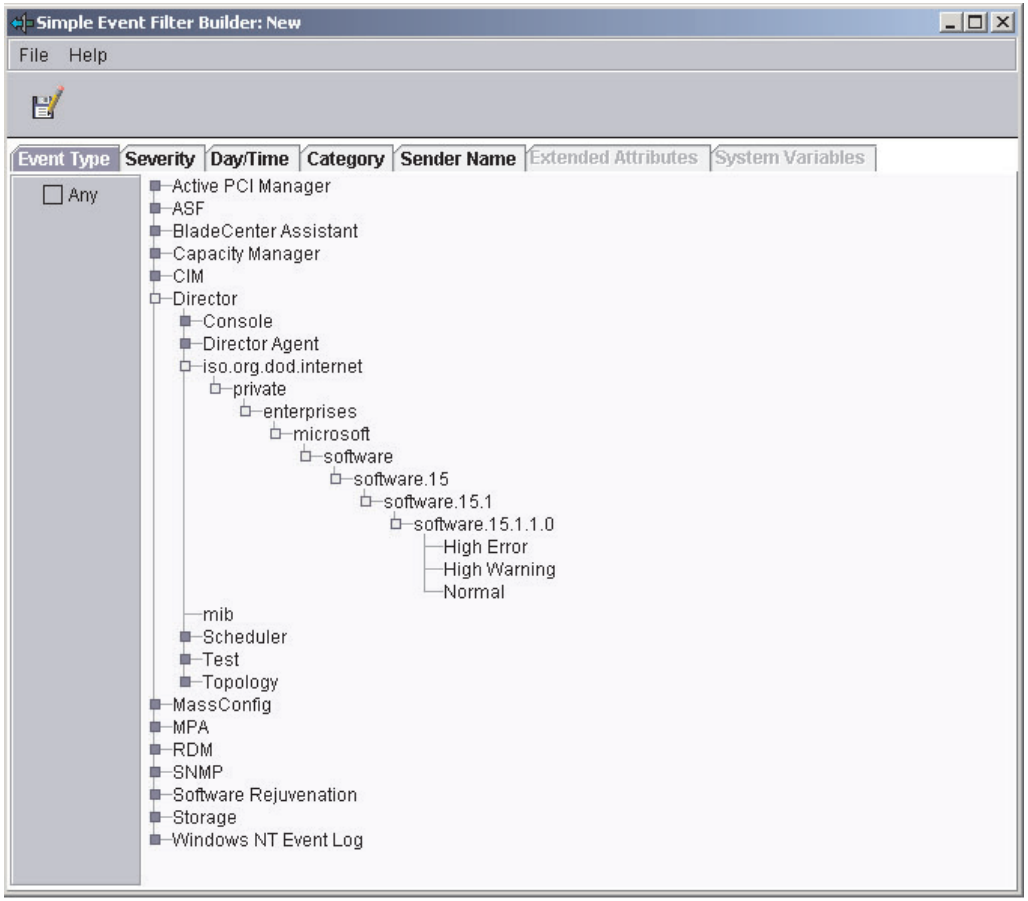

Figure 9. Resource monitor example of an integer variable

Resource monitor event types

Events sent by resource monitors that you configure in IBM Director are displayed in the Event Filter Builder. You can use the information in the following table when working with the resource monitor event details.

Table 13. IBM Director resource monitor event details

Event details		
Threshold name	String	The name you assigned the threshold.
Monitor resource	String	The type of monitor configured with a threshold.
Threshold value	Double	The configured value you assigned in the **Above or Equal** or **Below or Equal** field of the “Threshold Configuration” window.
Duration	Long	The configured value you assigned in the **Minimum Duration** field of the “Threshold Configuration” window.
Actual value	Double	Current reading of the monitored resource at the time the event is sent.

Process monitor event types

Events sent by process monitors that you configure in IBM Director are displayed in the “Event Filter Builder” window. You can use the information in the following table when working with the process monitor event details.

Table 14. Process monitor event details

Event details	
Threshold name	String
Monitor resource	String
Threshold value	Double
Duration	Long
Actual value	Double

Scheduler event types

The Scheduler events are displayed in the IBM Director tree in the “Event Filter Builder” window. These events contain a job ID that is created when you create a new job.

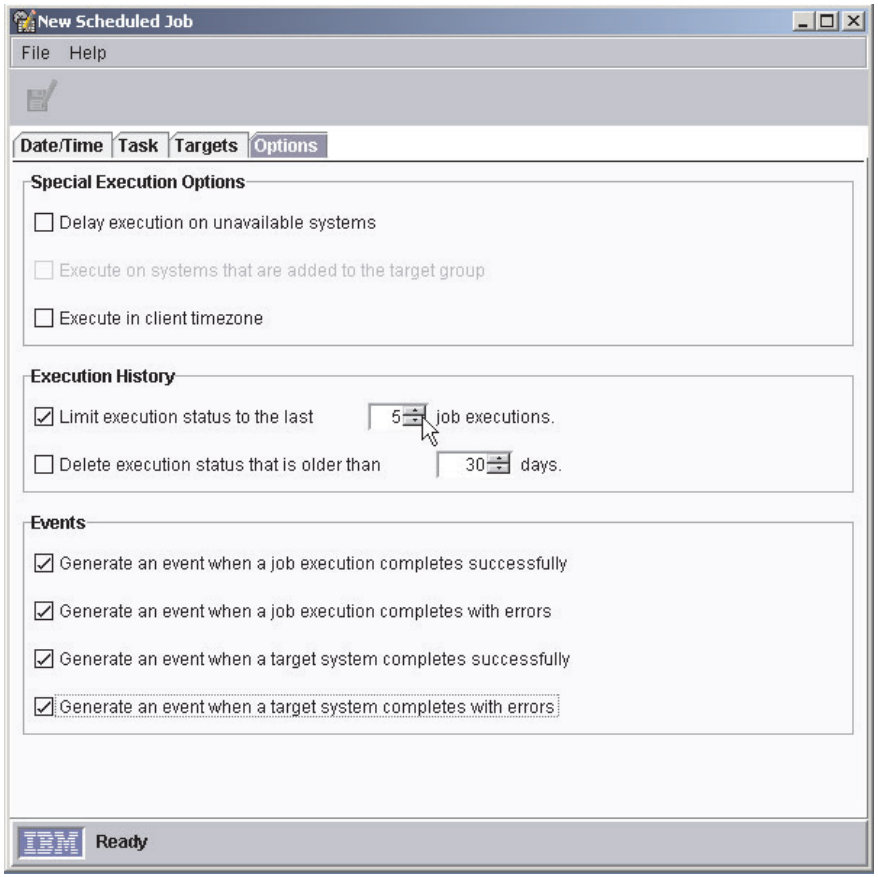

Figure 10. “New Scheduled Job” window

Table 15. New scheduled job event details

Event details	
Job ID	String
Job Activation Time	String
Client Status	String
Job Current Task ID	String
Job Current Subtask ID	String
Job Current Task Name	String

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Table 16. IBM Director events

Tree node	**Event type**	**Description**	**Severity**	**Resolution or alert**	**Extended attributes**	**Generated by OS or by IBM Director**
1	Console					
2	Logon Failure					
3	Bad Password					
3	Bad User ID	Incorrect user id entered.	Warning	Alert	Userid and address	IBM Director

Table 16. IBM Director events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes	Generated by OS or by IBM Director
3	Disabled User ID	Entered user id is disabled.	Warning	Alert	Userid and address	IBM Director
3	Downlevel Console	User tried log on using a lower-level IBM Director Console.	Warning	Alert	Userid and address	IBM Director
3	Expired Password	Entered password expired.	Warning	Alert	Userid and address	IBM Director
3	Too many active IDS	Too many active user ids on IBM Director Server.	Warning	Alert	Userid and address	IBM Director
3	Too many active Logons	Too many active logons on IBM Director Server.	Warning	Alert	Userid and address	IBM Director
3	Uplevel Console	User tried to log in using an IBM Director Console version level that is too high.	Warning	Alert	Userid and address	IBM Director
2	User Logoff	User logged off.	Harmless	Alert	Address, description, locale, userid, username generated	IBM Director
2	User Logon	User logged on.	Harmless	Alert	Address, description, locale, userid, username generated	IBM Director
1	Director Agent					

Table 16. IBM Director events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes	Generated by OS or by IBM Director
2	Resource Monitors	This is dynamic and dependent on the monitor you create.	This is configured with the threshold for the monitor.	Alert	See Table 13 on page 74.	
2	MPA	This event is sent if the MPA Agent fails.		Alert		
2	Process Monitors	This is dynamic and dependent on the process monitor that you create.	This is dependent on the severity of the process event.	Alert		
3	Process Alert	This is dynamic and dependent on the process monitor that you create.	This is dependent on the severity of the process event.	Alert		
4	Process Failed to Start	The monitored process did not start.	Warning	Alert	See Table 14 on page 74.	
4	Process Started	The monitored process started.	Harmless	Alert	See Table 14 on page 74.	
4	Process Terminated	The monitored process terminated.	Critical	Alert	See Table 14 on page 74.	
2	mib	This event is dynamic. For more information see Figure 8 on page 72.				

Table 16. IBM Director events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes	Generated by OS or by IBM Director
1	Scheduler	This event is dynamic. See “Scheduler event types” on page 75.				
2	Job	This event is sent when a scheduled job is successful or if it fails.				
3	Success		Harmless			
4	Name of scheduled job	Name of scheduled job.			See Table 15 on page 76.	
3	Error		Warning			
4	Name of scheduled job.	Name of scheduled job.			See Table 15 on page 76.	
2	System	This event is sent when a scheduled job completes or fails on a target system.				
3	Success		Harmless			
4	Name of scheduled job.	Name of scheduled job.			See Table 15 on page 76.	
3	Error		Warning			
4	Name of scheduled job.	Name of scheduled job.			See Table 15 on page 76.	
1	Test					

Table 16. IBM Director events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes	Generated by OS or by IBM Director
2	Action	Used to generate test event action handlers. Right-click, and click test menu.	Harmless	Alert	None	IBM Director
1	Topology					
2	Offline	IBM Director Agent is offline.	Harmless	Alert	None	IBM Director
2	Online	IBM Director Agent is online.	Harmless	Resolution	None	IBM Director

Chapter 9. Mass Configuration events

These events are sent by the Mass Configuration tool associated with the Asset ID, Configure Alert Standard Format, Configure SNMP Agent, and Network Configuration tasks. When configuring the Mass Configuration profiles for these tasks, an **Enable Changes** check box is provided. You must select this check box to enable access for other administrators to change the configured values. If the check box is selected and an administrator without access attempts to change a value, the Overwritten event is sent.

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Table 17. Mass Configuration events

Tree node	Event type	Description	Severity	Resolution or alert	Generated by OS or by IBM Director
2	Conflict	More than one profile that has a value for the same field has been applied to a system.	Warning	Alert	IBM Director
2	Overwritten	More than one server has sent mass configuration profiles to a system.	Warning	Alert	IBM Director

Chapter 10. Management Processor Assistant (MPA) events

Events are generated by the MPA Agent locally in response to indications sent from an in-band service processor. Service processors that have been properly configured will forward events over the LAN to IBM Director Server. IBM Director Server maps these events to one of the events that is displayed in the MPA tree. Any xSeries server and BladeCenter unit that has a supported service processor can forward events to IBM Director Server. For more information, see the *IBM Director 4.1 Systems Management Guide.* When events are generated by IBM Director Server in response to an event received from a service processor over a LAN, the target managed object of the specific event might vary.

The availability of certain extended attributes will vary depending on the system from which an event is generated.

Service processor type	Target system
RXE-100 Remote Expansion Enclosure	RIOEnclosure
ISMP, Remote Supervisor Adapter, Remote Supervisor Adapter II system	Physical Platform and associated IBM Director Server
Advanced System Management processor (ASM processor) or Advanced System Management PCI adapter (ASM PCI adapter) system running the MPA Agent.	Physical Platform and associated IBM Director Server
ASM processor or ASM PCI adapter system not running the MPA Agent.	None; the source will be identified as the IP address of the service processor that sent the indication to the management server.

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.

- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Component events

The component events provide information about specific components located on your systems.

Table 18. MPA component events

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
1	Component				*Source UUID* and *Sender UUID*, provide the universally unique identifier of the source and sender physical systems. *Unit* identifies the component that has failed.
2	Chassis				
3	Configuration	A problem with the configuration of the system was detected.	Minor	Alert	There is an additional attribute of `issue` available for this event. It can have one of the following values: • `blade_power` Blade inserted in a slot with no power. • `rs485` RXE-100 Remote Expansion Enclosure local RS485 is improperly cabled. • `pci` RXE-100 Remote Expansion Enclosure has a PCI configuration error.
		Configuration issue has been resolved.	Harmless	Resolution	
3	Failed	There is a serious problem with the chassis.	Critical	Alert	There is an additional attribute of `issue` available for this event. It can have one of the following attributes: • `no-fans` The BladeCenter unit does not have any operational fans. • `all_ps_over_temp` All BladeCenter power supplies are over temperature.
		The problem has been resolved.	Harmless	Resolution	

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
2	DASD				There are two additional attributes available: *unit* which indicates the target drive by physical location or *SCSI Id* which indicates the target drive by SCSI Id.
3	Failed	Hard disk drive has failed.	Minor	Alert	
		Hard disk drive has recovered.	Harmless	Resolution	
3	Inserted	Hard disk drive has been inserted.	Harmless	Alert	
3	Removed	Hard disk drive has been removed.	Warning	Alert	
2	Fan				
3	Failed	Fan has failed.	Critical	Alert	
3	Recovered	Fan has recovered.	Harmless	Resolution	
3	Inserted	Fan has been inserted.	Harmless	Alert	
3	Removed	Fan has been removed.	Warning	Alert	

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
3	PFA	A Predictive Failure Analysis® (PFA) has been detected for a fan.	Warning	Alert	
		The fan is no longer in a state of PFA.	Harmless	Resolution	
3	Removed	Fan has been removed.	Warning	Alert	
2	KVM (keyboard, video, mouse)				
3	Owner	Failed to switch KVM owner.	Critical	Alert	
		The KVM has successfully switched after a previous failure.	Harmless	Resolution	
2	Management Processor				
3	Configuration	Changes in configuration have been made.			
3	Log	Log is full.	Minor	Alert	
		Log is 75% full.	Warning	Alert	
		Log has been cleared.	Harmless	Resolution	

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
3	Network Stack	Verifies that the service processor network stack has restarted. This event notifies IBM Director if the IP address used by a service processor has changed.	Warning	Alert	There are two attributes: • *IP Address 1* which is the IP address used by network interface 1 (external interface on the BladeCenter management module). • *IP Address 2* which is the IP address used by network interface 2 (internal interface on the BladeCenter management module). The data for each attribute is a hexadecimal string representing the four bytes of an IP address.

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
2	Memory DIMM				
3	Failed	Memory dual inline memory module (DIMM) has failed.	Warning	Alert	
		Memory DIMM has recovered.	Harmless	Resolution	
2	PFA	A PFA has been detected for a component.	Warning	Alert	
2	Power Subsystem				
3	Low Fuel	The power subsystem is in a low-fuel state.	Critical	Alert	
		The power subsystem is no longer in a low-fuel state.	Harmless	Resolution	
3	Over Current	Current draw exceeds maximum rating.	Critical	Alert	
		Current draw no longer exceeds maximum rating.	Harmless	Resolution	
3	Over Power	Power draw on a bus exceeds maximum.	Critical	Alert	When generated for an RXE-100 Remote Expansion Enclosure, an attribute by the name of `bus` is present. This attribute identifies the main power bus where the failure occurred. It is identified by the letter A, B, C, or D.

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
		Power draw on a bus no longer exceeds maximum.	Harmless	Resolution	
3	Redundancy	Loss of redundancy has occurred.	Minor	Alert	
		Loss of redundancy has recovered.	Harmless	Resolution	
2	Power Supply				
3	Failed	Power supply has failed.	Critical	Alert	There is an attribute of *Reason* identifying the reason the power supply failed. This attribute has one of the following values: • *epow* - early off power warning • *dc* - DC good is no longer detected • *current* - the power supply is over current • *power_good* - the power supply is no longer supporting good power • *voltage_over* - the power supply is supporting a voltage above its range • *voltage_under* - the power supply is supporting a voltage that is under its range
		Power supply has recovered.	Harmless	Warning	

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
3	Inserted	Power supply has been inserted.	Harmless	Alert	
3	Removed	Power supply has been removed.	Warning	Alert	
2	Processor Blade				
3	Inserted	Processor blade has been inserted.	Harmless	Alert	
3	Removed	Processor blade has been removed.	Warning	Alert	
2	Server	IBM Director received an unknown event from the service processor indicating a fault.	Critical	Alert	Firmware code (server event type only). This is a hexadecimal string identifying the unknown event that is received.
		IBM Director received an unknown event from a service processor indicating a recovery.	Harmless	Warning	
3	Power				
4	Off	Server has been powered off.	Harmless	Alert	
4	On	Server has been powered on.	Harmless	Resolution	
2	Switch Module				

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
3	Configuration	Switch configuration has changed.	Harmless	Alert	The *IP Address 1* attribute identifies the IP address being used by the BladeCenter switch module.

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
3	Failed	Switch module has failed.	Critical	Alert	
		Switch module has recovered.	Harmless	Resolution	
3	Inserted	Switch module has been inserted.	Harmless	Alert	
3	Power				
4	Off	Switch module is powered off.	Warning	Alert	
4	On	Switch module is powered on.	Harmless	Alert	
3	Redundancy	Redundancy has been lost.	Minor	Alert	
3	Removed	Switch module has been removed.	Warning	Alert	
2	USB				
3	Inserted	Universal Serial Bus (USB) has been inserted.	Harmless	Alert	
3	Owner	Indicates that an error occurred trying to reassign shared USB media to a new owner.	Minor	Alert	
3	Removed	USB has been removed.	Warning	Alert	
2	VRM				

Table 18. MPA component events (continued)

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
3	Failed	Voltage Regulator Module (VRM) has failed.	Critical	Alert	
		A recovery has occurred.	Harmless	Resolution	

Deployment events

Deployment events have four types of deployment: Boot (restart) deployment, operating-system deployment, operating-system loader, and Power On Self Test (POST) deployment. For servers with service-processor firmware, a recovery event exists for each of these event types.

Table 19. Deployment events

Tree node	Event types	Description	Severity	Resolution or alert	Extended attributes
1	Deployment				Sender UUID and Source UUID

Table 19. Deployment events (continued)

Tree node	Event types	Description	Severity	Resolution or alert	Extended attributes
2	BOOT	The operating system has failed to start.	Critical	Alert	
		The operating system started after a previous failure.	Harmless	Resolution	
2	OS	Operating system stopped.	Critical	Alert	
		Operating system has restarted after it stopped.	Harmless	Resolution	
2	OS Loader	The OS loader failed to assume control over the system.	Critical	Alert	
		Control was successfully passed the OS loader after a previous failure.	Harmless	Resolution	
2	POST	The system failed to complete POST.	Critical	Alert	
		The system successfully completed POST after a previous failure.	Harmless	Resolution	

Environmental events

The environmental event reports the system temperature and voltage. If the firmware supports recoveries, there are recovery events for both of these environmental event types when the value returns to the warning reset threshold.

