IBM Director 4.0 for BladeCenter products

Systems Management Guide

SC01-R051-40

Note: Before using this information and the product it supports, be sure to read the general information in Appendix D, “Notices” on page 103.

First Edition (November 2002)

Contents

Figures

Tables

Preface

This book provides instructions for using IBM® Director 4.0 for BladeCenter™ products for systems-management tasks.

How this book is organized

Chapter 1, “Introducing IBM Director 4.0 for BladeCenter products” on page 1, contains an overview of IBM Director.

Chapter 2, “Using IBM Director Console” on page 5, details the basic functionality of IBM Director Console, including group creation and management.

Chapter 3, “IBM Director tasks” on page 15, describes the tasks that you can perform on BladeCenter products using IBM Director.

Chapter 4, “Event management” on page 73, contains information about planning, designing, and building event action plan implementations.

Chapter 5, “Solving IBM Director problems” on page 87, lists solutions to problems you might encounter with IBM Director.

Appendix A, “Resource-monitor attributes” on page 93, details the resource-monitor attributes available using the Resource Monitors task.

Appendix B, “Terminology summary and abbreviation list” on page 97, contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

Appendix C, “Getting help and technical assistance” on page 101, contains information about accessing IBM Support Web sites for help and technical assistance.

Appendix D, “Notices” on page 103, contains product notices and trademarks.

Notices that are used in this book

This book contains the following notices 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) on the *IBM Director* CD in the /docs directory:

- *IBM Director 4.0 for BladeCenter products Installation and Configuration Guide* (dir40_install.pdf)
- *IBM Director 4.0 for BladeCenter products Systems Management Guide* (dir40_sysmgt.pdf)

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

- *IBM @server BladeCenter Systems Management* (REDP3582)
- *The Cutting Edge: IBM @server BladeCenter* (REDP3581)
- *Deploying Microsoft Exchange on IBM @server BladeCenter* (REDP3585)
- *Deploying Lotus Domino on IBM @server BladeCenter* (REDP3584)
- *IBM @server BladeCenter Type 8677 Planning and Installation Guide* (GA27-4327-00)
- *Managing IBM TotalStorage NAS with IBM Director* (SG24-6830-00)
- *IBM Director Security* (REDPO417)
- *Implementing IBM Director Management Solutions* (SG 24-6188-00)
- *Integrating IBM Director with Enterprise Management Solutions* (SG24-5388-01)
- *Implementing Asset ID* (SG 24-6165-00)

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 users. 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 about the next release of IBM Director.

Systems Management - Quick Reference Guide

http://www.ibm.com/pc/qtechinfo/MIGR-4WEP53.html?

This Web page includes links to software downloads, eFixes, Microsoft® Service Packs, and publications for supported releases of IBM Director.

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 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**.

If you are preparing to install IBM Director and you need to download updates for your server, click **Servers** on the IBM Support Web site. The IBM xSeries™, Netfinity®, and PC Server support Web page opens. On the left, click **Downloadable files**. The **Downloadable files by category** drop-down list is displayed. Click the category of downloadable files that you need. If you want to use Update*Xpress*™ to update your server, on the right click **UpdateXpress CD** for the latest release of Update*Xpress*.

Chapter 1. Introducing IBM Director 4.0 for BladeCenter products

IBM Director is a comprehensive systems-management solution. A powerful suite of tools and utilities, IBM Director automates many of the processes required to manage systems proactively, including preventive maintenance, diagnostic monitoring, troubleshooting, and more. It offers a graphical user interface that provides system administrators easy access to both local and remote systems. IBM Director can be used in environments with multiple operating systems (heterogeneous environments).

IBM Director 4.0 for BladeCenter products is a version of IBM Director released for use with IBM @server BladeCenter and @server BladeCenter HS20 *only*.

Important

IBM Director 4.0 for BladeCenter products is supported *only* for use managing BladeCenter chassis and blade servers.

IBM Director 3.x and IBM Director 4.0 for BladeCenter products cannot be installed on the same system. For example, you cannot install IBM Director Server 3.x and IBM Director Server 4.0 on the same server, nor can you run IBM Director Console 3.x and IBM Director Console 4.0 on the same system.

While both versions of IBM Director can coexist in an environment, you must take care to ensure that IBM Director Server 3.x manages *only* systems running IBM Director Agent 3.x and that IBM Director Server 4.0 manages *only* systems running IBM Director Agent 4.0. If you have an existing IBM Director 3.x environment, consider taking the following actions:

- Installing IBM Director 4.0 on a separate subnet.
- Using unicast discovery only, to ensure that IBM Director Server 4.0 discovers *only* blade servers running IBM Director Agent 4.0.
- Ensure that all managed systems running IBM Director Agent 3.x are secured.

You cannot upgrade to IBM Director 4.0 for BladeCenter products from any previous version of IBM Director. Nor will you be able to upgrade from IBM Director 4.0 for BladeCenter products to IBM Director 4.1. However, you can uninstall IBM Director 4.0 for BladeCenter products and install IBM Director 4.1.

IBM Director 4.1 will include support for migrating such management server data as event action plans and thresholds.

IBM Director components

The hardware in an IBM Director environment can be divided into the following groups:

- One or more servers on which IBM Director Server is installed. Such servers are called *management servers*.
- Systems that are managed by IBM Director. Such systems are called *managed systems*.
- Network drivers, printers, or computers that have SNMP agents installed or embedded. Such devices are called *SNMP devices*.

The IBM Director software has three components: IBM Director Server, IBM Director Agent, and IBM Director Console. Each group of hardware in your IBM Director environment requires a different combination of these components.

All three components (IBM Director Server, IBM Director Console, and IBM Director Agent) must be installed on the management server. IBM Director Agent must be installed on each managed system. IBM Director Console must be installed on any system (called a *management console*) from which a system administrator will remotely access the management server. IBM Director software does not need to be installed on SNMP devices.

IBM Director Server

IBM Director Server is the main component of IBM Director; it contains the management data, the server engine, and the application logic. IBM Director Server 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 stores the inventory data in a Structured Query Language (SQL) database. You can access information that is stored in this relational database even when the managed systems are not available. You can use the Microsoft Jet 4.0 database engine, which is included in Microsoft Windows® 2000, or you can use another database application.

When you install IBM Director Server, IBM Director Console and IBM Director Agent are installed automatically.

IBM Director Server can be installed on the following operating systems:

- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Advanced Server (Service Pack 3 required)

IBM Director Server requires a license. Every IBM xSeries server and @server BladeCenter chassis comes with an IBM Director Server license.

IBM Director Agent

IBM Director Agent provides management data to IBM Director Server. Data can be transferred using several network protocols, including TCP/IP, NetBIOS, IPX, and SNA. IBM Director Server can communicate with all systems in your network that have IBM Director Agent installed.