Table 20. Environmental events

Tree node	Event types	Description	Severity	Resolution or alert	Extended attributes
1	Environment				Sender UUID, Source UUID, Side. If the fault originated in an RXE-100 Remote Expansion Enclosure where side A or B is where the fault is located.
2	Temperature	Temperature has exceeded the shutdown threshold.	Critical	Alert	Temperature Sensor having one of the following problems: • Ambient • Management processor • CPU • DASD • Power supply • Switch module The *Unit* attribute is applicable if the sensor is associated with a component for which there are multiple power supplies.
		Temperature has exceeded the warning threshold.	Minor	Alert	
		Temperature has fallen below the warning reset threshold.	Harmless	Resolution	

Table 20. Environmental events (continued)

Tree node	Event types	Description	Severity	Resolution or alert	Extended attributes
2	Voltage	The value of this specific voltage is outside of the shutdown threshold.	Critical	Alert	The *voltage sensor* attribute identifies the voltage sensor where the fault occurred. • 5V Standby • 3.35V Standby • 5V PCI • 3.35V PCI • 18V • 12V • 5V • 3.35V • 2.5V • 1.8V • 1.5V • 1.25V • -5V • -12V • 1.25V • 18V This is high if the voltage exceeded the threshold, or low if the voltage fell below the threshold of the attribute identifier where the fault occurred. It can be the daughter card, the system, or the voltage regulator module.

Table 20. Environmental events (continued)

Tree node	Event types	Description	Severity	Resolution or alert	Extended attributes
		The value of this specific voltage is outside the warning threshold.	Minor	Alert	
		The value of this specific voltage is now within the warning reset threshold.	Harmless	Resolution	

Platform events

You can use these platform events to monitor the state of the nodes that are part of a scalable partition.

Table 21. Platform events

Tree node	Event type	Description	Severity	Resolution or alert	Extended attributes
1	Logical Platform		Warning	Alert	Sender UUID, Source UUID,

Table 21. Platform events (continued)

2	Alert		Warning	Alert	
2	State				
3	Null	State of the server is null.	Harmless	Alert	
3	Powered Off	State of the server is powered off.	Harmless	Alert	
3	Powering On	State of the server is powering on.	Harmless	Alert	
3	Powered On	State of the server is powered on.	Harmless	Resolution	
3	Resetting	State of the server is resetting.	Warning	Alert	
3	Shutting Down	State of the server is shutting down.	Warning	Alert	
1	Physical Node				
2	Mode				
3	Null	State of the physical node is null.	Harmless	Resolution	
3	Primary	The mode of the physical node is primary. (This is the primary node in a multinode system.)	Harmless	Resolution	
3	Secondary	The mode of the physical node is secondary. (This node is not the primary node in a multinode system.)	Warning	Alert	

Table 21. Platform events (continued)

3	Standalone	The mode of the physical node is standalone. (This mode is set for a single node system.)	Warning	Alert	
2	Standalone				
4	Mode				
6	Primary	The physical node (which is a primary node in a multinode system) has entered permanent standalone mode.	Warning	Alert	
6	Secondary	The physical node (which is a secondary node in a multinode system) has entered permanent standalone mode.	Warning	Alert	
5	Reset				
6	Primary	The physical node (which is a primary node in a multinode system) has entered standalone mode.	Warning	Alert	
6	Secondary	The physical node (which is a secondary node in a multinode system) has entered standalone mode.	Warning	Alert	

Component events technical information

This component events information is helpful when working with upward integration modules (UIMs).

Table 22. MPA events component technical information

Tree node	Event type	Event qualifier	Extended attributes
1	Component	component	The attributes: • event.asm.uuid.source • event.asm.uuid.sender provide the UUID of the source and sender physical systems respectively. The *event.asm.unit* attribute is the one-based index of the failing component.
2	Chassis	component.chassis	
3	Configuration	component.chassis.configuration	The attribute *event.asm.issue* can have the following values: • *blade_power* Blade Server inserted in a slot with no power. • *rs485* RXE-100 Remote Expansion Enclosure local RS485 is improperly cabled. • *pci* RXE-100 Remote Expansion Enclosure has a PCI configuration error.
3	Failed	component.chassis.failed	The attribute `event.asm.issue` can have the following values: • *no-fans* The BladeCenter unit does not have any operational fans. • *all_ps_over_temp* All BladeCenter power supplies are over temperature.

Table 22. MPA events component technical information (continued)

Tree node	Event type	Event qualifier	Extended attributes
2	DASD	component.dasd	There are two attributes; • *event.asm.unit* which identifies the target drive by physical location • *event.asm.SCSI Id*, which identifies the target drive by SCSI ID.
3	Failed	component.dasd.failed	
3	Inserted	component.dasd.inserted	
3	Removed	component.dasd.removed	
2	Fan	component.fan	
3	Failed	component.fan.failed	
3	Inserted	component.fan.inserted	
3	Removed	component.fan.removed	
3	PFA	component.fan.pfa	
2	KVM (keyboard, video, mouse)	component.kvm	
3	Owner	component.kvm.owner	
2	Management Processor	component.management_processor	
3	Configuration	component.management_processor.configuration	
3	Log	component.management_processor.log	

Table 22. MPA events component technical information (continued)

Tree node	Event type	Event qualifier	Extended attributes
3	Network Stack	component.management_processor.network.stack	There are two attributes: • *event.asm.ip1* is the IP address used by network interface 1 (external interface on the BladeCenter management module). • *event.asm.ip2* is the IP address used by network interface 2 (internal interface on the BladeCenter management module). The data for each attribute is a hexadecimal string representing the four bytes of an IP address.
2	Memory DIMM	component.memory	
3	Failed	component.memory.failed	
2	PFA	component.pfa	
2	Power Subsystem	component.power_subsystem	
3	Low Fuel	component.power_subsystem.low_fuel	
3	Over Current	component.power_subsystem.over_current	
3	Over Power	component.power_subsystem.over_power	If the event is generated for an RXE-100 Remote Expansion Enclosure, the attribute *event.asm.bus* is available. It identifies the power bus where the fault occurred, and has a value of A,B,C, or D.
3	Redundancy	component.power_subsystem.redundancy	
2	Power Supply	component.power_supply	*event.asm.unit* identifies the component.

Table 22. MPA events component technical information (continued)

Tree node	Event type	Event qualifier	Extended attributes
3	Failed	component.power_supply.failed	
3	Inserted	component.power_supply.inserted	
3	Removed	component.power_supply.removed	
2	Processor Blade	component.processor_blade	*event.asm.unit* identifies the component.

Table 22. MPA events component technical information (continued)

Tree node	Event type	Event qualifier	Extended attributes
3	Inserted	component.processor_blade.inserted	
3	Removed	component.processor_blade.removed	
2	Server	component.server	
3	Power	component.power	
4	Off	component.server.power.off	
4	On	component.server.power.on	
2	Switch Module	component.switch_module	
3	Configuration	component.switch_module.configuration	
3	Failed	component.switch_module.failed	
3	Inserted	component.switch_module.inserted	
3	Power	component.switch_module.power	
4	Off	component.switch_module.power.off	
4	On	component.switch_module.power.on	
3	Redundancy	component.switch_module.redundancy	
3	Removed	component.switch_module.redundancy	
2	USB	component.usb	
3	Inserted	component.usb.inserted	
3	Owner	component.usb.owner	
3	Removed	component.usb.removed	
2	VRM	component.vrm	
3	Failed	component.vrm.failed	

Deployment events technical information

Deployment events have four types of deployment: Boot (restart) deployment, operating-system deployment, operating-system loader, and POST deployment. For servers with service-processor firmware, a recovery event exists for each of these event types.

Table 23. Deployment events

Tree node	Event types	Event qualifier	Extended attributes
1	Deployment	deployment	event.asm.uuid.source event.asm.uuid.sender
2	Boot	deployment.boot	
2	OS	deployment.os	
2	OS Loader	deployment.loader	
2	POST	deploymnet.post	

Environmental events technical information

The environmental event provides the system temperature. If the firmware supports recoveries, there are recovery events for both of these environmental event types when the value returns to the warning reset threshold.

Table 24. Environmental events

Tree node	Event types	Event qualifier	Extended attributes
1	Environment		• event.asm.uuid.source • event.asm.uuid.sender • event.asm.side If the fault originated in an RXE-100 Remote Expansion Enclosure on which side A or B is where the fault is located.
2	Temperature	environmental.temperature	• event.asm.temperature Temperature sensor is having one of the following problems: ambient, management processor, CPU, DASD, power supply, switch module. • event.asm.unit If the sensor is associated with a component of which there are more than one, this attribute identifies the component.

Table 24. Environmental events (continued)

Tree node	Event types	Event qualifier	Extended attributes
2	Voltage	environmental.voltage	• event.asm.voltage Where the detected voltage might be one of the following: – 5V Standby – 3.35V Standby – 5V PCI – 3.35V PCI – 18V – 12V – 5V – 3.35V – 2.5V – 1.8V – 1.5V – 1.25V – -5V – -12V – 1.25V – 18V • event.asm.threshold Identifies where the voltage exceeded a high threshold or fell below a low threshold. • event.asm.component Indicates the daughter card, the system, or the voltage regulator module.

Platform events technical information

You can use platform events to monitor the state of the nodes that are part of a scalable partition.

Table 25. Platform events

Tree node	Event type	Event qualifier	Severity	Extended attributes
1	Logical Platform			event.asm.uuid.source event.asm.uuid.sender
2	Alert	platform.logical_platform.alert	Warning	
2	State			
3	Null	platform.logical_platform.state.null	Harmless	
3	Powered Off	platform.logical_platform.state.powered_off	Harmless	
3	Powered On	platform.logical_platform.state.powered_on	Harmless	
3	Powering On	platform.logical_platform.state.powering_on	Harmless	
3	Resetting	platform.logical_platform.state.resetting	Harmless	
3	Shutting Down	platform.logical_platform.state.shutting_down	Harmless	
1	Physical Node			
2	Mode			
3	Null	platform.physical_node.mode.null	Harmless	
3	Primary	platform.physical_node.mode.primary	Harmless	
3	Secondary	platform.physical_node.mode.secondary	Harmless	
3	Standalone	platform.physical_node.mode.standalone	Harmless	
4	Mode			
5	Primary	platform.physical_node.standalone.mode.primary	Harmless	
5	Secondary	platform.physical_node.standalone.mode.secondary	Harmless	

Table 25. Platform events (continued)

5	Reset			
6	Primary	platform.physical_node.mode.reset.primary	Harmless	
6	Secondary	platform.physical_node.mode.reset.secondary	Harmless	

Chapter 11. SNMP events

When you compile MIB files they contain the trap definition of the traps that are displayed under the SNMP tree node in the Event Filter Builder. SNMP traps are generated by the SNMP agents that are installed on the SNMP devices being managed by IBM Director Server.

The trap definitions can conform to either SNMP v1 or SNMP v2. The root node for the traps in the Event Filter Builder is SNMP.iso.org.internet. The exact subnode under which the traps are displayed depends on which branch of the standard MIB the traps' MIB is under: experimental, mgmt, private, or snmpV2. Trap definitions from most MIBs, are displayed under the private subnode SNMP.iso.org.internet.private. Traps defined in the standard MIBs, such as MIB II, are displayed under the mgmt subnode SNMP.iso.org.internet.mgmt. There are two additional trees displayed under the SNMP node:

- **Hardware** - The event types displayed under the Hardware node are for IBM hardware known to send SNMP traps such as Alert on LAN NICs, the BladeCenter FibreChannel switch, ServeRAID adapters, tape drives, and UPS devices.
- **Software** - The event types displayed under the Software node correspond to software packages known to send SNMP traps such as BrightStor Arcserve, Veritas Backup Exec, and IBM Netfinity® Manager.

Note: When using these tables, be sure to remember the following information:

- The "Event type" column identifies the name of the event.
- The "Description" column provides a description of the event type.
- The "Severity" column identifies the severity of the event.
- The "Extended attributes" column for these traps are the community names and the variable bindings.
- The events in the following table are displayed under SNMP.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps

Table 26. SNMP events

Event type	Description	Severity	Extended attributes
Authentication failure	The SNMP entity has received a protocol message that is not properly authenticated. Typically, SNMP entities might be capable of generating this trap; the snmpEnableAuthenTraps object indicates whether this trap is generated.	Unknown	The community name and any of the variable bindings that come with the trap.
ColdStart	The SNMP entity supporting a notification originator application, is reinitializing itself and the configuration might have been altered.	Unknown	The community name and any of the variable bindings that come with the trap.
LinkDown	The SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from another state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	Unknown	The community name and any of the variable bindings that come with the trap.
LinkUp	The SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from another state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	Unknown	The community name and any of the variable bindings that come with the trap.
WarmStart	The SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered.	Unknown	The community name and any of the variable bindings that come with the trap.

Chapter 12. Software Rejuvenation events

Software Rejuvenation events are displayed in the event log for a specific managed system. You can use an event action plan for software rejuvenation events by specifying the events in the Event Action Plan Builder when creating event filters. For more information on Software Rejuvenation, see the *IBM Director 4.1 Systems Management Guide.*

Note: When using these tables, be sure to remember the following information:

- The “Tree node” column identifies the tree node in which the event is displayed.
- The “Event type” column identifies the name of the event.
- The “Description” column provides a description of the event type.
- The “Severity” column identifies the severity of the event.
- The “Resolution or alert” column identifies whether the event is an alert or a resolution.
- The “Generated by OS or by IBM Director” column identifies if the event is generated by IBM Director or by the operating system of the system being monitored.

Prediction

The Software Rejuvenation events are for creating prediction events.

Table 27. Software Rejuvenation prediction

Tree node	Event type	Description	Severity	Generated by OS or IBM Director
1	Linux Resource			
2	Breach Limit	100% of the available resource have been used.	Critical	IBM Director

Table 27. Software Rejuvenation prediction (continued)

Tree node	Event type	Description	Severity	Generated by OS or IBM Director
2	Exhaustion	The percentage of resources used has exceeded the automatically determined notify level as displayed in the Software Rejuvenation Trend Viewer.	Critical	IBM Director
1	Reconfigured	Prediction was reconfigured from a management server.	Harmless	IBM Director
1	Windows Resource			
2	Breach Limit	100% of the available resources have been used.	Critical	IBM Director
2	Exhaustion	The percentage of resources used has exceeded the automatically determined Notify Level as displayed in the Software Rejuvenation Trend Viewer.	Harmless	IBM Director

Schedule events

When the Scheduler is used to schedule software rejuvenation events or when prediction automatically schedules a rejuvenation, the following events might occur on managed systems that are running a Linux operating system.

Tree node	Event type	Description	Severity	Generated by OS or by IBM Director
1	Linux Daemon			
2	Cancelled			

Tree node	Event type	Description	Severity	Generated by OS or by IBM Director
3	Disabled	Rejuvenation Logic was not enabled in Rejuvenation Options.	Harmless	IBM Director
3	Minimum Rejuvenation Interval	Number of minimum rejuvenation interval days has not elapsed since the last rejuvenation.	Harmless	IBM Director
3	Node State Invalid	IBM Director Agent was inactive.	Harmless	IBM Director
3	Restricted	The day was restricted in the schedule filter but not ignored in the Prediction Configuration wizard.	Harmless	IBM Director
2	Deleted	Schedule was deleted on the Software Rejuvenation calendar.	Harmless	IBM Director
2	Failed	Scheduled software rejuvenation has failed.	Harmless	IBM Director
2	Scheduled	Software rejuvenation has been successfully scheduled.	Harmless	IBM Director
2	Succeeded	Scheduled rejuvenation was successful.	Harmless	IBM Director
1	Linux Server			
2	Cancelled	Rejuvenation was cancelled.	Harmless	IBM Director
3	Missed	Scheduled rejuvenation time was earlier than the current time.	Harmless	IBM Director
3	Minimum Rejuvenation Interval	The minimum number of rejuvenation days has not elapsed since the last rejuvenation.	Harmless	IBM Director
3	Missed	IBM Director Agent was inactive.	Harmless	IBM Director
3	Node State Invalid			

Tree node	Event type	Description	Severity	Generated by OS or by IBM Director
3	Restricted	The day was restricted in the schedule filter but not ignored in the Prediction Configuration wizard.	Harmless	IBM Director
2	Deleted	Schedule was deleted on the Software Rejuvenation calendar.	Harmless	IBM Director
2	Failed	Scheduled rejuvenation has failed.	Harmless	IBM Director
2	Scheduled	Rejuvenation has been successfully scheduled.	Harmless	IBM Director
2	Succeeded	Scheduled rejuvenation was successful.	Harmless	IBM Director
1	Windows Cluster Server			
2	Cancelled			
3	Minimum Rejuvenation Interval	The number of Minimum Rejuvenation Options has not elapsed since the last rejuvenation.	Harmless	IBM Director
3	Missed	Scheduled rejuvenation time was earlier than the current time.	Harmless	IBM Director
3	No Available Peers	No other cluster members were available.	Harmless	IBM Director
3	Node State Invalid	The IBM Director Agent was inactive.	Harmless	IBM Director
3	Peer State Invalid	Another cluster member was available, but IBM Director Agent was inactive.	Harmless	IBM Director

Tree node	Event type	Description	Severity	Generated by OS or by IBM Director
2	Deleted		Harmless	IBM Director
2	Failed		Harmless	IBM Director
2	Scheduled		Harmless	IBM Director
2	Succeeded		Harmless	IBM Director
1	Windows Service		Harmless	IBM Director
2	Cancelled		Harmless	IBM Director
3	Minimum Rejuvenation Interval	The minimum number of rejuvenation interval days has not elapsed since the last rejuvenation.	Harmless	IBM Director
3	Missed	Scheduled rejuvenation time was earlier than the current time.	Harmless	IBM Director
3	No Available Peers	No other cluster members were available.	Harmless	IBM Director
3	Node State Invalid	IBM Director Agent was inactive.	Harmless	IBM Director
3	Peer State Invalid	Another cluster member was available but IBM Director Agent was inactive.	Harmless	IBM Director
2	Deleted		Harmless	IBM Director
2	Failed		Harmless	IBM Director
2	Scheduled		Harmless	IBM Director
2	Succeeded		Harmless	IBM Director
1	Windows Server		Harmless	IBM Director
2	Cancelled	The schedule was cancelled.	Harmless	IBM Director
3	Disabled	The rejuvenation logic was not enabled in rejuvenation options.	Harmless	IBM Director

Tree node	Event type	Description	Severity	Generated by OS or by IBM Director
3	Minimum Rejuvenation Interval	The number of minimum rejuvenation interval days specified in Rejuvenation Options has not elapsed since the last rejuvenation.	Harmless	IBM Director
3	Missed	Scheduled rejuvenation time was earlier than the current time.	Harmless	IBM Director
3	No Available Peers	No other cluster members were available.	Harmless	IBM Director
3	Node State Invalid	IBM Director Agent was inactive.	Harmless	IBM Director
3	Peer State Invalid	Another cluster member was available but IBM Director Agent was inactive.	Harmless	IBM Director
3	Restricted	Day was restricted in the Schedule Filter and the schedule, due to a predicted exhaustion, was not selected to be ignored in the options for automatic scheduling in the Prediction Configuration wizard.	Harmless	IBM Director
2	Deleted			
2	Failed			
2	Scheduled			
2	Succeeded			
1	Windows Service			
2	Cancelled	Schedule was canceled.	Harmless	IBM Director
3	Disabled	Number of minimum rejuvenation options has not elapsed since the last rejuvenation.	Harmless	IBM Director
3	Minimum Rejuvenation Interval	Scheduled rejuvenation time was earlier than the current time.	Harmless	IBM Director

Tree node	Event type	Description	Severity	Generated by OS or by IBM Director
3	Missed	No other cluster members were available.	Harmless	IBM Director
3	Node State Invalid	IBM Director Agent was inactive.	Harmless	IBM Director
3	Restricted	Another cluster member was available but IBM Director Agent was inactive.	Harmless	IBM Director
2	Deleted	Number of minimum rejuvenation options had not elapsed since the last rejuvenation.	Harmless	IBM Director

Chapter 13. Storage (ServeRAID) events

The events under the Storage node in the Event Filter Builder are sent by the IBM ServeRAID Agent on all operating systems supported by IBM Director. The events are sent to notify IBM Director Server of state changes in the ServeRAID subsystem that are being reported by a supported ServeRAID adapter or an integrated SCSI controller with RAID capabilities. There is no relationship between the RAID events and the Hardware Status and System Health features of IBM Director.