IBM Director Agent can be installed on the following operating systems:

- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Red Hat Linux®, version 7.3
- SuSE Linux, version 8.0

IBM Director Console

IBM Director Console is the graphical user interface (GUI) for IBM Director Server. Data is transferred between IBM Director Console and IBM Director Server through TCP/IP. Using IBM Director Console, system administrators can conduct comprehensive systems management using either a drop-and-drag action or a single click.

When you install IBM Director Console on a system, IBM Director Agent is not installed automatically. If you want to manage the system on which you have installed IBM Director Console (a management console), you also must install IBM Director Agent on that system.

IBM Director Console can be installed on the following operating systems:

- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Professional (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)

IBM Director Agent features

When you install IBM Director Agent, you have the opportunity to install the following features.

System Health Monitoring (Windows only)

System Health Monitoring provides active monitoring of critical system functions, including disk space availability, drive alerts, temperatures, and power supply voltage. It produces and relays hardware alerts.

Note: You *must* install System Health Monitoring if you want to monitor the managed system hardware and send alerts.

SNMP Access and Trap Forwarding

This feature enables SNMP as a protocol for accessing managed-system data. This permits SNMP-based managers to poll the managed system and receive its alerts. If System Health Monitoring is also enabled, this feature enables hardware alerts to be forwarded as SNMP traps.

Note: If you want IBM Director Server to poll SNMP devices and receive their alerts, verify that the Windows SNMP Service and Windows SNMP Trap Service are running on the management server.

Chapter 2. Using IBM Director Console

You can use IBM Director 4.0 for BladeCenter products to centrally manage BladeCenter products, including chassis and blade servers. IBM Director automates tasks such as inventory taking, monitoring of environmental sensors, configuring alerts, and viewing system-health information.

One key to using IBM Director is understanding the concept of managed systems. IBM Director recognizes two types of managed systems: native systems and SNMP devices. Native systems have the IBM Director Agent code installed, whereas SNMP devices are network devices, printers, desktop computers, or servers that have SNMP agents installed or embedded.

Starting tasks

You can start most tasks in IBM Director in five different ways:

- From the menu bar
- From the toolbar
- Dragging a task onto a managed system (or a managed group, in some cases)
- Dragging a managed system (or a managed group, in some cases) onto a task
- Right-clicking a managed system (or managed group, in some cases).

Throughout this guide, only dragging a task onto a managed system or group is explained as the method of starting tasks, although you can use one of the methods listed above as well.

Understanding the IBM Director Console interface

Before you begin using IBM Director Console, review the layout of its interface. Along with a menu bar and toolbar at the top, there are three panes:

- The Groups pane lists all the groups available.
- The Group Contents pane lists the managed systems included in the group selected in the Groups pane.
- The Tasks pane lists IBM Director tasks that are available.

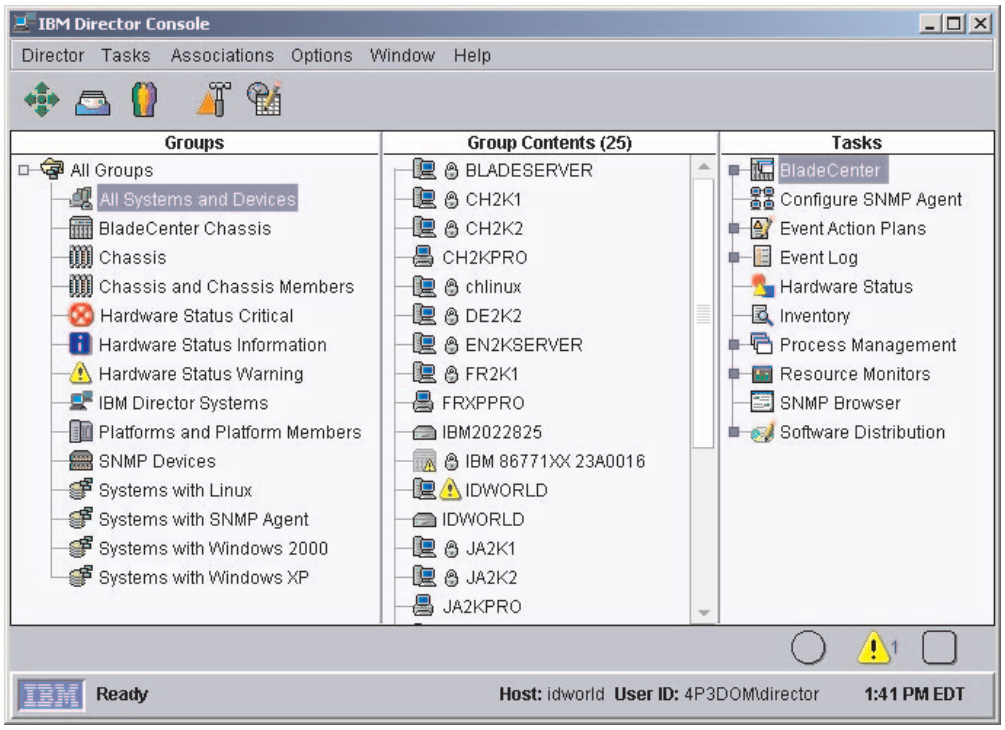

Figure 1. IBM Director Console interface

In the Group Contents pane, the icon beside each managed system indicates whether the system is offline (in which case the icon is gray) or online and also can indicate what kind of managed system it is, such as a chassis.

A padlock icon next to a managed system indicates that the system is being used by another management server and inventory information about the system cannot be collected. You can request access to the system by right-clicking the system and clicking **Request Access**. By providing a valid user name and password, you can access the system.

You can right-click a managed system in the Group Contents pane to see what actions you can perform on the system, for example, view system-specific information.

You also can right-click any blank space in the Group Contents pane to create new managed systems and devices manually, find and view systems, change the view and sort managed systems by status or by ascending or descending name order, make associations, and discover managed systems.

Along the top of the IBM Director Console interface is a toolbar containing five icons.

Figure 2. IBM Director Console toolbar

From left to right, the icons represent:

- Discover All Managed Systems (see the *IBM Director 4.0 for BladeCenter products Installation and Configuration Guide*)
- Message Browser (see “Message Browser” on page 12)
- User Administration (see “User Administration” on page 13)
- Event Action Plan Builder (see “Event action plans” on page 21)
- Scheduler (see “Scheduler” on page 51)

Along the bottom of the IBM Director Console interface is the marquee area and hardware-status alert display. The ticker-tape messages scroll across the marquee area. The hardware-status alert display is located in the bottom-right corner of the interface.

Groups

Groups are logical sets of managed systems. An example might be a group that contains managed systems that have Linux installed. When you start the IBM Director Console for the first time, the default groups are displayed. This includes the All Systems and Devices group, which contains all discovered managed systems and devices.

When you select a group, the systems that are members of that group are displayed in the Group Contents pane.