Those features use the information provided by the CIM.Director Agent Events.ServeRAID Health events documented in Table 12 on page 67. On managed systems running the Windows operating system, both types of events are issued. Specifically, there is an event type Storage.* that reports the details of the state change. There will be a CIM.Director Agent Events.ServeRAID Overall Health event sent that reports the status of the overall RAID subsystem in light of the state change. Also, there will be a granular event type CIM.Director Agent Events.ServeRAID Health. The severity of the CIM.Director Agent Events.ServeRAID Overall Health event determines the severity level of the system in Hardware Status. The CIM.Director Agent Events.ServeRAID Health events provide a history of the RAID subsystem in the Hardware Status task when you select the ServeRAID node in this task.

There is additional information about the events and the ServeRAID adapter in the following chapters:

- Appendix A, “SNMP information”, on page 119.
- Appendix C, “IBM Director Agent events found in the Windows event log”, on page 196.
- There is additional information regarding ServeRAID health in Table 12 on page 67.

Note: Additional information about ServeRAID events will be provided soon in an updated edition of this book.

Appendix A. SNMP information

IBM Director Agent gathers system information and reads it in an SNMP format. The following information provides the events that IBM Director Agent sends, a short description of the event, and the variable binding details.

Note: When using these tables, be sure to remember the following information:

- The “Event attribute” column contains the object identifier (OID) of the trap, followed by the variable bindings of the trap.
- The “Value” column lists the OIDs of the variable bindings.
- The “Syntax” column identifies the data type of the variable bindings.
- The “Description” column provides the descriptions of the variable bindings. In the case of the description variable binding, the value of the description is provided in quotation marks.
- The “New in IBM Director 4.1″ column identifies events that are new in IBM Director 4.1.

iBMPSGTemperatureEvent

This event occurs when the state of a system temperature sensor changes with respect to a manufacturer-defined or user-defined threshold. The MIB file for this event is umsevent.MIB. The access is read-write and the status is mandatory. The TRAP-TYPE = 2, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 28. iBMPSGTemperatureEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGTemperatureEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.2		SNMP v1 standard OID defined in enterprise ’director’	No
iBMPSGTemperatureEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.2.1	String	Internal ID for this event type	

Table 28. iBMPSGTemperatureEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGTemperatureEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.2.2	String	CIM device ID value for the monitored temperature sensor instance	
iBMPSGTemperatureEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.2.3	String	CIM device ID value for the monitored temperature sensor instance	
iBMPSGTemperatureEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.2.4	Uint16	2 = Critical: The temperature has exceeded a user-defined or manufacturer-defined critical level threshold. 1 = Warning: The temperature has exceeded a user-defined or manufacturer-defined warning-level threshold. 0 = Normal: The temperature has returned to its normal value.	

Table 28. iBMPSGTemperatureEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGTemperatureEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.2.5	String	Critical = "Temperature Sensor %d exceeded the manufacturer/user defined threshold of %d Celsius/Fahrenheit. The current value is %d Celsius/Fahrenheit." Warning = "Temperature Sensor %d exceeded the manufacturer/user defined threshold of %d Celsius/Fahrenheit. The current value is %d Celsius/Fahrenheit." Normal = "Temperature Sensor %d reports normal."	
iBMPSGTemperatureEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.2.6	DateTime	The date and time when the state change occurred for the component. The Greenwich Mean Time (GMT) standard timestamp is used. For example: 20030416155614.000000-240.	

iBMVoltageEvent

This event occurs when the state of a system voltage sensor changes with respect to a

manufacturer-defined threshold. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 3, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 29. iBMPSGVoltageEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGVoltageEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.3		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGVoltageEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.3.1	String	Internal ID for this event type	
iBMPSGVoltageEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.3.2	String	CIM device ID value for the monitored voltage sensor instance	
iBMPSGVoltageEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.3.3	String	CIM device ID value for the monitored voltage sensor instance	
iBMPSGVoltageEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.3.4	Uint16	2 = Critical: The voltage has exceeded a manufacturer-defined critical threshold. 0 = Normal: The voltage has returned to its normal value.	
iBMPSGVoltageEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.3.5	String	Critical = "Voltage Sensor %d exceeded/fell below threshold of %.2f Volts. The current value is %.2f Volts." Normal = "Voltage Sensor %d reports normal."	

Table 29. iBMPSGVoltageEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGVoltageEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.3.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGChassisEvent

This event occurs when the state of a system chassis changes. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 4, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 30. iBMPSGChassisEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGChassisEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.4		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGChassisEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.4.1	String	Internal ID for this event type	
iBMPSGChassisEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.4.2	String	CIM device ID value for the system whose intrusion state is being monitored.	
iBMPSGChassisEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.4.3	String	CIM device ID value for the system whose intrusion state is being monitored.	

Table 30. iBMPSGChassisEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGChassisEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.4.4	Uint 16	2 = Critical: The system cover has been removed. 0 = Normal: The system cover has been replaced.	
iBMPSGChassisEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.4.5	String	Critical = “System Enclosure Sensor reported intrusion detection.” Normal = “System Enclosure Sensor reports normal.”	
iBMPSGChassisEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.4.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGFanEvent

This event occurs when the state of a system fan has changed with respect to manufacturer-defined Rotation per minute (RPM) values. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 5, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 31. iBMPSGFanEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGFanEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.5		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGFanEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.5.1	String	Internal ID for this event type	
iBMPSGFanEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.5.2	String	CIM device ID value for the monitored fan sensor instance	
iBMPSGFanEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.5.3	String	CIM device ID value for the monitored fan sensor instance	
iBMPSGFanEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.5.4	Uint16	2 = Critical: The fan fell below a critical threshold. 1 = Warning: The fan fell below a warning level threshold. 0 = Normal: The fan RPMs returned to normal levels.	
iBMPSGFanEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.5.5	String	Critical = "Fan Sensor %d fell below threshold of %d RPM. The current value is %d RPM." Warning = "Fan Sensor %d fell below threshold of %d. The current value is %d RPM." Normal = "Fan Sensor reports normal."	

Table 31. iBMPSGFanEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGFanEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.5.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGProcessorEvent (reserved for later use)

This event is a reserved trap type. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 6, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 32. iBMPSGProcessorEvent

Event attribute	Value	Syntax	Description
iBMPSGProcessorEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.6		
iBMPSGProcessorEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.6.1	String	
iBMPSGProcessorEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.6.2	String	
iBMPSGProcessorEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.6.3	String	
iBMPSGProcessorEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.6.4	Uint16	
iBMPSGProcessorEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.6.5	String	
iBMPSGProcessorEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.6.6	Datetime	

iBMPSGStorageEvent

This event occurs when the state of system hard disk drive space changes with respect to user-defined levels of hard disk drive space remaining. By default, the warning level is 5% remaining and critical level is

3% remaining. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 7, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 33. iBMPSGStorageEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGStorageEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.7		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGStorageEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.7.1	String	Internal ID for this event type	
iBMPSGStorageEventSourceObject Path	1.3.6.1.4.1.2.6.159.1.1.0.7.2	String	CIM device ID value for the monitored logical disk drive instance	
iBMPSGStorageEventTargetObject Path	1.3.6.1.4.1.2.6.159.1.1.0.7.3	String	CIM device ID value for the monitored logical disk drive instance	
iBMPSGStorageEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.7.4	Uint16	2 = Critical: The remaining disk space fell below a critical threshold. 1= Warning: The remaining disk space fell below a warning level threshold. 0 = Normal: The remaining disk space returned to normal levels.	

Table 33. iBMPSGStorageEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGStorageEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.7.5	String	Critical = “Logical drive %s fell below threshold of %0.2f MB. The current value is %0.2f MB.” Warning = “Logical drive %s fell below threshold of %0.2f MB. The current value is %0.2f MB.” Normal= “Logical drive %s free space is normal. The current value is %0.2f MB.”	
iBMPSGStorageEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.7.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGAssetEvent (reserved for later use)

This event is a reserved trap type. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 8, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 34. iBMPSGAssetEvent

Event attribute	Value	Syntax	Description
iBMPSGAssetEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.8.1		
iBMPSGAssetEvent.SourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.8.2	String	
iBMPSGAssetEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.8.3	String	
iBMPSGAssetEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.8.4	Uint16	
iBMPSGAssetEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.8.5	String	
iBMPSGAssetEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.8.6	Datetime	

iBMSMARTEvent

This event occurs when the state of an IDE or SCSI hard disk drive that complies with the self-monitoring, analysis, and reporting technology (SMART) changes with respect to its availability. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 9, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 35. iBMPSGSMARTEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGSMARTEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.9		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGSMARTEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.9.1	String	Internal ID for this event type	
iBMPSGSMARTEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.9.2	String	CIM device ID value for the monitored physical hard disk drive instance	
iBMPSGSMARTEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.9.3	String	CIM device ID value for the monitored physical hard disk drive instance	

Table 35. iBMPSGSMARTEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGSMARTEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.9.4	Uint16	2 = Critical: The hard disk drive is experiencing an imminent failure. 0 = Normal: The hard disk drive has been recovered.	
iBMPSGSMARTEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.9.5	String	Critical = “IDE/SCSI device identified as physical drive %i is predicting an imminent failure.” Normal = “IDE/SCSI device identified as physical drive %i is not predicting a failure.”	
iBMPSGSMARTEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.9.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGPOSTEvent (reserved for later use)

This event is a reserved trap type. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 10, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 36. iBMPSGPOSTEvent (reserved for later use)

Event attribute	Value	Syntax	Description
iBMPOSTEventIdentifier OID	1.3.6.1.4.1.2.6.159.1.1.0.10		
iBMPSGPOSTEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.10.1	String	
iBMPSGPOSTEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.10.2	String	
iBMPSGPOSTEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.10.3	String	
iBMPSGPOSTEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.10.4	Uint16	
iBMPSGPOSTEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.10.5	String	
iBMPSGPOSTEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.10.6	Datetime	

iBMPSGConfigurationChangeEvent (reserved for later use)

This event is a reserved trap type. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 11, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 37. iBMPSGConfigurationChangeEvent (reserved for later use)

Event attribute	Value	Syntax	Description
iBMPSGConfigurationChangeEventEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.11		
iBMPSGConfigurationChangeEvent Identifier	1.3.6.1.4.1.2.6.159.1.1.0.11.1	String	
iBMPSGConfigurationChangeEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.11.2	String	
iBMPSGConfigurationChangeEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.11.3	String	
iBMPSGConfigurationChangeEventEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.11.4	Uint16	
iBMPSGConfigurationChangeEventEventdescription	1.3.6.1.4.1.2.6.159.1.1.0.11.5	String	
iBMPSGConfigurationChangeEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.11.6	Datetime	

iBMPSGLANLeashEvent

This event occurs when the state of the system LAN connectivity changes with respect to the physical

connection between Alert on LAN-capable NICs and the LAN. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 12, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Note: This event is sent by IBM Director Agent 3.1.x and earlier versions that are installed on managed systems with Alert on LAN-capable NICs.

Table 38. iBMPSGLANLeashEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGLANLeashEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.12	String	SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGLANLeashEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.12.1	String	Internal ID for this event type	
iBMPSGLANLeashEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.12.2	String	CIM device ID value for the monitored system	
iBMPSGLANLeashEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.12.3	String	CIM device ID value for the monitored system	
iBMPSGLANLeashEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.12.4	Uint16	2 = Critical: The system has been disconnected from the network. 0 = Normal: The system is connected to the network.	
iBMPSGLANLeashEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.12.5	String	Critical = "The computer is disconnected from the network." Normal = "The computer is connected to the network."	

Table 38. iBMPSGLANLeashEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGLANLeashEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.12.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000 -240.	

iBMPSGLeaseExpirationEvent

This event occurs when the system lease expiration date has been reached with respect to the value configured for the date in the Asset ID task. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 13, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 39. iBMPSGLeashExpirationEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGLeaseExpirationEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.13		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGLeaseExpirationEvent.dentifier	1.3.6.1.4.1.2.6.159.1.1.0.13.1	String	Internal ID for this event type	
iBMPSGLeaseExpirationEventSourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.13.2	String	CIM device ID value for the system whose lease has expired.	

Table 39. iBMPSGLeashExpirationEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGLeaseExpirationEventTargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.13.3	String	CIM device ID value for the system whose lease has expired.	
iBMPSGLeaseExpirationEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.13.4	Uint16	1 = Warning: The system lease has expired. 0 = Normal	
iBMPSGLeaseExpirationEvent.Description	1.3.6.1.4.1.2.6.159.1.1.0.13.5	String	Warning = “The lease on %s expired. It expired on %s.” Normal = “The lease on %s is normal. It will expire on %s.”	
iBMPSGLeaseExpirationEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.13.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGWarrantyExpirationEvent

This event occurs when the system warranty expiration date has been reached with respect to the value configured for the date in the Asset ID task. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 14, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 40. iBMPSGWarrantyExpirationEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGWarrantyExpirationEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.14	String	SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGWarrantyExpirationEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.14.1	String	Internal ID for this event type	
iBMPSGWarrantyExpirationEventSourceObject Path	1.3.6.1.4.1.2.6.159.1.1.0.14.2	String	CIM device ID value for the system whose warranty has expired.	
iBMPSGWarrantyExpirationEventTargetObject Path	1.3.6.1.4.1.2.6.159.1.1.0.14.3	String	CIM device ID value for the system whose warranty has expired.	
iBMPSGWarrantyExpirationEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.14.4	Uint16	1= Warning, 0 = Normal	
iBMPSGWarrantyExpirationEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.14.5	String	Warning = "The warranty on %s has expired. It expired on %s." Normal ="The warranty on %s is normal. It will expire on %s."	
iBMPSGWarrantyExpirationEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.14.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614. 000000-240.	

iBMPSGRedundantNetworkAdapterEvent

This event occurs when the state of a system NIC changes state with respect to redundancy. There are certain limitations of the NIC that cannot be compensated for between a switchover and a switch back. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 15, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 41. iBMPSGRedundantNetworkAdapterEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGRedundantNetworkAdapterEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.15		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGRedundantNetworkAdapterEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.15.1	String	Internal ID for this event type	
iBMPSGRedundantNetworkAdapterEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.15.2	String	CIM device ID value for the source redundant NIC instance whose status has changed.	
iBMPSGRedundantNetworkAdapterEventTargetObject Path	1.3.6.1.4.1.2.6.159.1.1.0.15.3	String	CIM device ID value for the NIC instance whose status has changed.	
iBMPSGRedundantNetworkAdapterEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.15.4	Uint16	1 = Warning: A redundant NIC event occurred.	
iBMPSGRedundantNetworkAdapterEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.15.5	String	Warning = "A redundant NIC event occurred."	

Table 41. iBMPSGRedundantNetworkAdapterEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGRedundantNetworkAdapterEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.15.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614. 000000-240.	

iBMPSGRedundantNetworkAdapterSwitchoverEvent

This event occurs in a teamed NIC configuration when the active NIC in the team fails over to the standby NIC. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 16, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 42. iBMPSGRedundantNetworkAdapterSwitchoverEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGRedundantNetworkAdapterSwitchoverEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.16	String	SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGRedundantNetworkAdapterSwitchoverEvent Identifier	1.3.6.1.4.1.2.6.159.1.1.0.16.1	String	Internal ID for this event type	

Table 42. iBMPSGRedundantNetworkAdapterSwitchoverEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGRedundantNetworkAdapterSwitchoverEvent SourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.16.2	String	CIM device ID value for the monitored NIC instance	
iBMPSGRedundantNetworkAdapterSwitchoverEvent TargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.16.3	String	CIM device ID value for the monitored network adapter instance	
iBMPSGRedundantNetworkAdapterSwitchoverEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.16.4	Uint16	1 = Warning: A failing NIC failed over to a redundant NIC.	
iBMPSGRedundantNetworkAdapterSwitchoverEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.16.5	String	Warning = “NIC in Port/PCI Slot %d has Switched Over”	
iBMPSGRedundantNetworkAdapterSwitchoverEventTime Stamp	1.3.6.1.4.1.2.6.159.1.1.0.16.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 2003041615561 000000-240	

iBMPSGRedundantNetworkAdapterSwitchbackEvent

This event occurs in a teamed NIC configuration when the primary NIC in the team is restored. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 17, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 43. iBMPSGRedundantNetworkAdapterSwitchbackEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGRedundantNetworkAdapterSwitchbackEvent	1.3.6.1.4.1.2.6.159.1.1.0.17	String	SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGRedundantNetworkAdapterSwitchbackEvent Identifier	1.3.6.1.4.1.2.6.159.1.1.0.17.1	String	Internal ID for this event type	
iBMPSGRedundantNetworkAdapterSwitchbackEvent SourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.17.2	String	CIM device ID value for the monitored NIC instance.	
iBMPSGRedundantNetworkAdapterSwitchbackEvent TargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.17.3	String	CIM device ID value for the monitored NIC instance.	
iBMPSGRedundantNetworkAdapterSwitchbackEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.17.4	Uint16	1= Warning: The system NIC has recovered and switched back, reinstating redundancy.	

Table 43. iBMPSGRedundantNetworkAdapterSwitchbackEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGRedundantNetworkAdapterSwitchback EventDescription	1.3.6.1.4.1.2.6.159.1.1.0.17.5	String	Warning = “NIC in Port/PCI Slot %d has Switched Back”	
iBMPSGRedundantNetworkAdapterSwitchbackEvent TimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.17.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614 000000-240.	

iBMPSGProcessorPFEvent

This event occurs when the state of a system processor changes with respect to availability. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE =18, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 44. iBMPSGProcessorPFEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGProcessorPFEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.18		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGProcessorPFEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.18.1	String	Internal ID for this event type	
iBMPSGProcessorPFEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.18.2	String	CIM device ID value for the monitored processor instance	
iBMPSGProcessorPFEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.18.3	String	CIM device ID value for the monitored processor instance	
iBMPSGProcessorPFEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.18.4	Uint16	2 = Critical: The system processor is experiencing an imminent failure. 0 = Normal: The system processor has been restored.	
iBMPSGProcessorPFEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.18.5	String	Critical = "Processor device identified as processor in slot %d is predicting an imminent failure." Normal = "Processor device identified as processor in slot %d is not predicting a failure."	
iBMPSGProcessorPFEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.18.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGMemoryPFEvent

This event occurs when a memory DIMM in a system changes with respect to availability. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 19, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 45. iBMPSGMemoryPFEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGMemoryPFEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.19		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGMemoryPFEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.19.1	String	Internal ID for this event type	
iBMPSGMemoryPFEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.19.2	String	CIM device ID value for the monitored memory DIMM.	
iBMPSGMemoryPFEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.19.3	String	CIM device ID value for the monitored memory DIMM.	
iBMPSGMemoryPFEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.19.4	Uint16	2 = Critical: The memory device is predicting an imminent failure. 0 = Normal: The memory device is not predicting an imminent failure.	
iBMPSGMemoryPFEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.19.5	String	Critical = "Memory device identified as memory in bank %d is predicting an imminent failure." Normal = "Memory device identified as memory in bank %d is not predicting a failure."	

Table 45. iBMPSGMemoryPFEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGMemoryPFEventTime Stamp	1.3.6.1.4.1.2.6.159.1.1.0.19.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGPFAEvent

This event occurs when the Remote Supervisor Adapter detects that a component in a system is about to fail. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 22, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 46. iBMPSGPFAEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGPFAEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.22		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGPFAEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.22.1	String	Internal ID for this event type	
iBMPSGPFAEventSourceObject Path	1.3.6.1.4.1.2.6.159.1.1.0.22.2	String	text string: System Management Processor PFA	
iBMPSGPFAEventTargetObject Path	1.3.6.1.4.1.2.6.159.1.1.0.22.3	String	text string: System Management Processor PFA	
iBMPSGPFAEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.22.4	Uint16	2 = Critical: The system is experiencing an imminent failure.	

Table 46. iBMPSGPFAEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGPFAEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.22.5	String	Critical = “Predictive Failure Detected. Please check the system management processor error log for more information. This event must be cleared manually.”	
iBMPSGPFAEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.22.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGPowerSupplyEvent

This event occurs when the state of a system power supply changes with respect to availability. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 23, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 47. iBMPSGPowerSupplyEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGPowerSupplyEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.23		SNMP v1 standard OID defined in enterprise ’director’	No
iBMPSGPowerSupplyEvent Identifier	1.3.6.1.4.1.2.6.159.1.1.0.23.1	String	Internal ID for this event type	
iBMPSGPowerSupplyEvent SourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.23.2	String	CIM device ID value for the monitored power supply instance	

Table 47. iBMPSGPowerSupplyEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGPowerSupplyEvent TargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.23.3	String	CIM device ID value for the monitored power supply instance	
iBMPSGPowerSupplyEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.23.4	Uint16	2 = Critical: A power supply in a system has failed. 1 = Warning: A power supply is experiencing an imminent failure. 0 = Normal: The power supply has been recovered.	
iBMPSGPowerSupplyEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.23.5	String	Critical = “PowerSupply device identified as PowerSupply %d reports critical state with possible loss of redundancy.” Warning = “Power Supply device identified as PowerSupply %d has lost AC power and loss of standby power is imminent.” Normal = “PowerSupply device identified as PowerSupply %d reports normal.”	
iBMPSGPowerSupplyEvent TimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.23.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGErrorLogEvent

This event occurs when the Remote Supervisor Adapter detects that its error log is 75% or 100% of its capacity. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 24, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 48. iBMPSGErrorLogEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGErrorLogEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.24		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGErrorLogEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.24.1	String	Internal ID for this event type	
iBMPSGErrorLogEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.24.2	String	text string: System Management Processor Log	
iBMPSGErrorLogEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.24.3	String	text string: System Management Processor Log	
iBMPSGErrorLogEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.24.4	Uint16	1=Warning: The Remote Supervisor Adapter error log is 75% full. 2=Critical: The Remote Supervisor Adapter error log is 100% full.	
iBMPSGErrorLogEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.24.5	String	Critical = "The system management processor error log is full. This event must be cleared manually." Warning = "The system management processor error log is 75% full. This event must be cleared manually."	

Table 48. iBMPSGErrorLogEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGErrorLogEventTime Stamp	1.3.6.1.4.1.2.6.159.1.1.0.24.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGRemoteLoginEvent

This event occurs when an end-user or application has logged into the Remote Supervisor Adapter. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 25, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 49. iBMPSGRemoteLoginEvent

Event attribute	Value	Severity	Description	New in IBM Director 4.1
iBMPSGRemoteLoginEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.25		SNMP v1 standard OID defined in enterprise 'director'	No
iBMPSGRemoteLoginEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.25.1	String	Internal ID for this event type	
iBMPSGRemoteLoginEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.25.2	String	text string: System Management Processor Remote Login	
iBMPSGRemoteLoginEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.25.3	String	text string: System Management Processor Remote Login	
iBMPSGRemoteLoginEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.25.4	Uint16	1 = Warning: A user or application has logged in remotely to the Remote Supervisor Adapter	

Table 49. iBMPSGRemoteLoginEvent (continued)

Event attribute	Value	Severity	Description	New in IBM Director 4.1
iBMPSGRemoteLoginEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.25.5	String	Warning = "The system management processor has been accessed via a remote login. This event must be cleared manually."	
iBMPSGRemoteLoginEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.25.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGNetworkAdapterFailedEvent

This event occurs when a NIC in a system fails. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 27, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 50. iBMPSGNetworkAdapterFailedEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGNetworkAdapterFailedEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.26		SNMP v1 standard OID defined in enterprise 'director'	Yes
iBMPSGNetworkAdapterFailedEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.26.1	String	Internal ID for this event type	

Table 50. iBMPSGNetworkAdapterFailedEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGNetworkAdapterFailedEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.26.2	String	Standard CIM ObjectPath value for the monitored NIC instance	
iBMPSGNetworkAdapterFailedEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.26.3	String	Standard CIM ObjectPath value for the monitored NIC instance	
iBMPSGNetworkAdapterFailedEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.26.4	Uint16	2=Critical: The NIC referenced in the target object path has failed	
iBMPSGNetworkAdapterFailedEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.26.5	String	Critical= “The NIC in Port/PCI Slot %d has Failed”	
iBMPSGNetworkAdapterFailedEvent TimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.26.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	
iBMPSGNetworkAdapterFailedEvent ComponentID	1.3.6.1.4.1.2.6.159.1.1.0.26.7	Uint16	The physical PCI slot number or the onboard port number of the NIC.	

iBMPSGNetworkAdapterOfflineEvent

This event occurs when a NIC in a system goes offline. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 27, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 51. iBMPSGNetworkAdapterOfflineEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGNetworkAdapterOfflineEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.27		SNMP v1 standard OID defined in enterprise 'director'	Yes
iBMPSGNetworkAdapterOfflineEvent Identifier	1.3.6.1.4.1.2.6.159.1.1.0.27.1	String	Internal ID for this event type	
iBMPSGNetworkAdapterOfflineEvent SourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.27.2	String	Standard CIM ObjectPath value for the monitored network adapter instance.	
iBMPSGNetworkAdapterOfflineEvent TargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.27.3	String	Standard CIM ObjectPath value for the monitored network adapter instance.	
iBMPSGNetworkAdapterOfflineEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.27.4	Uint16	1 = Warning: The network adapter referenced in the target object path has gone offline.	
iBMPSGNetworkAdapterOfflineEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.27.5	String	Warning = "NIC in Port/PCI Slot %d is Offline"	

Table 51. iBMPSGNetworkAdapterOfflineEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGNetworkAdapterOfflineEvent TimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.27.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	
iBMPSGNetworkAdapterOfflineEvent ComponentID	1.3.6.1.4.1.2.6.159.1.1.0.27.7	Uint16	The physical PCI slot number or the onboard port number of the NIC.	

iBMPSGNetworkAdapterOnlineEvent

This event occurs when the state of a system NIC is online. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 28, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 52. iBMPSGNetworkAdapterOnlineEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGNetworkAdapterOnlineEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.28		SNMP v1 standard OID defined in enterprise 'director'	Yes
iBMPSGNetworkAdapterOnlineEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.28.1	String	Internal ID for this event type	

Table 52. iBMPSGNetworkAdapterOnlineEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGNetworkAdapterOnlineEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.28.2	String	Standard CIM ObjectPath value for the monitored NIC instance	
iBMPSGNetworkAdapterOnlineEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.28.3	String	Standard CIM ObjectPath value for the monitored NIC instance	
iBMPSGNetworkAdapterOnlineEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.28.4	Uint16	0 = Normal: The NIC referenced in the target object path is online.	
iBMPSGNetworkAdapterOnlineEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.28.5	String	Normal = “NIC in Port/PCI Slot %d is Online”	
iBMPSGNetworkAdapterOnlineEventTime Stamp	1.3.6.1.4.1.2.6.159.1.1.0.28.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000 -240.	
iBMPSGNetworkAdapterOnlineEvent ComponentID	1.3.6.1.4.1.2.6.159.1.1.0.28.7	Uint16	The physical PCI slot number or the onboard port number of the NIC.	

iBMPSGSPPowerSupplyEvent

This event occurs when the ASM processor detects that the state of the system power supply has changed

with respect to availability. This event is sent from servers that do not have a power backplane and do not support a recovery severity or alert type. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 29, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 53. iBMPSGSPPowerSupplyEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGSPPowerSupplyEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.29		SNMP v1 standard OID defined in enterprise 'director'	Yes
iBMPSGSPPowerSupplyEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.29.1	String	Internal ID for this event type	
iBMPSGSPPowerSupplyEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.29.2	String	SP_POWERSUPPLY	
iBMPSGSPPowerSupplyEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.29.3	String	SP_POWERSUPPLY	
iBMPSGSPPowerSupplyEventSeverity	1.3.6.1.4.1.2.6.159.1.1.0.29.4	Uint16	2 = Critical: A power supply in a system has failed and there has been a possible loss of redundancy.	
iBMPSGSPPowerSupplyEventDescription	1.3.6.1.4.1.2.6.159.1.1.0.29.5	String	Critical = "PowerSupply device identified as PowerSupply %d has failed. This event must be cleared manually"	

Table 53. iBMPSGSPPowerSupplyEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGSPPowerSupplyEventTimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.29.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGDASDBackplaneEvent

This event occurs when the Remote Supervisor Adapter detects that the state of the system hard disk drive has changed with respect to availability. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 30, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 54. iBMDASDBackplaneEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGDASDBackplaneEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.30		SNMP v1 standard OID defined in enterprise 'director'	Yes
iBMPSGDASDBackplaneEvent Identifier	1.3.6.1.4.1.2.6.159.1.1.0.30.1	String	Internal ID for this event type	
iBMPSGDASDBackplaneEvent SourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.30.2	String	CIM device ID value for the monitored physical hard disk drive instance	
iBMPSGDASDBackplaneEvent TargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.30.3	String	CIM device ID value for the monitored physical hard disk drive instance	

Table 54. iBMDASDBackplaneEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGDASDBackplaneEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.30.4	Uint16	2 = Critical: A hard drive failure has occurred.	
iBMPSGDASDBackplaneEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.30.5	String	Critical = “Drive %d has reported a fault. This event must be cleared manually.”	
iBMPSGDASDBackplaneEvent TimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.30.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGGenericFanEvent

This event occurs when the Remote Supervisor Adapter or ASM processor detects that the state of a system fan has changed with respect to manufacturer-defined RPM thresholds, but the precise fan instance cannot be determined. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 31, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 55. iBMPSGGenericFanEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGGenericFanEvent OID	1.3.6.1.4.1.2.6.159.1.1.0.31		SNMP v1 standard OID defined in enterprise ’director’	Yes
iBMPSGGenericFanEventIdentifier	1.3.6.1.4.1.2.6.159.1.1.0.31.1	String	Internal ID for this event type	
iBMPSGGenericFanEventSource ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.31.2	String	text string: Generic Fan	

Table 55. iBMPSGGenericFanEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGGenericFanEventTarget ObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.31.3	String	text string: Generic Fan	
iBMPSGGenericFanEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.31.4	Uint16	2=Critical: The fan has stopped.	
iBMPSGGenericFanEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.31.5	String	Critical = “A fan has failed. This event must be cleared manually.”	
iBMPSGGenericFanEvent TimeStamp	1.3.6.1.4.1.2.6.159.1.1.0.31.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

iBMPSGGenericVoltageEvent

This event occurs when the Remote Supervisor Adapter or the ASM processor detects that the state of a system voltage sensor has changed with respect to a manufacturer-defined threshold, but the precise voltage sensor cannot be determined. The MIB file for this event is umsevent.mib. The access is read-write and the status is mandatory. The TRAP-TYPE = 32, the enterprise is director, the enterprise OID=1.3.6.1.4.1.2.6.159.

Table 56. iBMGenericVoltageEvent

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGGenericVoltageEventOID	1.3.6.1.4.1.2.6.159.1.1.0.32		SNMP v1 standard OID defined in enterprise ’director’	Yes
iBMPSGGenericVoltageEvent Identifier	1.3.6.1.4.1.2.6.159.1.1.0.32.1	String	Internal ID for this event type	

Table 56. iBMGenericVoltageEvent (continued)

Event attribute	Value	Syntax	Description	New in IBM Director 4.1
iBMPSGGenericVoltageEvent SourceObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.32.2	String	text string: Generic Voltage	
iBMPSGGenericVoltageEvent TargetObjectPath	1.3.6.1.4.1.2.6.159.1.1.0.32.3	String	text string: Generic Voltage	
iBMPSGGenericVoltageEvent Severity	1.3.6.1.4.1.2.6.159.1.1.0.32.4	Uint16	2 = Critical: The voltage has exceeded a manufacturer-defined critical threshold.	
iBMPSGGenericVoltageEvent Description	1.3.6.1.4.1.2.6.159.1.1.0.32.5	String	Critical = “System voltage is out of specification. Please check the system management processor log for more information. This event must be cleared manually.”	
iBMPSGGenericVoltageEventTime Stamp	1.3.6.1.4.1.2.6.159.1.1.0.32.6	Datetime	The date and time when the state change occurred for the component. The GMT-standard timestamp is used. For example: 20030416155614.000000-240.	

ibmServeRAIDNoControllers

This event occurs when a ServeRAID controller is not detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 201, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 57. iBMPSGServeRAIDNoControllers

TRAP-TYPE Description	Event attribute	Value
"Informational: No controllers were found in this system."		
	ibmServeRAIDNoControllers OID	1.3.6.1.4.1.2.6.167.2.201
	ibmServeRAIDNoControllersAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDControllerFail

This event occurs when a ServeRAID controller has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 202, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 58. iBMServeRAIDControllerFail

TRAP-TYPE Description	Event attribute	Value
"Error: Commands not responding on Controller %d"		
	ibmServeRAIDControllerFail OID	1.3.6.1.4.1.2.6.167.2.202
	iBMServeRAIDControllerFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDControllerFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDDeadBattery

This event is sent when a ServeRAID battery has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 203, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 59. iBMServeRAIDDeadBattery

Description	Event attribute	Value
"Error: The battery-backup cache device on Controller %d needs a new battery"		

Table 59. iBMServeRAIDDeadBattery (continued)

Description	Event attribute	Value
	iBMServeRAIDDeadBattery OID	1.3.6.1.4.1.2.6.167.2.202
	iBMServeRAIDDeadBatteryServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDDeadBatteryAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMPSGServeRAIDDeadBatteryCache

This event occurs when the ServeRAID battery-backup cache has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 204, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 60. iBMPSGServeRAIDDeadBatteryCache

Description	Event attribute	Value
“Error: The battery-backup cache device on Controller %d is defective %d.”		
	iBMServeRAIDDeadBatteryCache OID	1.3.6.1.4.1.2.6.167.2.204
	iBMServeRAIDDeadBatteryCacheServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDDeadBatteryCacheAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDDeadBatteryCacheErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDPollingFail

This event occurs when the ServeRAID polling has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 205, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 61. iBMServeRAIDPollingFail

Description	Event attribute	Value
“Error: Background polling commands not responding on Controller %d %d.”		