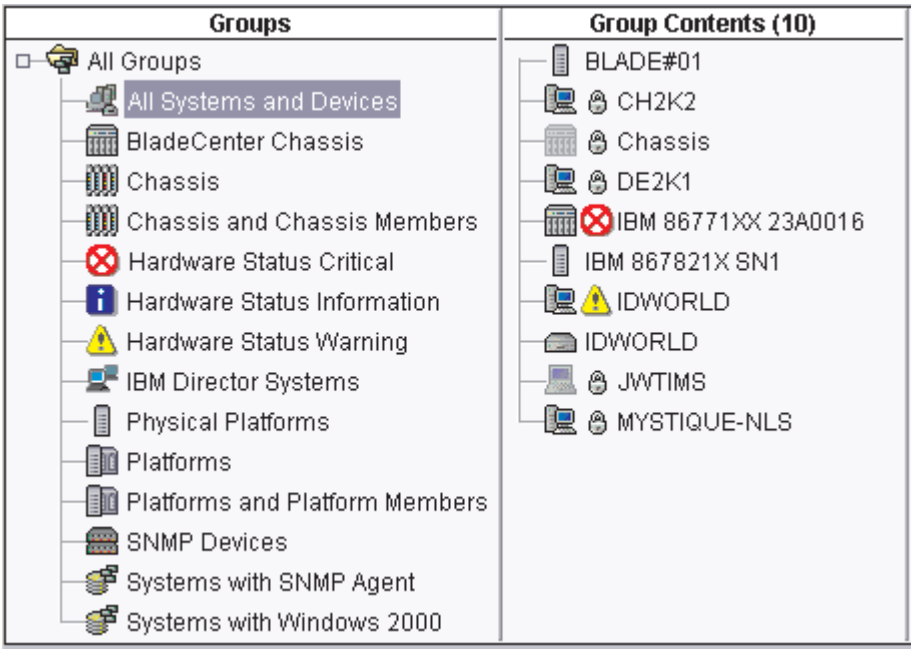

Figure 3. A selected group listed in the Group Contents pane

You can select one group at a time. To perform tasks simultaneously on multiple groups, create a new group and include all the desired managed systems from the multiple groups, or combine several separate groups into one group.

There are two types of groups in IBM Director: dynamic groups and static groups. To create a new group, see “Creating a dynamic group” on page 8 or “Creating a static group” on page 10.

Dynamic groups

Dynamic groups are based on specified inventory or task criteria. You can create a dynamic group by specifying criteria that the attributes and properties of the managed systems must match. IBM Director automatically adds or removes managed systems to or from the group when their attributes and properties change to match the group criteria.

Creating a dynamic group

Complete the following steps to create a dynamic group:

1. Right-click the Groups pane and click **New Dynamic**. The Dynamic Group Editor window opens.

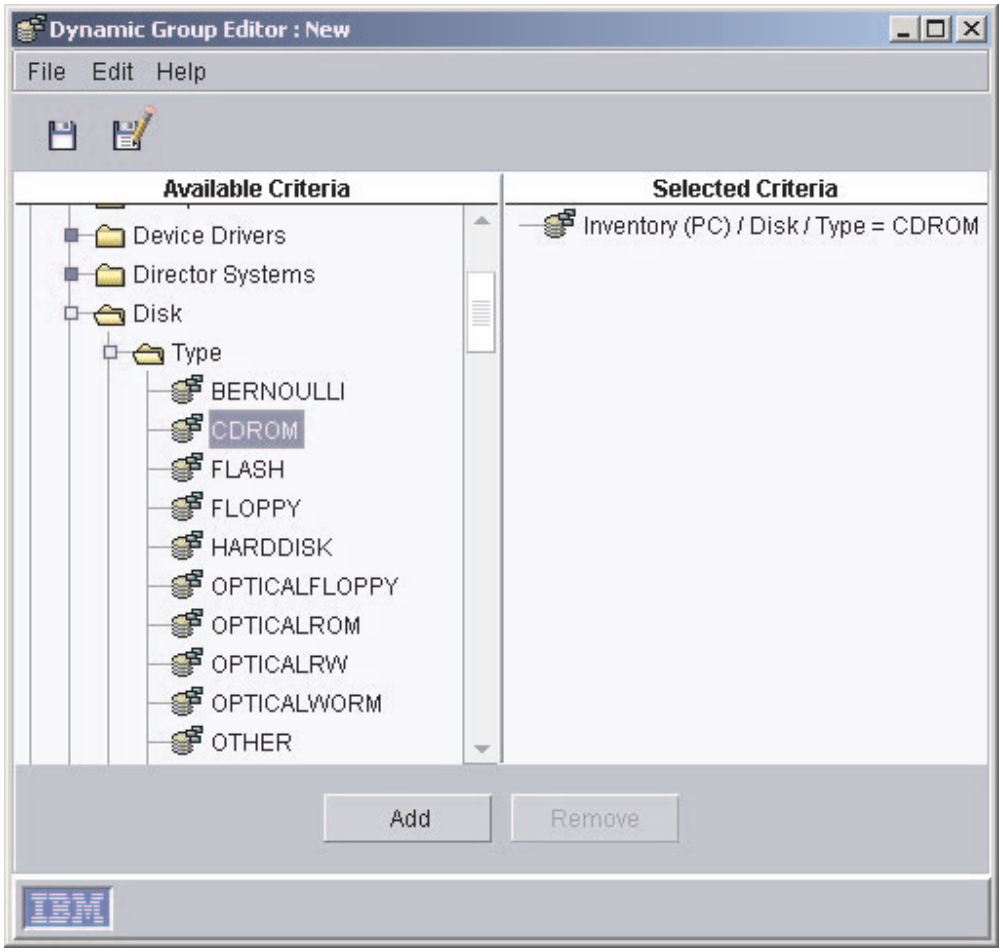

Figure 4. Dynamic Group Editor window

2. In the Available Criteria pane, expand the tree that has the criterion you want to use to define the group. Click a criterion and click **Add**. The criterion is displayed in the Selected Criteria pane.

   The default operator is equal to (=). You can change the operator for any criterion by right-clicking the criterion and selecting another operator.

   Repeat this step to add more criteria. When you add criteria, the Choose Add Operation window opens. Click **All True** or **Any True** and click **OK**.

3. Click **File** → **Save As** to save the new dynamic group. The Save As window opens.

4. Type a descriptive name for the group. This is the group name that will be listed in the Groups pane. Click **OK**.

The group is displayed under **All Groups** in the Groups pane.

Using the Task Based Group Editor

Use the Task Based Group Editor to create a dynamic group based on the types of tasks for which the group of managed systems is enabled. This type of dynamic group saves you time because you can drag a task directly onto all managed systems that support that task.

Complete the following steps to create a task-based group:

1. Right-click the Groups pane and click **New Task Based**. The Task Based Group Editor window opens.

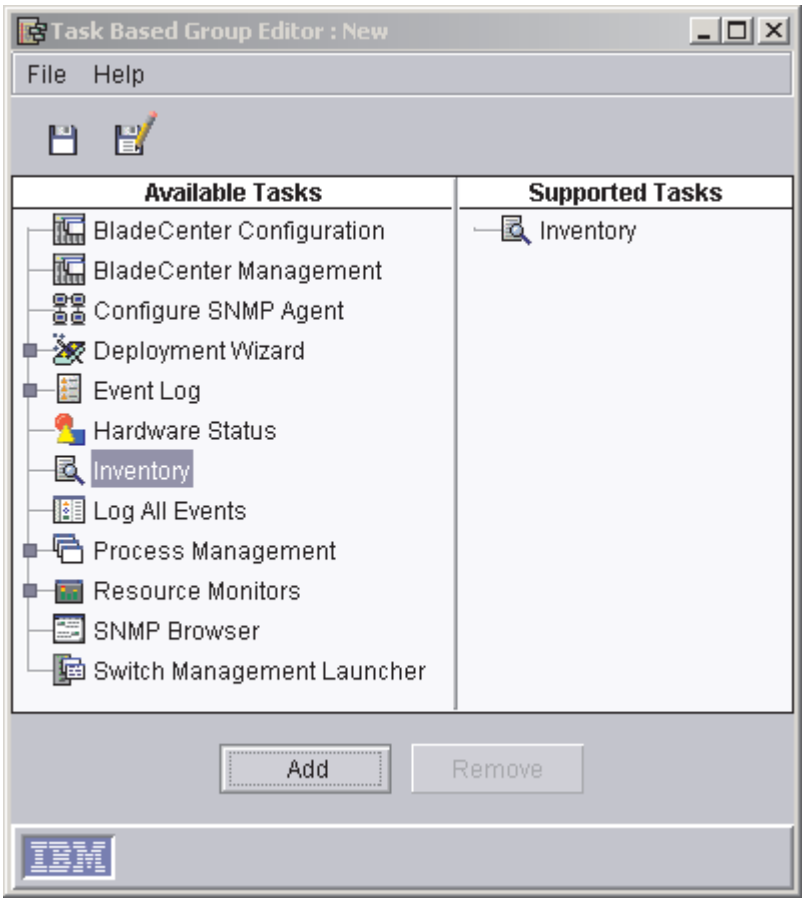

Figure 5. Task Based Group Editor window

2. In the Available Tasks pane, click a task you want to perform using this group; then, click **Add**. The task is displayed in the Supported Tasks pane.
3. When you are finished adding tasks, click **File** → **Save As**. The Save As window opens.
4. Type a descriptive name for the group. Click **OK**. The group is added to the Groups pane.
5. Click **File** → **Close Group Editor** to close the Task Based Group Editor window.

Static groups

You can specify a set of managed systems to create a static group. IBM Director Server does not automatically update the contents of a static group.

Creating a static group

Complete the following steps to create a static group:

1. Right-click the Groups pane and click **New Static**. The Groups pane splits and the Static Group Editor opens in the bottom half of the Groups pane.

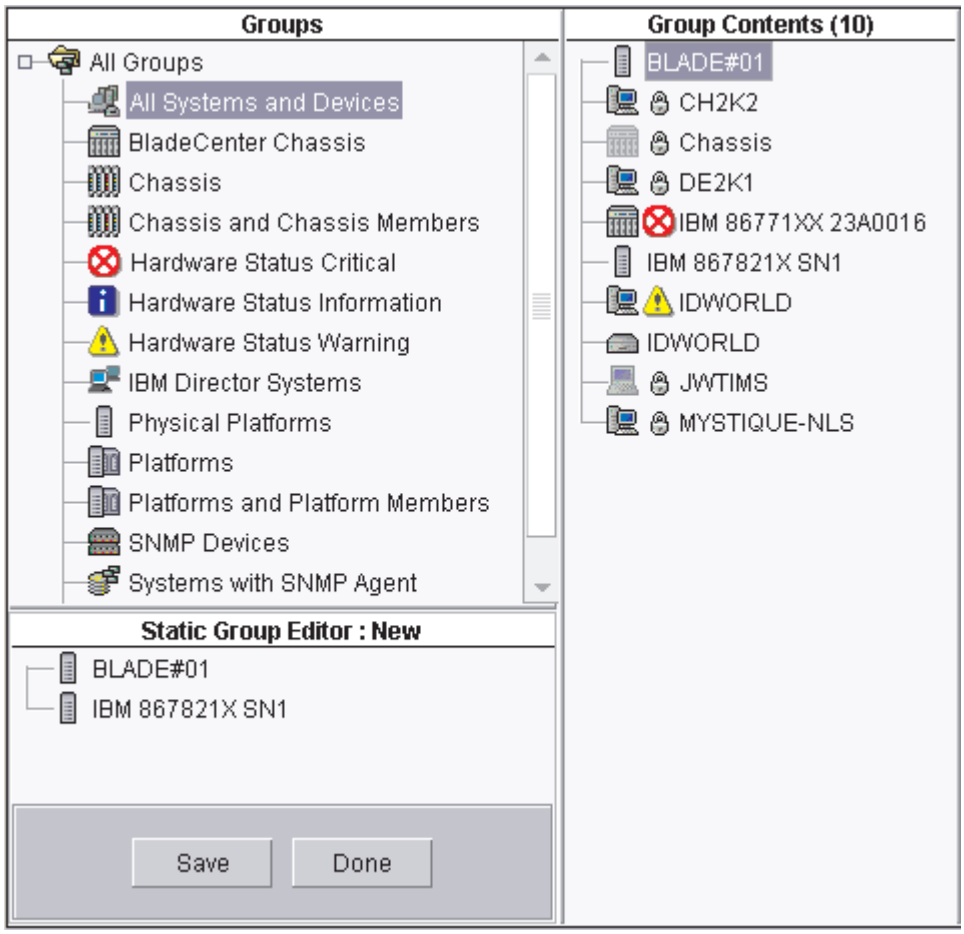

Figure 6. Static Group Editor window

2. Drag the managed systems you want to add to the new static group onto the Static Group Editor window. The selected managed systems are added to the group.
3. When you are finished adding managed systems, click **Save**. The Save As window opens.
4. Type a descriptive name for the group. Click **OK**. The group is displayed under **All Groups** in the Groups pane.
5. Click **Done** to close the Static Group Editor.

Using the Category Editor

Use the Category Editor to organize large numbers of groups by creating group categories. Group categories created with the Group Category Editor are static, although the groups included in a category can be dynamic or static.

Complete the following steps to create a group category:

1. Right-click the Groups pane and click **New Group Category**. The Groups pane splits, and the Category Editor opens in the bottom half of the Groups pane.