Table 61. iBMServeRAIDPollingFail (continued)

Description	Event attribute	Value
	iBMServeRAIDPollingFail OID	1.3.6.1.4.1.2.6.167.2.205
	iBMServeRAIDPollingFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDPollingFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDPollingFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDConfigFail

This event occurs when a ServeRAID configuration has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 206, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 62. iBMServeRAIDConfigFail

Description	Event attribute	Value
“Error: Cannot read controller configuration.”		
	iBMServeRAIDConfigFail OID	1.3.6.1.4.1.2.6.167.2.201
	iBMServeRAIDConfigFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8

iBMServeRAIDControllerAdded

This event occurs when a ServeRAID controller is added. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 207, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 63. iBMServeRAIDControllerAdded

Description	Event attribute	Value
“Informational: Controller %d has been added to the system.”		
	iBMServeRAIDControllerAdded OID	1.3.6.1.4.1.2.6.167.2.207
	iBMServeRAIDControllerAddedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDControllerAddedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDControllerReplaced

This event occurs when the ServeRAID controller is replaced. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 208, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 64. iBMServeRAIDControllerReplaced

Description	Event attribute	Value
"Informational: Controller %d has been replaced in the system."		
	iBMServeRAIDControllerReplaced OID	1.3.6.1.4.1.2.6.167.2.208
	iBMServeRAIDControllerReplacedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDControllerReplacedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMPSGServeRAIDControllerFailover

This event occurs when a ServeRAID controller has failed over. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 209, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 65. iBMServeRAIDControllerFailover

Description	Event attribute	Value
"Informational: Controller %d failover detected. Passive controller is now active."		
	iBMServeRAIDControllerMismatchedVersions OID	1.3.6.1.4.1.2.6.167.2.210
	iBMServeRAIDControllerMismatchedVersionsServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDControllerMismatchedVersionsAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDControllerBatteryOvertemp

This event occurs when a ServeRAID controller battery has exceeded its temperature threshold. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 211, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 66. iBMServeRAIDControllerBatteryOvertemp

Description	Event attribute	Value
"Warning: Controller %d battery has exceeded normal operating temperature."		
	iBMServeRAIDControllerBatteryOvertemp OID	1.3.6.1.4.1.2.6.167.2.211
	iBMServeRAIDControllerBatteryOvertempServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDControllerBatteryOvertempAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDLogicalDriveCritical

This event occurs when a ServeRAID logical drive is in a critical state. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 301, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 67. iBMServeRAIDLogicalDriveCritical

Description	Event attribute	Value
"Warning: Logical Drive %d is Critical on Controller %d."		
	iBMServeRAIDLogicalDriveCritical OID	1.3.6.1.4.1.2.6.167.2.301
	iBMServeRAIDLogicalDriveCriticalServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDLogicalDriveCriticalLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDLogicalDriveCriticalAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDLogicalDriveBlocked

This event occurs when the ServeRAID logical drive is in a blocked state. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 302, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 68. iBMServeRAIDLogicalDriveBlocked

Description	Event attribute	Value
"Error: Logical Drive %d is Blocked on Controller %d."		
	iBMServeRAIDLogicalDriveBlocked OID	1.3.6.1.4.1.2.6.167.2.302
	iBMServeRAIDLogicalDriveBlockedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDLogicalDriveBlockedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDLogicalDriveBlockedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMPSGServeRAIDLogicalDriveOffLine

This event occurs when a ServeRAID logical drive is in an offline state. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 303, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 69. iBMServeRAIDLogicalDriveOffLine

Description	Event attribute	Value
"Error: Logical Drive %d is Offline on Controller %d."		
	iBMServeRAIDLogicalDriveOffLine OID	1.3.6.1.4.1.2.6.167.2.303
	iBMServeRAIDLogicalDriveOffLineServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDLogicalDriveOffLineLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDLogicalDriveOffLineAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDRebuildDetected

This event occurs when a ServeRAID rebuild operation is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 304, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 70. iBMServeRAIDRebuildDetected

Description	Event attribute	Value
"Informational: Rebuilding Logical Drive %d on Controller %d."		
	iBMServeRAIDRebuildDetected OID	1.3.6.1.4.1.2.6.167.2.301
	iBMServeRAIDRebuildDetectedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDRebuildDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDRebuildDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDRebuildComplete

This event occurs when a ServeRAID rebuild operation is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 305, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 71. iBMServeRAIDRebuildComplete

Description	Event attribute	Value
"Informational: Rebuild complete on Logical Drive %d of Controller %d."		
	iBMServeRAIDRebuildComplete OID	1.3.6.1.4.1.2.6.167.2.305
	iBMServeRAIDRebuildCompleteServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDRebuildCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDRebuildCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDRebuildFail

This event occurs when a ServeRAID rebuild operation has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 306, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 72. iBMServeRAIDRebuildComplete

Description	Event attribute	Value
"Error: Rebuild failed on Logical Drive %d of Controller %d %d."		
	iBMServeRAIDRebuildFail OID	1.3.6.1.4.1.2.6.167.2.306
	iBMServeRAIDRebuildFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDRebuildFailLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDRebuildFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDRebuildFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDsyncDetected

This event occurs when a ServeRAID synchronization is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 307, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 73. iBMServeRAIDsyncDetected

Description	Event attribute	Value
"Informational: synchronizing Logical Drive %d on Controller %d."		
	iBMServeRAIDsyncDetected OID	1.3.6.1.4.1.2.6.167.2.307
	iBMServeRAIDsyncDetectedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDsyncDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDsyncDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDsyncComplete

This event occurs when a ServeRAID synchronization is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 308, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 74. iBMServeRAIDsyncComplete

Description	Event attribute	Value
“Informational: synchronization complete on Logical Drive %d of Controller %d.”		
	iBMServeRAIDsyncComplete OID	1.3.6.1.4.1.2.6.167.2.308
	iBMServeRAIDsyncCompleteServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDsyncCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDsyncCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDsyncFail

This event occurs when a ServeRAID synchronization has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 309, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 75. iBMServeRAIDsyncFail

Description	Event attribute	Value
“Error: synchronization failed on Logical Drive %d of Controller %d %d.”		
	iBMServeRAIDsyncFail OID	1.3.6.1.4.1.2.6.167.2.309
	iBMServeRAIDsyncFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDsyncFailLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDsyncFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDsyncFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDMigrationDetected

This event occurs when a ServeRAID logical-drive migration is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 310, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 76. iBMServeRAIDMigrationDetected

Description	Event attribute	Value
"Informational: Migrating Logical Drive %d on Controller %d."		
	iBMServeRAIDMigrationDetected OID	1.3.6.1.4.1.2.6.167.2.310
	iBMServeRAIDMigrationDetectedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDMigrationDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDMigrationDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDMigrationComplete

This event occurs when a ServeRAID logical-drive migration is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 311, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 77. iBMServeRAIDMigrationComplete

Description	Event attribute	Value
"Informational: Migration complete on Logical Drive %d of Controller %d."		
	iBMServeRAIDMigrationComplete OID	1.3.6.1.4.1.2.6.167.2.311
	iBMServeRAIDMigrationCompleteServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDMigrationCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDMigrationCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDMigrationFail

This event occurs when a ServeRAID logical-drive migration has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 312, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 78. iBMServeRAIDMigrationFail

Description	Event attribute	Value
"Error: Migration failed on Logical Drive %d of Controller %d %d."		
	iBMServeRAIDMigrationFail OID	1.3.6.1.4.1.2.6.167.2.312
	iBMServeRAIDMigrationFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDMigrationFailLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDMigrationFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDMigrationFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDCompressionDetected

This event occurs when a ServeRAID logical-drive compression is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 313, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 79. iBMServeRAIDCompressionDetected

Description	Event attribute	Value
"Informational: Compressing Logical Drive %d on Controller %d."		
	iBMServeRAIDCompressionDetected OID	1.3.6.1.4.1.2.6.167.2.313
	iBMServeRAIDCompressionDetectedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDCompressionDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDCompressionDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDCompressionComplete

This event occurs when a ServeRAID logical-drive compression is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 314, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 80. iBMServeRAIDCompressionComplete

Description	Event attribute	Value
"Informational: Compressing Logical Drive %d of Controller %d."		
	iBMServeRAIDCompressionComplete OID	1.3.6.1.4.1.2.6.167.2.314
	iBMServeRAIDCompressionCompleteServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDCompressionCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDCompressionCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDCompressionFail

This event occurs when a ServeRAID logical-drive compression has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 315, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 81. iBMServeRAIDCompressionFail

Description	Event attribute	Value
"Error: Compression failed on Logical Drive %d of Controller %d %d."		
	iBMServeRAIDCompressionFail OID	1.3.6.1.4.1.2.6.167.2.315
	iBMServeRAIDCompressionFail.ServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDCompressionFail.LogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDCompressionFail.AdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDCompressionFail.ErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDDecompressionDetected

This event occurs when a ServeRAID logical drive decompression is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 316, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 82. iBMServeRAIDCompressionDetected

Description	Event attribute	Value
“Informational: Decompressing Logical Drive %d on Controller %d.”		
	iBMServeRAIDDecompressionDetected OID	1.3.6.1.4.1.2.6.167.2.316
	iBMServeRAIDDecompressionDetectedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDDecompressionDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDDecompressionDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDDecompressionComplete

This event occurs when a ServeRAID logical drive decompression is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 317, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 83. iBMServeRAIDCompressionComplete

Description	Event attribute	Value
″Informational: Decompressing Logical Drive %d of Controller %d.”		
	iBMServeRAIDDecompressionComplete OID	1.3.6.1.4.1.2.6.167.2.312
	iBMServeRAIDDecompressionCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDDecompressionCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDDecompressionFail

This event occurs when a ServeRAID logical drive decompression has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 318, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 84. iBMServeRAIDCompressionFail

Description	Event attribute	Value
"Error: Decompression failed on Logical Drive %d on Controller %d."		
	iBMServeRAIDDecompressionFail OID	1.3.6.1.4.1.2.6.167.2.318
	iBMServeRAIDDecompressionFailLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDDecompressionFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDDecompressionFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDFlashCopyDetected

This event occurs when a ServeRAID FlashCopy® operation is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 319, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 85. iBMServeRAIDFlashCopyDetected

Description	Event attribute	Value
"Informational: Flashcopying Logical Drive %d on Controller %d."		
	iBMServeRAIDFlashCopyDetected OID	1.3.6.1.4.1.2.6.167.2.319
	iBMServeRAIDFlashCopyDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDFlashCopyDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDFlashCopyComplete

This event occurs when a ServeRAID FlashCopy operation is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 320, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 86. iBMServeRAIDFlashCopyComplete

Description	Event attribute	Value
"Informational: Flashcopy complete on Logical Drive %d of Controller %d."		
	iBMServeRAIDFlashCopyComplete OID	1.3.6.1.4.1.2.6.167.2.320
	iBMServeRAIDFlashCopyCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDFlashCopyCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDFlashCopyFail

This event occurs when a ServeRAID FlashCopy operation has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 321, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 87. iBMServeRAIDFlashCopyFail

Description	Event attribute	Value
"Error: FlashCopy failed on Logical Drive %d of Controller %d %d."		
	iBMServeRAIDFlashCopyFail OID	1.3.6.1.4.1.2.6.167.2.321
	iBMServeRAIDFlashCopyFailLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDFlashCopyFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDFlashCopyFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDArrayRebuildDetected

This event occurs when a ServeRAID array rebuild operation is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 322, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 88. iBMServeRAIDArrayRebuildDetected

Description	Event attribute	Value
"Informational: Rebuilding Array %d on Controller %d."		
	iBMServeRAIDArrayRebuildDetected OID	1.3.6.1.4.1.2.6.167.2.322
	iBMServeRAIDArrayRebuildDetectedArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArrayRebuildDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDArrayRebuildComplete

This event occurs when a ServeRAID array rebuild operation is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 323, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 89. iBMServeRAIDArrayRebuildComplete

Description	Event attribute	Value
"Error: Rebuild failed on Array of %d of Controller %d %d."		
	iBMServeRAIDArrayRebuildComplete OID	1.3.6.1.4.1.2.6.167.2.323
	iBMServeRAIDArrayRebuildCompleteArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArrayRebuildCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDArrayRebuildFail

This event occurs when a ServeRAID array rebuild operation has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 324, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 90. iBMServeRAIDArrayRebuildFail

Description	Event attribute	Value
"Error:Rebuild failed on Array %d of Controller %d %d."		

Table 90. iBMServeRAIDArrayRebuildFail (continued)

Description	Event attribute	Value
	iBMServeRAIDArrayRebuildFail OID	1.3.6.1.4.1.2.6.167.2.324
	iBMServeRAIDArrayRebuildFailArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArrayRebuildFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDArrayRebuildFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDArraysyncDetected

This event occurs when a ServeRAID array synchronization is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 325, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 91. iBMServeRAIDArraysyncDetected

Description	Event attribute	Value
“Informational: synchronizing Array %d on Controller %d.”		
	iBMServeRAIDArraysyncDetected OID	1.3.6.1.4.1.2.6.167.2.325
	iBMServeRAIDArraysyncDetectedArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArraysyncDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDArraysyncComplete

This event occurs when a ServeRAID array synchronization is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 326, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 92. iBMServeRAIDArraysyncComplete

Description	Event attribute	Value
“Informational: synchronization complete on Array %d of Controller %d.”		

Table 92. iBMServeRAIDArraysyncComplete (continued)

Description	Event attribute	Value
	iBMServeRAIDArraysyncComplete OID	1.3.6.1.4.1.2.6.167.2.326
	iBMServeRAIDArraysyncCompleteArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArraysyncCompletdAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDArraysyncFail

This event occurs when a ServeRAID array synchronization has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 327, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 93. iBMServeRAIDArraysyncFail

Description	Event attribute	Value
"Error: synchronization failed on Array %d of Controller %d %d"		
	iBMServeRAIDArraysyncFail OID	1.3.6.1.4.1.2.6.167.2.327
	iBMServeRAIDArraysyncFailArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArraysyncFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDArraysyncFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDArrayFlashCopyDetected

This event occurs when a ServeRAID array FlashCopy operation is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 328, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 94. iBMServeRAIDArrayFlashCopyDetected

Description	Event attribute	Value
"Informational: Flashcopying Array %d on Controller %d."		

Table 94. iBMServeRAIDArrayFlashCopyDetected (continued)

Description	Event attribute	Value
	iBMServeRAIDArrayFlashCopyDetected OID	1.3.6.1.4.1.2.6.167.2.328
	iBMServeRAIDArrayFlashCopyDetectedArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArrayFlashCopyDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDArrayFlashCopyComplete

This event occurs when the ServeRAID array FlashCopy operation is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 329, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 95. iBMServeRAIDArrayFlashCopyComplete

Description	Event attribute	Value
“Informational: FlashCopy complete on Array %d of Controller %d.”		
	iBMServeRAIDArrayFlashCopyComplete OID	1.3.6.1.4.1.2.6.167.2.329
	iBMServeRAIDArrayFlashCopyCompleteArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArrayFlashCopyCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDArrayFlashCopyFail

This event occurs when a ServeRAID array FlashCopy operation has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 330, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 96. iBMServeRAIDArrayFlashCopyFail

Description	Event attribute	Value
“Error:Flashcopy failed on Array %d of Controller %d %d.”		

Table 96. iBMServeRAIDArrayFlashCopyFail (continued)

Description	Event attribute	Value
	iBMServeRAIDArrayFlashCopyFail OID	1.3.6.1.4.1.2.6.167.2.330
	iBMServeRAIDArrayFlashCopyFailArrayID	1.3.6.1.4.1.2.6.167.2.1.3.9
	iBMServeRAIDArrayFlashCopyFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDArrayFlashCopyFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDLogicalDriveUnblocked

This event occurs when a ServeRAID logical drive is unblocked. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 331, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 97. iBMServeRAIDLogicalDriveUnblocked

Description	Event attribute	Value
"Informational: Logical Drive %d is unblocked on Controller %d."		
	iBMServeRAIDLogicalDriveUnblocked	1.3.6.1.4.1.2.6.167.2.331
	iBMServeRAIDLogicalDriveUnblockedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDLogicalDriveUnblockedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDCompactionDetected

This event occurs when a ServeRAID compaction operation is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 332, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 98. iBMServeRAIDCompactionDetected

Description	Event attribute	Value
"Informational: Compacting Logical Drive %d on Controller %d."		

Table 98. iBMServeRAIDCompactionDetected (continued)

Description	Event attribute	Value
	iBMServeRAIDCompactionDetected	1.3.6.1.4.1.2.6.167.2.332
	iBMServeRAIDCompactionDetectedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDCompactionDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDCompactionDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDCompactionComplete

This event occurs when a ServeRAID compaction operation is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 333, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 99. iBMServeRAIDCompactionComplete

Description	Event attribute	Value
“Informational: Compaction complete on Logical Drive %d of Controller %d.”		
	iBMServeRAIDCompactionComplete	1.3.6.1.4.1.2.6.167.2.333
	iBMServeRAIDCompactionCompleteServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDCompactionCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDCompactionCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDCompactionFail

This event occurs when a ServeRAID compaction operation has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 334, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 100. iBMServeRAIDCompactionFail

Description	Event attribute	Value
"Error: Compaction failed on Logical Drive %d of Controller %d %d."		
	iBMServeRAIDCompactionFail	1.3.6.1.4.1.2.6.167.2.334
	iBMServeRAIDCompactionFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDCompactionFailLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDCompactionFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDCompactionFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDExpansionDetected

This event occurs when a ServeRAID operation expansion is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 335, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 101. iBMServeRAIDExpansionDetected

Description	Event attribute	Value
"Informational: Expanding Logical Drive %d on Controller %d."		
	iBMServeRAIDExpansionDetected	1.3.6.1.4.1.2.6.167.2.335
	iBMServeRAIDExpansionDetectedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDExpansionDetectedLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDExpansionDetectedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDExpansionComplete

This event occurs when a ServeRAID operation expansion is completed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 336, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 102. iBMServeRAIDExpansionComplete

Description	Event attribute	Value
“Informational: Expansion complete on Logical Drive %d of Controller %d.”		
	iBMServeRAIDExpansionComplete	1.3.6.1.4.1.2.6.167.2.336
	iBMServeRAIDExpansionCompleteServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDExpansionCompleteLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDExpansionCompleteAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDExpansionFail

This event occurs when a ServeRAID operation expansion has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 337, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 103. iBMServeRAIDExpansionFail

Description	Event attribute	Value
“Error: Expansion failed on Logical Drive %d of Controller %d %d.”		
	iBMServeRAIDExpansionFail	1.3.6.1.4.1.2.6.167.2.337
	iBMServeRAIDExpansionFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDExpansionFailLogicalDriveID	1.3.6.1.4.1.2.6.167.2.1.3.2
	iBMServeRAIDExpansionFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDExpansionFailErrorCode	1.3.6.1.4.1.2.6.167.2.1.3.7

iBMServeRAIDLogicalDriveCriticalPeriodic

This event occurs when a ServeRAID logical drive is in a critical state. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 338, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 104. iBMServeRAIDLogicalDriveCriticalPeriodic

Description	Event attribute	Value
"Warning: Periodic scan found 1 or more critical logical drives on Controller %d."		
	iBMServeRAIDLogicalDriveCriticalPeriodic	1.3.6.1.4.1.2.6.167.2.338
	iBMServeRAIDLogicalDriveCriticalPeriodicServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDLogicalDriveCriticalPeriodicAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1

iBMServeRAIDDefunctDrive

This event occurs when a ServeRAID physical drive in a defunct state is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 401, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 105. iBMServeRAIDDefunctDrive

Description	Event attribute	Value
"Error: Defunct drive on Controller %d, Channel %d, SCSI ID %d."		
	iBMServeRAIDDefunctDrive	1.3.6.1.4.1.2.6.167.2.401
	iBMServeRAIDDefunctDriveServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDDefunctDriveAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDDefunctDriveChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3
	iBMServeRAIDDefunctDriveSCSIID	1.3.6.1.4.1.2.6.167.2.1.3.4

iBMServeRAIDPFADrive

This event occurs when a ServeRAID physical drive with a PFA is detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 402, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 106. iBMServeRAIDPFADrive

Description	Event attribute	Value
"Warning: PFA drive on Controller %d, Channel %d, SCSI ID %d."		
	iBMServeRAIDPFADrive	1.3.6.1.4.1.2.6.167.2.402
	iBMServeRAIDPFADriveServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDPFADriveAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDPFADriveChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3
	iBMServeRAIDPFADriveSCSIID	1.3.6.1.4.1.2.6.167.2.1.3.4

iBMServeRAIDDefunctReplaced

This event occurs when a ServeRAID defunct physical drive is replaced. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 403, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 107. iBMServeRAIDDefunctReplaced

	Event attribute	Value
"Informational: A drive is set to Hot-Spare on Controller %d, Channel %d, SCSI ID %d."		
	iBMServeRAIDDefunctReplaced	1.3.6.1.4.1.2.6.167.2.403
	iBMServeRAIDDefunctReplacedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDDefunctReplacedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDDefunctReplacedChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3
	iBMServeRAIDDefunctReplacedSCSIID	1.3.6.1.4.1.2.6.167.2.1.3.4

iBMServeRAIDDefunctDriveFRU

This event occurs when the field-replaceable unit (FRU) number is identified for a ServeRAID defunct

physical drive. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 404, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 108. iBMServeRAIDDefunctDriveFRU

Description	Event attribute	Value
"Error: Defunct drive (FRU Part # %d} on controller %d, channel %d, SCSI ID %d."		
	iBMServeRAIDDefunctDriveFRU	1.3.6.1.4.1.2.6.167.2.404
	iBMServeRAIDDefunctDriveFRUServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDDefunctDriveFRUFRU	1.3.6.1.4.1.2.6.167.2.1.3.10
	iBMServeRAIDDefunctDriveFRUAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDDefunctDriveFRUChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3
	iBMServeRAIDDefunctDriveFRUSCSIID	1.3.6.1.4.1.2.6.167.2.1.3.4

iBMServeRAIDPFADriveFRU

This event occurs when the FRU number is identified for a ServeRAID physical drive on which a PFA has been detected. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 405, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 109. iBMServeRAIDPFADriveFRU

Descriptions	Event attribute	Value
"Warning: PFA drive (FRU Part # %d) on Controller %d, Channel %d, SCSI ID %d."		