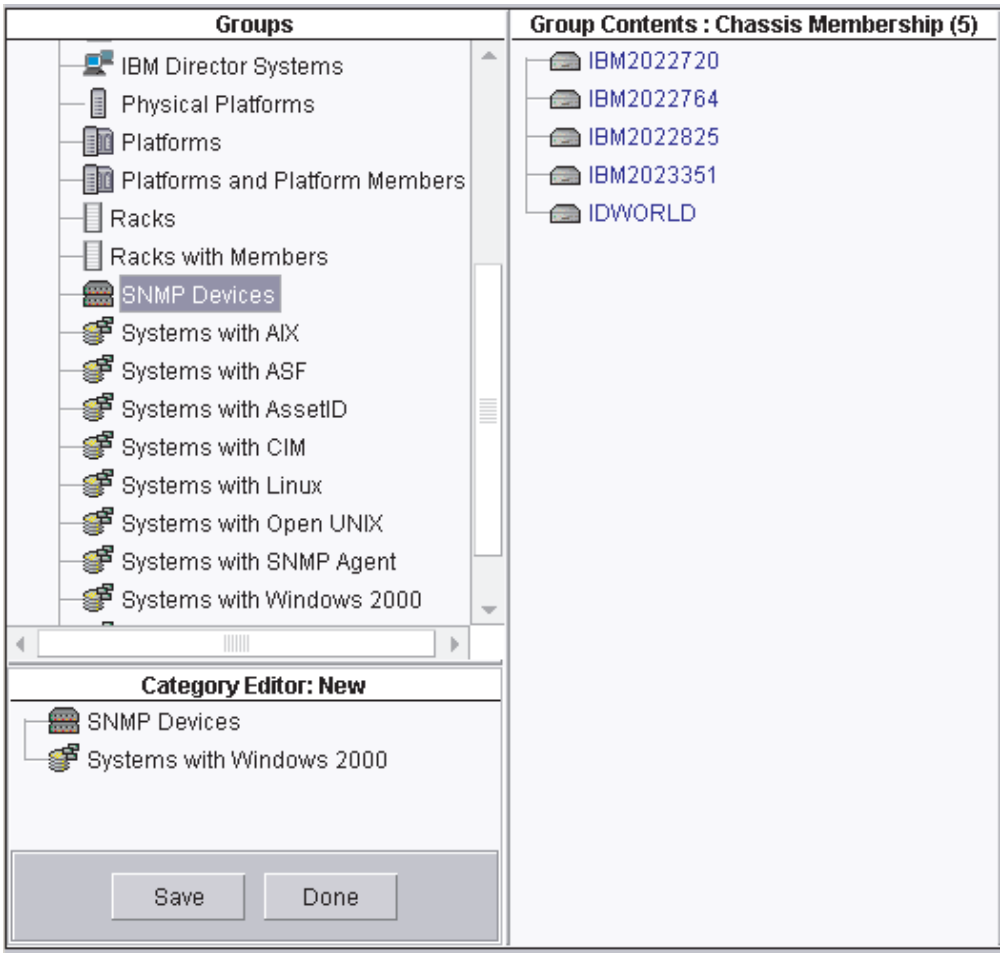

Figure 7. Category Editor window

2. Drag the groups you want to add to the new group category onto the Category Editor window. The selected groups are added to the category.
3. Click **Save** to name the new group category. The Save As window opens.
4. Type a descriptive name for the group category. Click **OK**. The group is displayed in the Groups pane.
5. Click **Done** to close the Category Editor.

Group import and export

You can export groups to archive or back up the contents of a group or import a previously exported group to distribute a selected set of groups to a remote location. You can import and export only dynamic groups, which include task-based groups.

Exporting a group

Complete the following steps to export a group:

1. Right-click the Groups pane and click **Export Group**. The Group Export window opens.

2. Click the group you want to export from the groups available for export.
3. Type a file name in the **Export Destination File** field, or click **Browse** to locate a file name.
4. Click **Export**. The group is exported to the file you specified.

Importing a group

Complete the following steps to import a group:

1. Right-click the Groups pane and click **Import Group**. The Group Import window opens.
2. Select the group you want to import by navigating the tree structure or typing the group name in the **File Name** field.
3. Click **OK**. The Group Import window opens.

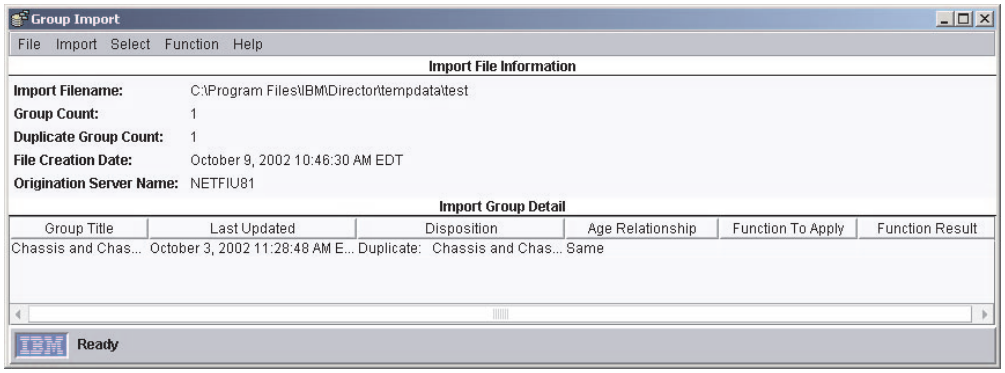

Figure 8. Group Import window

4. Click one or more groups in the Import Group Detail pane.
5. Click **Function** and click the applicable action.
6. Click **Import** → **Import Selected Groups**. The group or groups are added, updated, or skipped.

Message Browser

You can use the Message Browser to view event alerts sent to IBM Director Console. The Message Browser is displayed automatically whenever an event notification alert is sent to the management console. You can opt to be alerted in this manner when an event occurs by configuring an event action plan with the Send an Event Message to a Console User event action. (See “Event action plans” on page 21 for more information on event actions and event action plans.)

The Message Browser displays all alerts, including management console ticker-tape alerts. However, the Message Browser does not display any ticker-tape messages. (A ticker-tape message can display, for example, resource-monitor data. See “Viewing resource-monitor data on the ticker tape” on page 50 for more information.)

You can start the Message Browser to view all active messages received and clear any previous messages. To start the Message Browser, click **Tasks** → **Message Browser**. The Message Browser window opens.

User Administration

You can edit user profiles, including user properties and privileges, group access, and task access, and change the defaults for new IBM Director user IDs using the User Administration task. For more information about user administration tasks, see the *IBM Director 4.0 for BladeCenter products Installation and Configuration Guide*.

Note: If you want to authorize a new IBM Director Console user, you must use the tools provided by the operating system to add a new user ID to one of the operating-system groups.

Complete the following steps to edit an existing user profile:

1. In IBM Director Console, click **Options** → **User Administration**. The User Administration window opens.
2. Click the row of the user.
3. Click **User** → **Edit**. The User Editor window opens.
4. Make any changes. Click **OK** when you are finished making all changes in the window.

You can change the defaults for new IBM Director user IDs. You can specify the default information for the full name, description, privileges, group access limits, and task access limits for all new user IDs.

Complete the following steps to change the defaults for new IBM Director user IDs:

1. In IBM Director Console, click **Options** → **User Administration**. The User Administration window opens.
2. Click **User** → **User defaults**. The User Defaults Editor window opens.
3. Make any changes. Click **OK** to save the changes.

Associations

You can use associations to display the groups in the Group Contents pane in a logical ordering. For example, if you select the object type association, the managed systems and devices are grouped based on whether they are IBM Director managed systems, SNMP devices, or chassis; also, racks and platforms are displayed as groups in the Group Contents pane.

To display group contents according to an association, click **Associations**; then, click an association from the top portion of the menu. By default, **None** is selected. For those items in the top portion of the menu, you can select one association at a time.

For example, to view all the blade servers in a BladeCenter chassis, click **Associations** → **Chassis Membership**. All BladeCenter chassis containing blade servers are displayed in a tree structure, so you can view the individual blade servers in each BladeCenter chassis.

You also can display additional information about the managed systems displayed in the Group Contents pane by selecting options from the bottom half of the **Associations** menu. For example, you can view the managed systems and devices that have event action plans applied to them. If a managed system or device has an event action plan applied to it, the managed system or device is displayed as a

tree structure that you can expand to view which event action plans, if any, have been applied to it. You can select more than one of these options at a time. The following list includes all available options:

Software Packages
Shows which packages, if any, have been delivered to each managed system using the Software Distribution task.

Jobs Shows all tasks, if any, that are scheduled to be run against each managed system.

Activations
Shows all tasks, if any, that have been run against each managed system.

Resource Monitors
Shows the resource monitors, if any, that have been applied to each managed system.

Event Action Plans
Shows the event action plans, if any, that have been applied to each managed system.

Chapter 3. IBM Director tasks

This chapter provides information about IBM Director Console tasks that you can use with BladeCenter units. BladeCenter units consist of a chassis, one or more switches, and one or more blade servers (up to 14 total).

The chassis represents the physical enclosure that contains the blade servers. The chassis has a management module that contains a service processor. IBM Director discovers the chassis and gathers information from the chassis by way of the management module. You cannot install IBM Director Agent on the chassis.

The switch is an SNMP device and IBM Director considers the switch a managed device. When viewing the switch in IBM Director, it might be labeled remote monitor (RMON) or SNMP.

IBM Director can gather some information from a blade server *before* IBM Director Agent is installed on the blade server. The information is gathered from the blade server by way of the chassis management module. In IBM Director Console, the blade server is represented by a physical platform. However, after you install IBM Director Agent on the blade server, it is a managed system and the features and functions that you can use on the blade server are comparable to any managed system.

IBM Director Console tasks that you can use on your BladeCenter unit can vary, depending on the features and options you have installed. See Table 1 for a list of IBM Director tasks and whether you can use a task on the chassis, switch, or a blade server (with or without IBM Director Agent installed). Unless otherwise noted in this chapter, a task behaves the same for blade servers as any managed system.

Table 1. IBM Director tasks and the BladeCenter components you can use them on

Task	Chassis	Switch	Blade server	
			Without IBM Director Agent installed	With IBM Director Agent installed
BladeCenter configuration	X			
BladeCenter management	X			
BladeCenter deployment wizard	X			
BladeCenter switch management launcher		X		
Blue indicator light	X		X	X
Configure SNMP agent				X
Event action plans	X	X	X	X
Hardware Status	X		X	X
Inventory	X	X	X	X
Power management			X	X
Process Management				X
Resource Monitors		X		X
SNMP devices (browser)		X		
Software distribution				X

BladeCenter

You can use the BladeCenter task to manage your BladeCenter units.

Within the BladeCenter task, there are four subtasks:

- BladeCenter Configuration
- BladeCenter Management
- Deployment Wizard
- Switch Management Launcher

You can use the first two subtasks for BladeCenter unit configuration and management, and the Switch Management Launcher subtask for switches. The Deployment Wizard subtask is discussed in the *IBM Director 4.0 for BladeCenter products Installation and Configuration Guide*.

Starting the BladeCenter Configuration or BladeCenter Management subtask

In the IBM Director Console Tasks pane, expand the **BladeCenter** task. Drag the applicable subtask onto a BladeCenter unit. The Management Processor Assistant window opens.

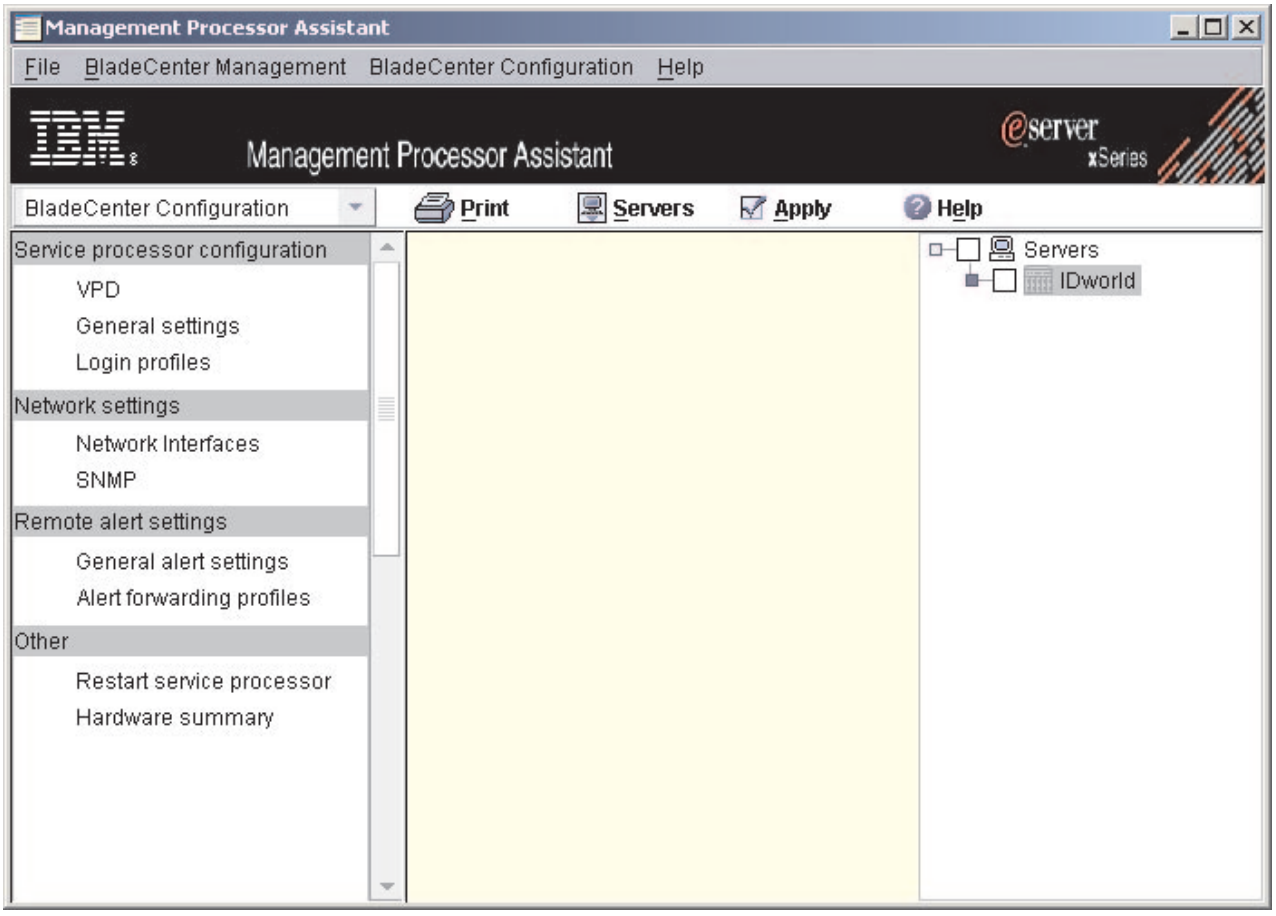

Figure 9. Management Processor Assistant window when activating the BladeCenter Configuration subtask