Table 109. iBMServeRAIDPFADriveFRU (continued)

Descriptions	Event attribute	Value
	iBMServeRAIDPFADriveFRU	1.3.6.1.4.1.2.6.167.2.405
	iBMServeRAIDPFADriveFRUServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDPFADriveFRUFRU	1.3.6.1.4.1.2.6.167.2.1.3.10
	iBMServeRAIDPFADriveFRUAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDPFADriveFRUChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3
	iBMServeRAIDPFADriveFRUSCSIID	1.3.6.1.4.1.2.6.167.2.1.3.4

iBMServeRAIDUnsupportedDrive

This event occurs when there is an unsupported physical drive is detected in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 406, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 110. iBMServeRAIDUnsupportedDrive

Description	Event attribute	Value
“Warning: Unsupported physical drive found on Controller %d, Channel %d, SCSI ID %d.”		
	iBMServeRAIDUnsupportedDrive	1.3.6.1.4.1.2.6.167.2.406
	iBMServeRAIDUnsupportedDriveServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDUnsupportedDriveAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDUnsupportedDriveChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3
	iBMServeRAIDUnsupportedDriveSCSIID	1.3.6.1.4.1.2.6.167.2.1.3.4

iBMServeRAIDEnclosureOK

This event occurs when an enclosure is functioning properly in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 501, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 111. iBMServeRAIDEnclosureOK

Description	Event attribute	Value
"Informational: Enclosure device responding on Controller %d, Channel %d."		
	iBMServeRAIDEnclosureOK	1.3.6.1.4.1.2.6.167.2.501
	iBMServeRAIDEnclosureOKServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDEnclosureOKAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDEnclosureOKChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDEnclosureFail

This event occurs when an enclosure has failed in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 502, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 112. iBMServeRAIDEnclosureFail

Description	Event attribute	Value
"Error; Enclosure device not responding on Controller %d, Channel %d."		
	iBMServeRAIDEnclosureFail	1.3.6.1.4.1.2.6.167.2.502
	iBMServeRAIDEnclosureFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDEnclosureFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDEnclosureFailChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDEnclosureFanOk

This event occurs when an enclosure fan is functioning properly in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 503, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 113. iBMServeRAIDEnclosureFanOk

Description	Extended attribute	Value
"Informational: Enclosure fan %d on Controller %d, Channel %d is now operational."		
	iBMServeRAIDEnclosureFanOk	1.3.6.1.4.1.2.6.167.2.503
	iBMServeRAIDEnclosureFanOkServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDEnclosureFanOkFanID	1.3.6.1.4.1.2.6.167.2.1.3.5
	iBMServeRAIDEnclosureFanOkAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDEnclosureFanOkChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDFanFail

This event occurs when the ServeRAID enclosure fan has failed. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 504, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 114. iBMServeRAIDFanFail

Description	Extended attribute	Value
"Error: Enclosure fan %d on Controller %d, Channel %d is malfunctioning."		
	iBMServeRAIDFanFail	1.3.6.1.4.1.2.6.167.2.504
	iBMServeRAIDFanFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDFanFailFanID	1.3.6.1.4.1.2.6.167.2.1.3.5
	iBMServeRAIDFanFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDFanFailChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDFanInstalled

This event occurs when an enclosure fan is installed in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 505, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 115. iBMServeRAIDFanInstalled

Description	Event attribute	Value
"Informational: Enclosure fan %d on Controller %d, Channel %d has been installed."		
	iBMServeRAIDFanInstalled	1.3.6.1.4.1.2.6.167.2.505
	iBMServeRAIDFanInstalledServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDFanInstalledFanID	1.3.6.1.4.1.2.6.167.2.1.3.5
	iBMServeRAIDFanInstalledAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDFanInstalledChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDFanRemoved

This event occurs when an enclosure fan is removed from a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 506, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 116. iBMServeRAIDFanRemoved

Enclosure	Event attribute	Value
"Warning: Enclosure fan %d on Controller %d, Channel %d has been removed."		

Table 116. iBMServeRAIDFanRemoved (continued)

Enclosure	Event attribute	Value
	iBMServeRAIDFanRemoved	1.3.6.1.4.1.2.6.167.2.506
	iBMServeRAIDFanRemovedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDFanRemovedFanID	1.3.6.1.4.1.2.6.167.2.1.3.5
	iBMServeRAIDFanRemovedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDFanRemovedChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDTempOk

This event occurs when an enclosure temperature is within a normal range in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 507, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 117. iBMServeRAIDTempOk

Description	Event attribute	Value
"Error: Enclosure temperature is in normal range on Controller %d, Channel %d."		
	iBMServeRAIDTempOk	1.3.6.1.4.1.2.6.167.2.507
	iBMServeRAIDTempOkServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDTempOkAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDTempOkChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDTempFail

This event occurs when an enclosure temperature exceeds a normal range in the ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 508, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 118. iBMServeRAIDTempFail

Description	Event attribute	Value
"Error: Enclosure temperature is out of normal range on Controller %d, Channel %d."		
	iBMServeRAIDTempFail	1.3.6.1.4.1.2.6.167.2.508
	iBMServeRAIDTempFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDTempFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDTempFailChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDPowerSupplyOk

This event occurs when an enclosure power supply is functioning properly in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 509, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 119. iBMServeRAIDPowerSupplyOk

Description	Event attribute	Value
"Informational: Enclosure power supply %d on Controller, Channel %d is operational."		
	iBMServeRAIDPowerSupplyOk	1.3.6.1.4.1.2.6.167.2.509
	iBMServeRAIDPowerSupplyOkServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDPowerSupplyOkPowerSupplyID	1.3.6.1.4.1.2.6.167.2.1.3.6
	iBMServeRAIDPowerSupplyOkAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDPowerSupplyOkChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDPowerSupplyFail

This event occurs when an enclosure power supply has failed in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 510, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 120. iBMServeRAIDPowerSupplyFail

Description	Event attribute	Value
"Error: Enclosure power supply %d on Controller %d, Channel %d is malfunctioning."		
	iBMServeRAIDPowerSupplyFail	1.3.6.1.4.1.2.6.167.2.510
	iBMServeRAIDPowerSupplyFailServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDPowerSupplyFailPowerSupplyID	1.3.6.1.4.1.2.6.167.2.1.3.6
	iBMServeRAIDPowerSupplyFailAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDPowerSupplyFailChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDPowerSupplyInstalled

This event occurs when an enclosure power supply is installed in a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 511, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 121. iBMServeRAIDPowerSupplyInstalled

Description	Event attribute	Value
"Informational: Enclosure power supply %d on Controller %d, Channel %d has been installed."		
	iBMServeRAIDPowerSupplyInstalled	1.3.6.1.4.1.2.6.167.2.511
	iBMServeRAIDPowerSupplyInstalledServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDPowerSupplyInstalledPowerSupplyID	1.3.6.1.4.1.2.6.167.2.1.3.6
	iBMServeRAIDPowerSupplyInstalledAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDPowerSupplyInstalledChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDPowerSupplyRemoved

This event occurs when enclosure power supply is removed from a ServeRAID configuration. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 512, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 122. iBMServeRAIDPowerSupplyRemoved

Description	Event attribute	Value
"Warning: Enclosure power supply %d on Controller %d, Channel %d has been removed."		
	iBMServeRAIDPowerSupplyRemoved	1.3.6.1.4.1.2.6.167.2.512
	iBMServeRAIDPowerSupplyRemovedServerName	1.3.6.1.4.1.2.6.167.2.1.3.8
	iBMServeRAIDPowerSupplyRemovedPowerSupplyID	1.3.6.1.4.1.2.6.167.2.1.3.6
	iBMServeRAIDPowerSupplyRemovedAdapterID	1.3.6.1.4.1.2.6.167.2.1.3.1
	iBMServeRAIDPowerSupplyRemovedChannelID	1.3.6.1.4.1.2.6.167.2.1.3.3

iBMServeRAIDTestEvent

This event occurs when a ServeRAID test event occurs. The MIB file is ibmServeRAID.mib. The TRAP-TYPE = 601, the enterprise is ibmServeRaidMIB, the enterprise OID=1.3.6.1.4.1.2.6.167.

Table 123. iBMServeRAIDTestEvent

Description	Event attribute	Value
"Informational: This is a test trap."		
	iBMServeRAIDTestEvent	1.3.6.1.4.1.2.6.167.2.601
	iBMServeRAIDTestEventServerName	1.3.6.1.4.1.2.6.167.2.1.3.8

Appendix B. CIM events

The information in this appendix provides the CIM event class names, the level of severity, indicates the default consumers for each severity level, and the corresponding IBM Director event types.

Note: The four columns contain the following information:

- The “CIM event class name” column indicates the name of the CIM event class.
- The “Severity” column indicates the severity level supported by a specific event.
- The “Default consumers” column lists the preconfigured event sinks for the CIM events. These can be modified through IBM Director Agent using the Health Configuration service in the Web-based Access feature.
- The “IBM Director event type” column indicates how the CIM event is displayed in the “Director” consumer.

Table 124. CIM event log

CIM event class name	Severity	Default consumers	IBM Director event type
IBMPSG_ChassisEvent	Normal	System Health, Tivoli Enterprise Console®, Microsoft System Management Server (SMS), Director, SNMP	CIM.Director Agent Events.System Enclosure
	Critical	System Health, Graphical User Interface (GUI), Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_FanEvent	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Fan
	Warning	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	

Table 124. CIM event log (continued)

CIM event class name	Severity	Default consumers	IBM Director event type
IBMPSG_StorageEvent	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Disk Space Low
	Warning	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_TemperatureEvent	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Temperature
	Warning	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_Voltage Event	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Voltage
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_LANLeashEvent	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	CIM.Director Agent Events.LAN Leash
IBMPSG_SMARTEvent	Normal	System Health, Tivoli Enterprise Console, SMS, Director	CIM.Director Agent Events.SMART Drive
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_RedundantNetwork AdapterFailoverEvent	Warning	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	CIM.Director Agent Events.Redundant Network Adapter Failover

Table 124. CIM event log (continued)

CIM event class name	Severity	Default consumers	IBM Director event type
IBMPSG_RedundantNetwork AdapterSwitchoverEvent	Warning	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	CIM.Director Agent Events.Redundant Network Adapter Switchover
IBMPSG_RedundantNetwork AdapterSwitchbackEvent	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Redundant Network Adapter Switchback
IBMPSG_LeaseExpirationEvent	Warning	None by default	CIM.Director Agent Events.Lease Expiration
IBMPSG_WarrantyExpiration Event	Warning	None by default	CIM.Director Agent Events.Warranty Expiration
IBMPSG_ProcessorPFEvent	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Processor PFA
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_MemoryPFEvent	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Memory PFA
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_PFAEvent	Critical	Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	CIM.Director Agent Events.PFA
IBMPSG_PowerSupply Event	Normal	System Health, Tivoli Enterprise Console, SMS, Director, SNMP	CIM.Director Agent Events.Server Power Supply
	Critical	System Health, GUI, Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	
IBMPSG_ErrorLogEvent	Warning	Tivoli Enterprise Console, SMS, Windows event log, Director, SNMP	CIM.Director Agent Events.Error Log

Table 124. CIM event log (continued)

CIM event class name	Severity	Default consumers	IBM Director event type
IBMPSG_RemoteLoginEvent	Warning	None by default	CIM.Director Agent Events.Remote Login
IBMPSG_StorageRAIDHealth Event	Normal	System Health, Director, SNMP	CIM.Director Agent Events.ServeRAID Health
	Warning	System Health, Director, SNMP	
IBMPSG_Network Event	Critical	System Health, GUI, Director, Windows event log, Tivoli Enterprise Console, SMS, SNMP	CIM.Director Agent Events.Network Adapter
IBMPSG_NetworkAdapter FailedEvent	Warning	System Health, GUI, Director, Windows event log, Tivoli Enterprise Console, SMS, SNMP	CIM.Director Agent Events.Network Adapter.Failed
IBMPSG_NetworkAdapter OfflineEvent	Normal	System Health, Director, Tivoli Enterprise Console, SMS, SNMP	CIM.Director Agent Events.Network Adapter.Offline
IBMPSG_NetworkAdapter OnlineEvent	Critical	Windows event log, Director, SMS, Tivoli Enterprise Console, GUI, SNMP	CIM.Director Agent Events.Network Adapter.Online
IBMPSG_GenericFanEvent	Critical	Windows event log, Director, SMS, Tivoli Enterprise Console, GUI, SNMP	CIM.Director Agent Events.Fan
IBMPSG_GenericVoltageEvent	Critical	Windows event log, Director, SMS, Tivoli Enterprise Console, GUI, SNMP	CIM.Director Agent Events.Voltage
IBMPSG_DASDBackplane Event	Critical	Windows event log, Director, SMS, Tivoli Enterprise Console, SNMP	CIM.Director Agent Events.DASD Backplane
IBMPSG_StorageRAIDEvent	Normal	Tivoli Enterprise Console, SMS, SNMP	CIM.Director Agent Events.ServeRAID Health
	Warning	Director, Windows event log, Tivoli Enterprise Console, SMS, SNMP	
	Critical	Director, Windows event log, Tivoli Enterprise Console, SMS, SNMP	

Appendix C. IBM Director Agent events found in the Windows event log

You can use this Windows event log information to help you to find information for IBM Director Agent events only.

Note: The table columns contain the following information:

- The “Event ID” column indicates the numerical identifier for an event.
- The “Severity” column indicates the severity of an event.
- The “Descriptions” column is a description of an event.
- The “Source of the event” column indicates of the event was generated by IBM Director or by the operating system of the managed system.
- The “New in IBM Director 4.1” column identifies events that are new in the latest release.

Table 125. IBM Director Agent events

Event ID	Severity	Descriptions	Source of the event	New in IBM Director 4.1
1		Reserved		
2	Critical	“Temperature Sensor %d exceeded the manufacturer/user defined threshold of %d Celsius/Fahrenheit. The current value is %d Celsius/Fahrenheit.”	IBM Director Agent	No
2	Warning	“Temperature Sensor %d exceeded the manufacturer/user defined threshold of %d Celsius/Fahrenheit. The current value is %d Celsius/Fahrenheit.”	IBM Director Agent	No
2	Normal	“Temperature Sensor %d reports normal.”	IBM Director Agent	No
3	Critical	“Voltage Sensor %d exceeded/fell below threshold of %.2f Volts. The current value is %.2f Volts.”	IBM Director Agent	No
3	Normal	“Voltage Sensor %d reports normal.”	IBM Director Agent	No
4	Critical	“System Enclosure Sensor reported intrusion detection.”	IBM Director Agent	No

Table 125. IBM Director Agent events (continued)

Event ID	Severity	Descriptions	Source of the event	New in IBM Director 4.1
4	Normal	“System Enclosure Sensor reports normal.”	IBM Director Agent	No
5	Critical	“Fan Sensor %d fell below threshold of %d RPM. The current value is %d RPM.”	IBM Director Agent	No
5	Warning	“Fan Sensor %d fell below threshold of %d. The current value is %d RPM.”	IBM Director Agent	No
5	Normal	“Fan Sensor reports normal.”	IBM Director Agent	No
6	Warning	Reserved		
7	Critical	“Logical drive %s fell below threshold of %0.2f MB. The current value is %0.2f MB.”	IBM Director Agent	No
7	Warning	“Logical drive %s fell below threshold of %0.2f MB. The current value is %0.2f MB.”	IBM Director Agent	No
7	Normal	“Logical drive %s free space is normal. The current value is %0.2f MB.”	IBM Director Agent	No
8		Reserved		
9	Critical	“IDE/SCSI device identified as physical drive %i is predicting an imminent failure.”	IBM Director Agent	No
9	Normal	“IDE/SCSI device identified as physical drive %i is not predicting a failure.”	IBM Director Agent	No
10		Reserved		
11		Reserved		
12	Critical	“The computer is disconnected from the network.“	IBM Director Agent	No
12	Normal	“The computer is connected to the network.”	IBM Director Agent	No
13	Warning	“The lease on %s expired. It expired on %s.”	IBM Director Agent	No

Table 125. IBM Director Agent events (continued)

Event ID	Severity	Descriptions	Source of the event	New in IBM Director 4.1
13	Normal	“The lease on %s is normal. It will expire on %s.”	IBM Director Agent	No
14	Warning	“The warranty on %s has expired. It expired on %s.”	IBM Director Agent	No
14	Normal	“The warranty on %s is normal. It will expire on %s.”	IBM Director Agent	No
15	Warning	“A redundant NIC event occurred.”	Requires a teamed configuration	No
16	Warning	“NIC in Port/PCI Slot %d has Switched Over”	IBM Director Agent	No
17	Warning	“NIC in Port/PCI Slot %d has Switched Back”	IBM Director Agent	No
18	Critical	“Processor device identified as processor in slot %d is predicting an imminent failure.”	IBM Director Agent	No
18	Normal	“Processor device identified as processor in slot %d is not predicting a failure.”	IBM Director Agent	No
19	Critical	“Memory device identified as memory in bank %d is predicting an imminent failure.”	IBM Director Agent	No
19	Normal	“Memory device identified as memory in bank %d is not predicting a failure.”	IBM Director Agent	No
22	Critical	“Predictive Failure Detected. Please check the system management processor error log for more information. This event must be cleared manually.”	IBM Director Agent	No
23	Critical	“PowerSupply device identified as PowerSupply %d reports critical state with possible loss of redundancy.”	IBM Director Agent	No
23	Warning	“PowerSupply device identified as PowerSupply %d has lost AC power and loss of standby power is imminent.”	IBM Director Agent	No
23	Normal	“PowerSupply device identified as PowerSupply %d reports normal.”	IBM Director Agent	No

Table 125. IBM Director Agent events (continued)

Event ID	Severity	Descriptions	Source of the event	New in IBM Director 4.1
24	Critical	“The system management processor error log is full. This event must be cleared manually.”	IBM Director Agent	No
24	Warning	“The system management processor error log is 75% full. This event must be cleared manually.”	IBM Director Agent	No
25	Warning	“The system management processor has been accessed via a remote login. This event must be cleared manually.”	IBM Director Agent	No
26	Warning	“The NIC in Port/PCI Slot %d has Failed”	IBM Director Agent	Yes
27	Warning	“NIC in Port/PCI Slot %d is Offline”	IBM Director Agent	Yes
28	Normal	“NIC in Port/PCI Slot %d is Online”	IBM Director Agent	Yes
29	Critical	“PowerSupply device identified as PowerSupply %d has failed. This event must be cleared manually.”	IBM Director Agent	Yes
30	Critical	“Drive %d has reported a fault. This event must be cleared manually.”	IBM Director Agent	Yes
31	Critical	“A fan has failed. This event must be cleared manually.”	IBM Director Agent	Yes
32	Critical	“System voltage is out of specification. Please check the system management processor log for more information. This event must be cleared manually.”	IBM Director Agent	Yes

Table 126. IBM Director ServeRAID events in the Windows event log

Type	Event	Description
Warning	20	Defunct drive (FRU Part # + [number] +” } on controller “+ [number] +” , channel “+ [number] +” , SCSI ID “+ [number] +” .“
Critical	20	Commands not responding on Controller + [number] +” .“
Critical	20	The battery-backup cache device on Controller + [number] +” needs a new battery.“

Table 126. IBM Director ServeRAID events in the Windows event log (continued)

Type	Event	Description
Critical	20	The battery-backup cache device on Controller + [number] +" is defective "+ [number] +" "
Critical	20	Background polling commands not responding on Controller + [number] +" "+ [number] +" "
Critical	20	Cannot read controller configuration
Warning	20	Controller + [number] +" failover detected. Passive controller is now active."
Critical	20	Logical Drive + [number] +" is Critical on Controller "+ [number] +" ."
Critical	20	Logical Drive + [number] +" is Offline on Controller "+ [number] +" ."
Critical	20	Rebuild failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	Synchronization failed on Logical + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	Migration failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	Compression failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	Decompression failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	FlashCopy failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	Rebuild failed on Array + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	Synchronization failed on Array + [number] +" of Controller "+ [number] +" "+ [number] +" ."
Critical	20	FlashCopy failed on Array + [number] +" of Controller "+ [number]+" "+ [number] +" ."
Critical	20	Defunct drive on Controller + [number] +" , Channel "+ [number] +" , SCSI ID "+ [number] +" ."
Warning	20	PFA drive on Controller + [number] +" , Channel "+ [number] +" , SCSI ID "+ [number] +" ."
Critical	20	Defunct drive (FRU Part # + [number] +" } on controller "+ [number] +" , channel "+ [number] +" , SCSI ID "+ [number] +" ."
Warning	20	PFA drive (FRU Part # + [number] +") on Controller "+ [number] +" , Channel "+ [number] +" , SCSI ID "+ [number] +" ."
Warning	20	Unsupported physical drive found on Controller + [number] +" , Channel "+ [number] +" , SCSI ID "+ [number] +" ."