The left pane contains menu options for the subtask you selected. To change which menu options for each of the two subtasks are displayed in the left pane, click the list in the upper left, above the left pane.

To select which servers you want to work with, click **Servers** at the top of the right pane. The right pane is subdivided, the far-right subpane displaying all servers that you targeted when starting the task.

To save any changes, click **Apply**.

Viewing environmental data

You can view environmental data such as temperature, voltage, and fan speeds.

To view temperature data, click **BladeCenter Management** → **Temperatures**, and click the applicable option. The data is displayed in the middle pane.

To view voltage data, click **BladeCenter Management** → **Voltages**, and click the applicable option. The data is displayed in the middle pane.

To view fan speed, click **BladeCenter Management** → **Status and VPD** → **Fan speed**. The data is displayed in the middle pane.

Viewing component data

You can view component data, which includes component type, slot, field-replaceable unit (FRU) number, part number, serial number, and manufacturer ID.

To view component data, click **BladeCenter Management** → **Status and VPD** → **Component VPD**. The data is displayed in the middle pane.

Viewing service processor data

You can view service processor data, which includes build information, such as firmware type, and file name, and microcontroller information.

To view service processor data, click **BladeCenter Configuration** → **VPD**. The data is displayed in the middle pane.

Viewing the event log

The event log is a list of all events that have been received by the management module. It includes information about the event, for example, the event severity. To view the event log stored on the management module, click **BladeCenter Management** → **Status and VPD** → **Event log**.

Viewing hardware status summary

The hardware status summary includes such information as the chassis and blade servers, server type, model, and serial number, and Universal Unique ID (UUID).

To view the hardware status summary, click **BladeCenter Management** → **Status and VPD** → **Hardware summary**. The data is displayed in the middle pane.

Viewing power supply status

To view the power supply status, click **BladeCenter Management** → **Status and VPD** → **Fuel Gauge**. The data is displayed in the middle pane.

Viewing Light Path Diagnostics

You can view the Light Path Diagnostics™ for a BladeCenter unit. Complete the following steps to view the LEDs:

1. Click **BladeCenter Management** → **Status and VPD** → **Light Path Diagnostics**.
2. Click the applicable tab to view the information you want.

Viewing the blue indicator light

You can use the blue indicator light to locate a blade server that has a problem. Complete the following steps to change the LED status on a blade server:

1. Click **BladeCenter Management** → **Status and VPD** → **Blue indicator light**. The Blue indicator light information is displayed in the middle pane.
2. In the table, click the row for the server you want to work with; then, click the State cell and select a choice from the list. The options are On, Off, or Flashing.
3. Click **Apply**.

Powering servers on and off

You can power a server on or off remotely. Complete the following steps to power off a server:

1. Click **BladeCenter Management** → **Power control** → **Power off server**.
2. Select the applicable check box (**Power off immediately** or **Power off with shutdown**).
3. Click **Apply**.

Complete the following steps to power on a server:

1. Click **BladeCenter Management** → **Power control** → **Power on server**.
2. To power the server on immediately, select the **Power on immediately** check box.

   To power the server on in a specified number of seconds, double-click the **Power on in n seconds** cell and type the number of seconds.

   To power on the server on a specified day and time, click **Power on date** cell and type a date, and click the **Power on time** cell and type a time.
3. Click **Apply**.

Restarting the managed system

Complete the following steps to restart a managed system:

1. Click **BladeCenter Management** → **Power control** → **Restart server**.
2. Select the applicable check box (**Restart immediately** or **Restart with shutdown**).
3. Click **Apply**.

Viewing and changing KVM policy

You can enable or disable the keyboard, video, and mouse (KVM) select button. Complete the following steps to enable or disable this button:

1. Click **BladeCenter Management** → **Policy** → **KVM**.
2. Select the applicable **Assigned** cell check box to enable the power control button for that bay, or clear the check box to disable the power control button for that bay.
3. Click **Apply**.

Viewing and changing KVM assignment

You can view which blade server bay owns the KVM and change this assignment. Complete the following steps to view and change KVM ownership:

1. Click **BladeCenter Management** → **Shared resources** → **KVM assignment**.

2. In the **Set new owner** cell, click the blade server you want to own the KVM from the list. If you do not want the KVM media assigned to any blade server, in the **Park** cell, select the check box.
3. Click **Apply**.

Viewing and changing USB policy

You can enable or disable the USB select button for each blade server bay. Complete the following steps to enable or disable the select button:

1. Click **BladeCenter Management** → **Policy** → **USB**.
2. Select the applicable **Assigned** cell check box to enable the select button for that blade server bay, or clear the check box to disable the select button for that bay.
3. Click **Apply**.

Viewing and changing USB media assignment

You can view which blade server bay controls the USB media and change the assignment. Complete the following steps to view and change the USB media assignment:

1. Click **BladeCenter Management** → **Shared resources** → **USB media assignment**.
2. In the **Set new owner** cell, click the blade server you want to own the USB media from the list. If you do not want the USB media assigned to any blade server, in the **Park** cell, select the check box.
3. Click **Apply**.

Viewing and changing local power control

You can enable or disable the local power control button for each blade server bay. Complete the following steps to enable or disable this button:

1. Click **BladeCenter Management** → **Policy** → **Power control**.
2. Select the applicable **Assigned** cell check box to enable the power control button for that bay, or clear the check box to disable the power control button for that bay.
3. Click **Apply**.

Viewing and changing blade server boot options

You can view and change the start (boot) sequence for blade servers. Up to four devices can be defined as boot devices. The devices are ordered based on precedence, so the first device in the order will attempt to start the blade server. If the first device fails, then the second device is tried, and so on, until all devices specified have been tried.

Complete the following steps to view and change blade server start options:

1. Click **BladeCenter Management** → **Shared resources** → **Boot options**.
2. In the **Boot Order** cells, click the list to specify a device.
3. Click **Apply**.

Switch IP configuration

You can view and change current IP settings, such as the host IP address, subnet mask, gateway IP address, and configuration method, for each of the switches on the chassis.