Table 126. IBM Director ServeRAID events in the Windows event log (continued)

Type	Event	Description
Critical	20	Enclosure device not responding on Controller + [number] +" , Channel "+ [number] +" ."
Critical	20	Enclosure fan + [number] +" on Controller "+ [number] +" , Channel "+ [number] +" is malfunctioning."
Warning	20	Enclosure fan + [number] +" on Controller "+ [number] +" , Channel "+ [number] +" has been removed."
Critical	20	Enclosure temperature is in normal range on Controller + [number] +" , Channel "+ [number] +" ."
Critical	20	Enclosure temperature is out of normal range on Controller + [number] +" , Channel "+ [number] +" ."
Critical	20	Enclosure power supply + [number] +" on Controller "+ [number] +" , Channel "+ [number] +" is malfunctioning."
Warning	20	Enclosure power supply + [number] +" on Controller "+ [number] +" , Channel "+ [number] +" has been removed."

The following table provides ServeRAID event text that is sent to the CIM.Director.Agent Events.ServeRAID Health event type and describes the specific events that have occurred in the subsystem.

Table 127. ServeRAID Health event type text

Event text	Severity	Category
Defunct drive (FRU Part # + [number] + on controller "+ [number] +, channel "+ [number] +" , SCSI ID "+[number] +" ."	Warning	Alert
Commands not responding on Controller + [number] +" ."	Critical	Alert
The battery-backup cache device on Controller + [number]+" needs a new battery.	Critical	Alert
The battery-backup cache device on Controller +[number] +" is defective "+ [number] +" "	Critical	Alert
Background polling commands not responding on Controller + [number] +" "+ [number] +" "	Critical	Alert
Cannot read controller configuration.	Critical	Alert

Table 127. ServeRAID Health event type text (continued)

Event text	Severity	Category
Controller + [number] +" failover detected. Passive controller is now active."	Warning	Alert
Logical Drive + [number] + " is Critical on Controller "+ [number] +" ."	Critical	Alert
Logical Drive + [number] +" is Offline on Controller "+ [number] +" ."	Critical	Alert
Rebuild failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."	Critical	Alert
Synchronization failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."	Critical	Alert
Migration failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."	Critical	Alert
Compression failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."	Critical	Alert
Decompression failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."	Critical	Alert
FlashCopy failed on Logical Drive + [number] +" of Controller "+ [number] +" "+ [number] +" ."	Critical	Alert
Rebuild failed on Array + [number] +" of Controller "+ [number] +" "+ [number] +" ."	Critical	Alert
Synchronization failed on Array + [number] +" of	Critical	Alert

Appendix D. Terminology summary and abbreviation list

This appendix provides a summary of IBM Director terminology and a list of abbreviations and acronyms used in IBM Director publications.

IBM Director terminology summary

The following terminology is used in the IBM Director publications.

A *system* is a server, workstation, desktop computer, or mobile computer. An *SNMP device* is a device (such as a network printer) that has SNMP installed or embedded. An *IBM Director environment* is a group of systems managed by IBM Director.

IBM Director software is made up of three main components:

- IBM Director Server
- IBM Director Agent
- IBM Director Console

The hardware in an IBM Director environment is referred to in the following ways:

- A *management server* is a server on which IBM Director Server is installed.
- A *managed system* is a system on which IBM Director Agent is installed.
- A *management console* is a system on which IBM Director Console is installed.

The Server Plus Pack is a portfolio of tools for advanced server management that extends the functionality of IBM Director. These tools are called *extensions*.

The *IBM Director service account* is an operating-system user account on the management server. This account is used to install IBM Director Server and is the account under which the IBM Director Service runs.

The *database server* is the server on which the database application is installed.

Abbreviation and acronym list

The following table lists abbreviations and acronyms used in the IBM Director 4.1 publications.

Table 128. Abbreviations and acronyms used in IBM Director

Abbreviation or acronym	Definition
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI adapter
BIOS	basic input/output system
CIM	Common Information Model
CIMOM	CIM Object Manager
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management
CSV	comma-separated value
DES	data encryption standard
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DMI	Desktop Management Interface
DNS	Domain Name System
DSA	Digital Signature Algorithm
EEPROM	electrically erasable programmable read-only memory
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	file transfer protocol

Table 128. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
GB	gigabyte
Gb	gigabit
GMT	Greenwich Mean Time
GUI	graphical user interface
GUID	globally unique identifier
HTML	hypertext markup language
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPX	internetwork packet exchange
ISDN	integrated services digital network
ISMP	integrated system management processor
JVM	Java® Virtual Machine
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JFC	Java Foundation Classes
JRE	Java Runtime Environment
KB	kilobyte
Kb	kilobit
Kpbs	kilobit per second
KVM	keyboard/video/mouse

Table 128. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
LAN	local area network
LED	light-emitting diode
MAC	media access control
MB	megabyte
Mb	megabit
Mbps	megabits per second
MD5	message digest 5
MDAC	Microsoft Data Access Control
MHz	megahertz
MIB	Management Information Base
MIF	Management Information Format
MMC	Microsoft Management Console
MPA	Management Processor Assistant
MSCS	Microsoft Cluster Server
MST	Microsoft software transformation
NIC	network interface card
NNTP	Network News Transfer Protocol
NVRAM	nonvolatile random access memory
ODBC	Open DataBase Connectivity
OID	object ID
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended

Table 128. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
PDF	Portable Document Format
PFA	Predictive Failure Analysis
POST	Power On Self Test
RAM	random access memory
RDM	Remote Deployment Manager
RPM	(1) Red Hat Package Manager (2) rotations per minute
SID	(1) security identifier (2) Oracle system identifier
SLP	service location protocol
SMBIOS	System Management BIOS
SMI	System Management Information
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SNMP	Simple Network Management Protocol
SNA	Systems Network Architecture
SPB	software package block
SQL	Structured Query Language
SSL	Secure Sockets Layer
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
UDP	User Datagram Protocol

Table 128. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
UID	unique ID
UIM	upward integration module
UNC	universal naming convention
USB	Unversal serial bus
UUID	universal unique identifier
VPD	vital product data
VRM	voltage regulator module
WAN	wide area network
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
XML	extensible markup language

Appendix E. 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. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation® system, and 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:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Go to the IBM Support Web site at http://www.ibm.com/pc/support/ to check for technical information, hints, tips, and new device drivers.
- Use an IBM discussion forum on the IBM Web site to ask questions.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the publications that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

Using the documentation

Information about your IBM xSeries or IntelliStation system and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/pc/support/ and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi.

Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM xSeries and IntelliStation products, services, and support. The address for IBM xSeries information is http://www.ibm.com/eserver/xseries/. The address for IBM IntelliStation information is http://www.ibm.com/pc/intellistation/.

You can find service information for your IBM products, including supported options, at http://www.ibm.com/pc/support/.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to http://www.ibm.com/services/sl/products/.

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

Appendix F. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Some software may differ from its retail version (if available) and may not include all user manuals or all program functionality.

IBM makes no representations or warranties regarding third-party products or services.

Edition notice

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Active PCI
Acitve PCI-X
Alert on LAN
Asset ID
BladeCenter
e-business logo
eServer
FlashCopy
IBM
NetView
Predictive Failure Analysis
Redbooks
ServeRAID
ServerProven
Tivoli
Tivoli Enterprise
Tivoli Enterprise Console
TotalStorage

IntelliStation
Netfinity

Wake on LAN
xSeries

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Glossary

A

Active PCI Manager task. An IBM Director extension available in the Server Plus Pack that can be used to manage all PCI and PCI-X adapters in a managed system. The Active PCI Manager task provides two subtasks in IBM Director: Fault Tolerant Management Interface (FTMI) and Slot Manager (previously released under the name Active PCI Manager).

alert. A notification of an event occurrence. If an event action plan is configured to filter a specific event, when that event occurs an alert is generated in response to that event.

alert-forwarding profile. In the IBM Director Management Processor Assistant and BladeCenter Assistant tasks, a profile that specifies where any remote alerts for the service processor in a BladeCenter chassis are sent. Alert forwarding can ensure that alerts are sent, even if a managed system experiences a catastrophic failure, such as an operating-system failure.

alert standard format (ASF). A specification created by the Distributed Management Task Force (DMTF) that defines remote-control and alerting interfaces that can best serve a client (or agent) in an environment that does not have an operating system.

anonymous command execution. The ability to execute commands on a target system as either system account (for managed systems running Windows) or root (for managed systems running Linux). You can restrict anonymous command execution by disabling this feature and always requiring a user ID and password.

ASF. See alert standard format.

Advanced System Management (ASM) interconnect.
A feature of IBM service processors. It enables a network administrator to connect up to 24 servers to one service processor, thus eliminating the need for multiple modems, telephones, and LAN ports. It provides strong out-of-band management functions, including system power control, service processor event log management, firmware updates, alert notification, and user profile configuration.

Advanced System Management (ASM) interconnect network. A network of IBM servers created by using the ASM interconnect feature. The servers are connected through RS-485 ports and standard Cat-5 cables. When servers containing ISMPs and ASM processors are connected to such a network, IBM Director can manage them out-of-band.

Advanced System Management (ASM) PCI adapter.
An IBM service processor. It is built into the system board of Netfinity 7000 M10 and 8500R servers; it also was available as an

option that could be installed in a server that contained an ASM processor. When an ASM PCI adapter is used in conjunction with an ASM processor, the ASM PCI adapter acts as an Ethernet gateway, while the ASM processor retains control of the server. When used as an ASM gateway, the ASM PCI adapter can communicate with other ASM PCI adapters and ASM processors only.

Advanced System Management (ASM) processor. A service processor built into the system board of mid-range Netfinity and early xSeries servers. IBM Director can connect out-of-band to an ASM processor located on an ASM interconnect; either an ASM PCI adapter or a Remote Supervisor Adapter must serve as the ASM gateway.

Asset ID task. An IBM Director task that can be used to track lease, warranty, user, and system information, including serial numbers. You also can use the Asset ID feature to create personalized data fields to track custom information.

association. (1) A way of displaying the members of a group in a logical ordering. For example, the Object Type association displays the managed objects in a group in folders based on their type. (2) A way to display additional information about the members of the group. For example, the Event Action Plans association displays any event action plans applied to the managed objects in the group in an Event Action Plan folder.

B

blade server. An IBM eServer BladeCenter HS20 server. Each BladeCenter chassis can hold up to 14 of these high-throughput, two-way, SMP-capable Xeon-based servers.

BladeCenter Assistant task. An IBM Director task that can be used to configure and manage BladeCenter units.

BladeCenter chassis. A BladeCenter component that acts as an enclosure. This 7-U modular chassis can contain up to 14 blade servers. It enables the individual blade servers to share resources such as the management, switch, power, and blower modules.

BladeCenter Deployment wizard. A BladeCenter Assistant subtask that can be used to configure BladeCenter chassis, including setting up security protocols, enabling network protocols, and assigning IP addresses to the management and switch modules. It also can create a reusable profile that will automatically configure new BladeCenter chassis when they are added to the IBM Director environment.

BladeCenter Diagnostics. A Real Time Diagnostics subtask that can be used to determine problems in components in a BladeCenter unit.

bottleneck. In the Capacity Manager task, a condition in which one or more performance analysis monitors meet or exceed their preset threshold settings.

C

Capacity Manager task. An IBM Director extension, available in the Server Plus Pack, that can be used to plan resource management and monitor managed-system hardware performance. It can identify bottlenecks and potential bottlenecks, recommend ways to improve performance through performance analysis reports, and forecast performance trends.

CIM. See Common Information Model.

CIM Browser task. An IBM Director task that can provide in-depth information that you can use for problem determination or developing a system-management application using the CIM layer.

Common Information Model (CIM). A standard defined by the Distributed Management Task Force (DMTF). CIM is a set of methodologies and syntaxes that describes the management features and capabilities of computer devices and software.

complex. An IBM Director managed object that comprises two physical xSeries platforms that are interconnected through their SMP Expansion Modules, for example, a multi-node xSeries 440 server. A complex defines the system partition that is made from the physical platforms, or nodes, in the complex.

component association. In the IBM Director Rack Manager task, a function that can make a managed system or device rack mountable when the inventory collection feature of IBM Director does not recognize the managed system or device. The function associates the system or device with a predefined component.

D

data encryption standard (DES). A block cipher algorithm that can be used to encrypt data transmitted between managed systems and the management server. Designed by the National Bureau of Standards, DES enciphers and deciphers data using a 64-bit key.

database server. The server on which the database application and database used in conjunction with IBM Director Server is installed.

DES. See data encryption standard.

Desktop Management Interface (DMI). A specification from the Desktop Management Task Force (DMTF) that establishes a standard framework for managing networked computers. DMI includes hardware and software, desktop systems, and servers, and it defines a model for filtering events.

DMI provides a common path to access information about all aspects of a managed system, including microprocessor type, installation date, attached printers and other peripheral devices, power sources, and maintenance history. DMI is not related to any specific hardware, operating system, or management protocols. It is mappable to existing management protocols such as Simple Network Management Protocol (SNMP).

detect-and-deploy profile. A profile created by the BladeCenter Deployment wizard. When the profile is enabled and a new BladeCenter chassis is discovered by IBM Director, the profile settings (management module name, network protocols, and assigned IP addresses) are applied automatically to the new BladeCenter chassis.

Diffie-Hellman key exchange. A security protocol developed by Whitfield Diffie and Martin Hellman in 1976. This protocol enables two users to exchange a secret digital key over an insecure medium. IBM Director uses the Diffie-Hellman key exchange protocol when establishing encrypted sessions between the management server, managed systems, and management consoles.

digital signature algorithm (DSA). A security protocol used by IBM Director. DSA uses a pair of keys (one public and one private) and a one-way encryption algorithm to provide a robust way of authenticating users and systems. If a public key can successfully decrypt a digital signature, a user can be sure that the signature was encrypted using the private key.

DirAdmin. One of two operating-system groups that are created automatically when IBM Director Server is installed. By default, members of the DirAdmin group have basic administrative privileges in the IBM Director environment.

DIRCMD. The command-line interface to IBM Director. It enables members of the DirAdmin group to use a command-line prompt to access, control, and gather information from IBM Director Server.

DirSuper. One of two operating-system groups that are created automatically when IBM Director Server is installed. The IBM Director service account is assigned automatically to the DirSuper group. Members of the DirSuper group have the same privileges as the DirAdmin group, as well as the ability to permit or restrict users' access to IBM Director.

discovery. The process by which IBM Director Server identifies and establishes connections with systems on which IBM Director Agent is installed. In a discovery operation, the management server sends out a discovery request and waits for responses from managed systems. The managed systems wait for this request and respond to the management server.

discovery, BladeCenter chassis. The process by which IBM Director Server identifies and establishes communication with a BladeCenter chassis. If the management server and the BladeCenter chassis are on the same subnet, IBM Director uses Service Location Protocol (SLP) to discover the BladeCenter chassis automatically. Otherwise, a network administrator must use IBM Director Console to create a BladeCenter chassis managed object manually.

discovery, broadcast. A type of discovery supported by IBM Director, in which the management server sends out either a general broadcast packet over the LAN or a broadcast packet to a specific subnet.

discovery, broadcast relay. A type of discovery supported by IBM Director, in which the management server sends a special discovery request to a particular managed system, instructing the managed system to perform a discovery operation on the local subnet using a general broadcast. This method of discovery enables the management server to discover TCP/IP and IPX systems when the systems are not directly reachable by broadcast packets because of network configuration.

discovery, multicast. A type of discovery supported by IBM Director, in which the management server sends a packet to a specified multicast address. Multicasts are defined with a maximum time to live (TTL) and are discarded when the TTL expires. Multicast discovery is available only for TCP/IP systems.

discovery, SNMP. A type of discovery supported by IBM Director, in which IBM Director sends discovery requests to seed addresses (such as routers and name servers). The address tables found on the specified devices are then searched; the search continues until no additional SNMP devices are found.

discovery, unicast. A type of discovery supported by IBM Director, in which the management server sends a directed request to a specific address or range of addresses. This method of discovery is useful in networks where both broadcasts and multicasts are filtered.

DMI. See Desktop Management Interface.

DMI Browser task. An IBM Director task that can provide in-depth information about DMI components. Used primarily for systems management, DMI does not support management of network devices, such as bridges, routers, and printers, as SNMP does.

dynamic group. See group, dynamic.

E

event. An occurrence of a predefined (in IBM Director) condition relating to a specific managed object that identifies a change in a system process or a device. The notification of that change can be generated and tracked, for example, notification that a managed system is offline.

event action. The action that IBM Director takes in response to a specific event or events. In the Event Action Plan Builder, you can customize an event action type by specifying certain parameters and saving the event action. You must assign the customized event action (and an event filter) to an event action plan before IBM Director can execute the event action.

event action plan. A user-defined plan that determines how IBM Director will manage certain events. An event action plan is comprised of one or more event filters and one or more customized event actions. The event filters specify which events are managed, and the event actions specify what happens when the events occur.

Event Action Plan wizard. An IBM Director Console wizard that can be used to create simple event action plans.

event-data substitution variable. A variable that can be used to customize event-specific text messages for certain event actions.

event filter. A filter that specifies the event criteria for an event action plan. Events must meet the criteria specified in the event filter in order to be processed by the event action plan that the filter is assigned to.

extension. See IBM Director extension.

F

Fault Tolerant Management Interface (FTMI). An Active PCI Manager subtask that can be used to manage PCI and PCI-X network adapters on managed systems. FTMI can be used to view network adapters that are members of fault-tolerant groups. It also can be used to perform offline, online, failover, and eject operations on the displayed adapters.

field-replaceable unit (FRU). A component of an IBM system that can be replaced in the field by a service technician. Each FRU is identified by a unique seven-digit alphanumeric code.

File Transfer task. An IBM Director task that can be used to transfer files from one location (managed system or management server) to another location and synchronizes files, directories, or drives.

file-distribution server. In the Software Distribution task, an intermediate server that is used to distribute a software package when the redirected-distribution method is used.

forecast. A function in the Capacity Manager task that can provide a prediction of future performance of a managed system using past data collected on that managed system.

FRU. See field-replaceable unit.

FTMI. See Fault Tolerant Management Interface.

G

group. A logical set of managed objects. Groups can be dynamic, static, or task-based.

group, dynamic. A group of managed systems or managed objects based on a specific criterion, for example, a group of managed systems running Windows 2000 with Service Pack 3 or later. IBM Director automatically adds or removes managed systems or managed objects to or from a dynamic group when their attributes or properties change.

group, static. A user-defined group of managed systems or managed objects, for example, all servers in a particular department. IBM Director does not automatically update the contents of a static group.

group, task-based. A dynamic group based on the types of tasks for which the group of managed objects is enabled. For example, selecting Rack Manager in the Available Tasks pane includes only those managed objects that can be used with the Rack Manager task.

GUID. See Universal Unique Identifier.

H

Hardware Status task. An IBM Director task that can be used to view managed-system and -device hardware status from the management console. The Hardware Status task notifies you whenever a managed system or device has a hardware status change by displaying an icon in the lower-right corner of IBM Director Console. Whenever a managed system or device generates a hardware event, the Hardware Status task also adds the system or device to the applicable hardware status group (critical, warning, or information).

I

IBM Director Agent. A component of IBM Director software. When IBM Director Agent is installed on a system, the system can be managed by IBM Director. IBM Director Agent transfers data to the management server using several network protocols, including TCP/IP, NetBIOS, IPX, and SNA.

IBM Director Console. A component of IBM Director software. When installed on a system, it provides a graphical user interface (GUI) and enables network administrators to access IBM Director Server. IBM Director Console transfers data to and from the management server using TCP/IP.

IBM Director database. The database that contains the data stored by IBM Director Server.

IBM Director environment. The complex, heterogeneous environment managed by IBM Director. It encompasses systems, BladeCenter chassis, software, SNMP devices, and more.

IBM Director extension. A tool that extends the functionality of IBM Director. IBM Director extensions include the IBM Director Server Plus Pack, Remote Deployment Manager, Software Distribution, and others.

IBM Director Server. The main component of IBM Director software. When installed on the management server, it provides basic functions such as discovery of the managed systems, persistent storage of configuration and management data, an inventory database, event listening, security and authentication, management console support, and administrative tasks.

IBM Director Server Plus Pack. A portfolio of IBM Director extensions specifically designed for use with xSeries and Netfinity servers. It includes Active PCI Manager, Capacity Manager, Rack Manager, Software Rejuvenation, and System Availability.

IBM Director Server service. A service that runs automatically on the management server and provides the server engine and application logic for IBM Director.

IBM Director service account. The operating-system account that was used to install IBM Director Server.

in-band communication. Communication that occurs through the same channels as data transmissions, for example, the interprocess communication that occurs between IBM Director Server, IBM Director Agent, and IBM Director Console.

integrated systems management processor (ISMP). A service processor built into the system board of some xSeries servers. The successor to the ASM processor, the ISMP does not support in-band communication in systems running NetWare or Caldera Open UNIX®. In order for IBM Director Server to connect out-of-band to an ISMP, the server containing the ISMP must be installed on an ASM interconnect network with a Remote Supervisor Adapter serving as the ASM gateway.

interprocess communication (IPC). A system that lets threads and processes transfer data and messages among themselves; it is used to offer services to and receive services from other programs. Interprocess communication is used to transfer data and messages between IBM Director Server and IBM Director Agent, as well as IBM Director Server and service processors. It is also called in-band communication

inventory software dictionary. In the Inventory task, a file that tracks the software installed on managed systems in a network. The software dictionary file contains predefined software profiles that recognize most standard software packages after they are installed. If you have installed software that does not correspond to a predefined software profile included with IBM Director, you can edit the software dictionary file to update your software inventory.

Inventory task. An IBM Director task that can be used to collect data about the hardware and software currently installed on the managed systems in a network.

IPC. See interprocess communication.

ISMP. See integrated systems management processor.

J

job. In Scheduler, a single noninteractive task or set of noninteractive tasks scheduled to run at a later time.

K

keyboard/video/mouse (KVM). A select button on a BladeCenter server bay.

KVM. See keyboard/video/mouse.

L

Light Path Diagnostics. An IBM technology present in xSeries servers. It constantly monitors selected features; if a failure occurs, a light-emitting diode (LED) is illuminated, letting an administrator know that a specific component or subsystem needs to be replaced.

M

MAC address. See media access control (MAC) address.

managed device. An SMNP device managed by IBM Director.

managed group. A group of systems or objects managed by IBM Director.

managed object. An item managed by IBM Director. Managed objects include managed systems, Windows NT clusters, BladeCenter chassis, management processors, SNMP devices, multi-node servers (complexes), system partitions, physical platforms, nodes, and remote I/O enclosures. In IBM Director Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or complex, for example).

managed object ID. A unique identifier for each managed object. It is the key value used by IBM Director database tables.

managed system. A system (server, desktop computer, workstation, or mobile computer) on which IBM Director Agent is installed. Such a system is managed by IBM Director.

managed system, secured. A managed system that can be accessed only by an authorized management server.

managed system, unsecured. A managed system that can be accessed by any management server.

management console. A system (server, desktop computer, workstation, or mobile computer) on which IBM Director Console is installed.

management module. The BladeCenter component that handles systems-management functions. It configures the chassis and switch modules, communicates with the blade servers and all BladeCenter modules, multiplexes the keyboard/video/mouse (KVM), and monitors critical information about the chassis and blade servers.

management processor. See service processor.

Management Processor Assistant (MPA). An IBM Director task that can be used to configure, monitor, and manage service processors installed in Netfinity and xSeries servers.

Management Processor Assistant (MPA) Agent. An IBM Director Agent feature that enables in-band communication with the service processors installed in Netfinity and xSeries servers. It also handles in-band alert notification for service processors installed in managed systems running Linux, NetWare, and Caldera Open UNIX.

management server. The server on which IBM Director Server is installed.

media access control (MAC) address. A standardized data-link layer address for every port or device that is connected to a LAN. Other devices in the network use MAC addresses to locate specific ports and to create and update routing tables and data structures. The BladeCenter Deployment wizard uses the MAC address (preceded by “MM”) as the default name for a BladeCenter management module.

Message Browser. An IBM Director Console window that displays alerts sent to IBM Director Console.

Microsoft Cluster Browser task. An IBM Director task that can be used to display the structure, nodes, and resources associated with a Microsoft Cluster Server (MSCS) cluster; determine the status of a cluster resource, and view the associated properties of the cluster resources.

Microsoft Management Console (MMC). An application that provides a graphical user interface and a programming environment in which consoles (collections of administrative tools) can be created, saved, and opened. It is part of the Microsoft Platform Software Development Kit and is available for general use. On managed systems running Windows, the MMC is installed at the same time as Web-based Access.

MMC. See Microsoft Management Console.

MPA. See Management Processor Assistant.

multicast discovery. See discovery, multicast.

N

node. A physical platform that has at least one SMP Expansion Module. As of March 2003, the xSeries 440 is the only server model that contains chassis that can be nodes. Additional attributes are assigned to a physical platform when it is a node. These additional attributes record the number of SMP Expansion Modules, SMP Expansion Module Ports, and RXE Expansion ports on the physical chassis.

notification. See alert.

O

out-of-band communication. Communication that occurs through a modem or other asynchronous connection, for example, service processor alerts sent through a modem. In an IBM Director environment, such communication is independent of both the operating system and interprocess communication (IPC).

P

PCI. See Peripheral Component Interconnect.

PCI-X. See Peripheral Component Interconnect-Extended.

Peripheral Component Interconnect (PCI). A computer bussing architecture that defines electrical and physical standards for electronic interconnection.

Peripheral Component Interconnect-Extended (PCI-X). An enhanced computer bussing architecture that defines electrical and physical standards for electronic interconnection. PCI-X enhances the PCI standard by doubling the throughput capability and providing new adapter-performance options while maintaining backward compatibility with PCI adapters.

PFA. See Predictive Failure Analysis.

physical platform. (1) An IBM Director managed object that represents a remote system that is discovered out-of-band by IBM Director Server. The remote system is discovered through the use of the service location protocol (SLP) and the Remote Supervisor Adapter on the remote system. As of March 2003, the only server models whose chassis can be discovered as physical platforms in this manner are the xSeries 360 and xSeries 440. A physical platform enables identification of some systems without communicating through the operating system or any IBM Director Agent that has been installed on that system. Because IBM Director Agent is not used to provide the support for physical platforms, only limited functionality exists. (2) An IBM Director managed object representing a system that has IBM Director Agent and the Management Processor Assistant (MPA) agent installed.

plug in. See IBM Director extension.

Predictive Failure Analysis (PFA). An IBM technology that periodically measures selected attributes of component activity. If a predefined threshold is met or exceeded, a warning message is generated.

private key. A central component of the digital-signature algorithm. Each management server holds a private key and uses it to generate digital signatures that managed systems use to authenticate a management server's access.

Process Management task. An IBM Director task that manages individual processes on managed systems. Specifically, you can start, stop, and monitor processes and set up process monitors to generate an event whenever an application changes state. You also can issue commands on managed systems.

process monitor. A Process Management subtask that can be used to check for when a specified application process starts, stops, or fails to start running during a specified period of time after system startup or after the monitor is sent to a managed system.

process task. A Process Management subtask that can be used to simplify the running of programs and processes. You can predefine a command that can be run on a managed system or group by dragging a process task onto a managed system or systems.

public key. A central component of the digital-signature algorithm. Each managed system holds a public key that corresponds to the private key held by the management server. When the management server requests access, the managed system sends the management server the public key and a random data block. The management server then generates a digital signature of the data block using its private key and sends it back to the managed system. The managed system then uses the public key to verify the validity of the signature.

R

Rack Manager task. An IBM Director extension available in the Server Plus Pack that can be used to group equipment in virtual racks by associating equipment such as managed systems and devices, networking devices, power devices, and monitors with a rack to visually represent an existing rack in a network environment.

RDM. See Remote Deployment Manager.

Real Time Diagnostics. An IBM Director extension that administrators can use to run industry-standard diagnostic utilities on servers while they are running. It is available for use on servers running Windows 2000 or Windows 2000 Advanced Server only.

redirected distribution. A method of software distribution that uses a file-distribution server.

Remote Control task. An IBM Director task that can be used to manage a remote system by displaying the screen image of the managed system on a management console.

Remote Deployment Manager (RDM). An extension to IBM Director that handles deployment and configuration of IBM systems. Using RDM, a network administrator can remotely flash BIOS, modify configuration settings, perform automated installations of operating systems, back up and recover primary partitions, and permanently erase data when systems are redeployed or retired.

Remote Session task. An IBM Director task that can be used to run command-line programs on a remote managed system. Remote Session uses less network traffic and system resources than the Remote Control task, and therefore is useful in low-bandwidth situations.

Remote Supervisor Adapter. An IBM service processor. It is built into the system board of some xSeries servers and available as an optional adapter for use with others. When used as an ASM gateway, the Remote Supervisor Adapter can communicate with all service processors on the ASM interconnect.

Resource Monitors task. An IBM Director task that can be used to provide statistics about critical system resources, such as microprocessor, disk, and memory usage, and is used to set thresholds to detect potential problems with managed systems or devices. When a threshold is met or exceeded, an event is generated.

resource-monitor threshold. The point at which a resource monitor generates an event.

S

Scheduler. An IBM Director function that executes a single noninteractive task or set of noninteractive tasks at a specific date and time or in a repeating interval.

secure sockets layer (SSL). A security protocol developed by Netscape. Designed to enable secure data transmission on a unsecure network, it provides encryption and authentication using digital certificates such as those provided by the digital-signature algorithm. In the IBM Director environment, it can be used to secure communications between the management server and management console.

Server Plus Pack. See IBM Director Server Plus Pack.

ServeRAID Manager task. An IBM Director task that can be used to monitor ServeRAID controllers that are installed locally or remotely on servers. In IBM Director, you can use the ServeRAID Manager task to view information related to arrays, logical drives, hot-spare drives, and physical drives and view configuration settings. You also can view alerts and locate defunct disk drives.

service location protocol (SLP). A protocol developed by the Internet Engineering Task Force (IETF) to discover the location of services on a network automatically. It is used by IBM Director Server to discover BladeCenter chassis and multi-node servers such as the xSeries 440.

service processor. A generic term for Remote Supervisor Adapters, Advanced System Management processors, Advanced System Management PCI adapters, and integrated system management processors. These hardware-based management processors used in IBM Netfinity and xSeries servers work with IBM Director to provide hardware status and alert notification.

Slot Manager. An Active PCI Manager subtask that can be used to display information about all PCI and PCI-X adapters, analyze PCI and PCI-X performance, and determine the best slots in which to install PCI and PCI-X adapters in a managed system.

SLP. See service location protocol.

SMBIOS. See systems management BIOS.

SMP Expansion Module. An IBM xSeries hardware option. It is a single module that contains microprocessors, disk cache, random access memory, and three SMP Expansion port connections. Two SMP Expansion Modules can fit in a chassis. The IBM xSeries 440 is the first hardware platform that uses SMP Expansion Modules.

SMP Expansion Module Port. A dedicated high-speed port used to interconnect SMP Expansion Modules.

SNMP Access and Trap Forwarding. An IBM Director Agent feature that, when installed on a managed system, enables SNMP-based managers to poll the managed system and receive its alerts. If System Health Monitoring is installed on the managed system also, hardware alerts can be forwarded as SNMP traps.

SNMP Browser task. An IBM Director task that can be used to view and configure the attributes of SNMP devices, for example, hubs, routers, or other SNMP-compliant management devices. You also can use it for SNMP-based management, troubleshooting problems, or monitoring the performance of SNMP devices.

SNMP device. A network device, printer, or computer that has an SNMP device installed or embedded.

SNMP discovery. See discovery, SNMP.

Software Distribution task. An IBM Director task that can be used to import and distribute software packages to an IBM Director managed system or systems. To use the full-featured Software Distribution task (Premium Edition), you must purchase and install the *IBM Director Software Distribution (Premium Edition)* CD.

Software Rejuvenation task. An IBM Director extension available in the Server Plus Pack that can be used to schedule the restart of managed systems or services and configure predictive rejuvenation, which monitors resource utilization and rejuvenates managed systems automatically before utilization becomes critical.

SSL. See secure sockets layer.

static group. See group, static.

switch module. The BladeCenter component that provides network connectivity for the BladeCenter chassis and blade servers. It also provides interconnectivity between the management module and blade servers.

system. A desktop computer, workstation, server, or mobile computer.

System Availability task. An IBM Director extension available in the Server Plus Pack that can be used to analyze the availability of a managed system or group and display statistics about managed system uptime and downtime through reports and graphical representations. It also can identify problematic managed systems that have had too many unplanned outages over a specified period of time.

System Health Monitoring. An IBM Director Agent feature that handles in-band communication and alert notification for managed systems running Windows. In addition to providing active monitoring of critical system functions, it also facilitates upward integration.

system variable. A user-defined keyword and value pair that can be used to test and track the status of network resources. System variables can be referred to wherever event-data substitution is allowed.

systems management BIOS (SMBIOS). A key requirement of the WfM 2.0 specification. SMBIOS extends the system BIOS to support the retrieval of management data required by the WfM specification. To run IBM Director Agent, a system must support SMBIOS, version 2.2 or later.

T

target system. A managed system on which an IBM Director task is performed.

task-based group. See group, task-based.

time to live (TTL). The number of times a multicast discovery request is passed between subnets. When the TTL is exceeded, the packet is discarded.

triple data encryption standard (DES). A block cipher algorithm that can be used to encrypt data transmitted between managed systems and the management server. This is a security enhancement of DES that employs three successive DES block operations.

TTL. See time to live.

U

unicast discovery. See discovery, unicast.

Universal Unique Identifier (UUID). A 128-bit character string guaranteed to be globally unique and used to identify components under management. The UUID enables inventory-level functionality and event tracking of nodes, partitions, complexes, and remote I/O enclosures.

Update Assistant. A wizard that can be used to import IBM software and create software packages. It is part of the Software Distribution task.

upward integration. The methods, processes and procedures that allow lower-level systems-management software, such as IBM Director Agent, to work with higher-level systems-management software, such as Tivoli Enterprise™ or Microsoft SMS.

upward integration module. Software that enables higher-level systems-management software, such as Tivoli Enterprise or Microsoft SMS, to interpret and display data provided by IBM Director Agent. A module also can provide enhancements that allow a system administrator to start IBM Director Agent from within the higher-level systems-management console, as well as collect IBM Director inventory data, and view IBM Director alerts.

UUID. See Universal Unique Identifier.

V

vital product data (VPD). The key information about a server, its components, POST/BIOS, and service processor. This includes machine type, model and serial number, component FRU number, serial number, manufacturer ID, and slot number; POST/BIOS version number, build level, and build date; and service processor build ID, revision numbers, file name, and release date.

VPD. See vital product data.

W

Wake on LAN®. A technology that enables administrators to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, this technology permits an administrator to remotely turn on a server. Once started, the server can be controlled across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

Web-based Access. An IBM Director Agent feature that, when installed on a managed system running Windows, permits a network administrator to use a Web browser or Microsoft Management Console (MMC) to view real-time asset and health information about the managed system.

Index

A

B

C

D

E

H

I

M

N

P

R

S

T

V

W

Part Number: 01R0542

Printed in U.S.A.

(1P) P/N: 01R0542

SC01-R054-20