To view these settings, click **BladeCenter Management** → **Switches** → **IP configuration**.

Switch management

You can view and change settings, such as resetting the switch to default settings, whether the switch is powered on, and whether memory diagnostics are enabled, for each of the switches on the chassis.

To view and change settings, click **BladeCenter Management** → **Switches** → **Management**.

Viewing switch vital product data

You can view the vital product data, such as the build level of the switch hardware, the manufacture date, and the FRU number, for each of the switches on the chassis. To view this information, click **BladeCenter Management** → **Switches** → **VPD**.

Configuring an alert-forwarding profile

Alert forwarding can ensure that alerts are sent, even if a managed system experiences a catastrophic failure, such as an operating-system failure.

Complete the following steps to configure an alert-forwarding profile:

1. Click **BladeCenter Configuration** → **Remote alert settings** → **Alert forwarding profiles**.
2. To add a new alert-forwarding profile, click **Add an entry**.

   To change an alert-forwarding profile, click the alert-forwarding profile you want to change and make changes.

   To delete an alert forwarding strategy, click the alert-forwarding profile you want to delete, and click **Unused** in the Enable list.
3. Click **Apply**.

Configuring network settings for the service processor

Complete the following steps to configure network settings for the service processor:

1. Click **BladeCenter Configuration** → **Network settings** → **Network interfaces**.
2. Make any configuration changes. Click the tabs to view each page.
3. Click **Apply**.

Restarting a service processor

You must restart the service processor on the chassis to have your network settings take effect.

Complete the following steps to restart a service processor:

1. Click **BladeCenter Configuration** → **Other** → **Restart service processor**.
2. Select the **Restart now** check box.
3. Click **Apply**.

Switch Management Launcher subtask

The Switch Management Launcher subtask opens a Web browser or telnet session to launch a third-party application.

To start the Switch Management Launcher subtask, expand the **BladeCenter** task; then, drag the **Switch Management Launcher** subtask onto a switch. You are prompted to type the user name and password.

Event action plans

By creating event action plans and applying them to specific managed systems, you can be alerted by e-mail or pager, for example, when a specified threshold is reached or a specified event is generated. 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 resource-monitor events and process-monitor events to build an event action plan. See “Resource Monitors” on page 43 and “Process Management” on page 37 for details.

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 4, “Event management” on page 73.

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 *IBM Director 4.0 for BladeCenter products 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.

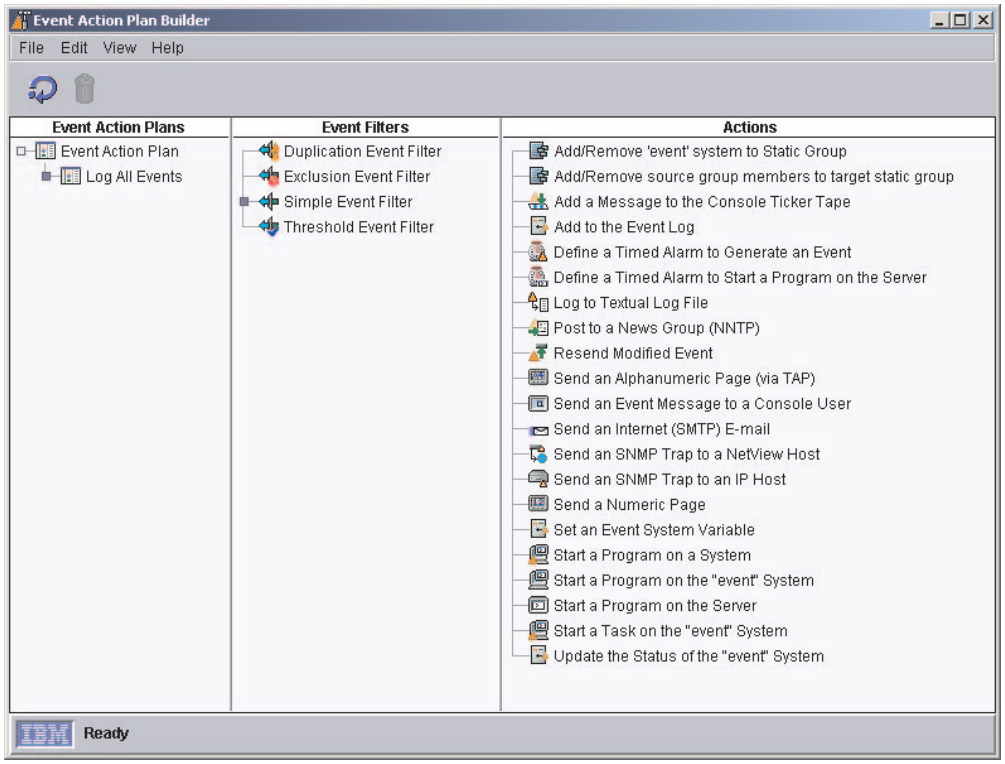

Figure 10. Event Action Plan Builder window

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 hardware event category event filters, such as Hardware Predictive Failure Analysis® Events. Using one of these pre-configured event filters ensures that the correct event type 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 hardware event category event filters, such as Hardware Predictive Failure Analysis Events. Using one of these pre-configured event filters ensures that the correct event type 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 Event Filter Builder window opens.

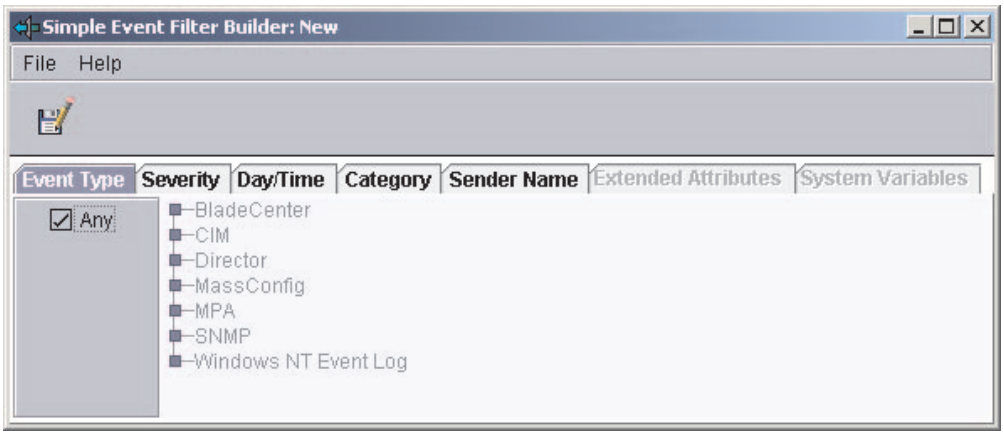

Figure 11. Simple Event Filter Builder window

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 task-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 IBM Director Server. System variables is enabled only if one or more system variables exist. See “Viewing and changing system variables” on page 25 for more information.

By default, the **Any** check box is selected for all filtering categories, indicating that all 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 22 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 12 is for ticker-tape alerts.

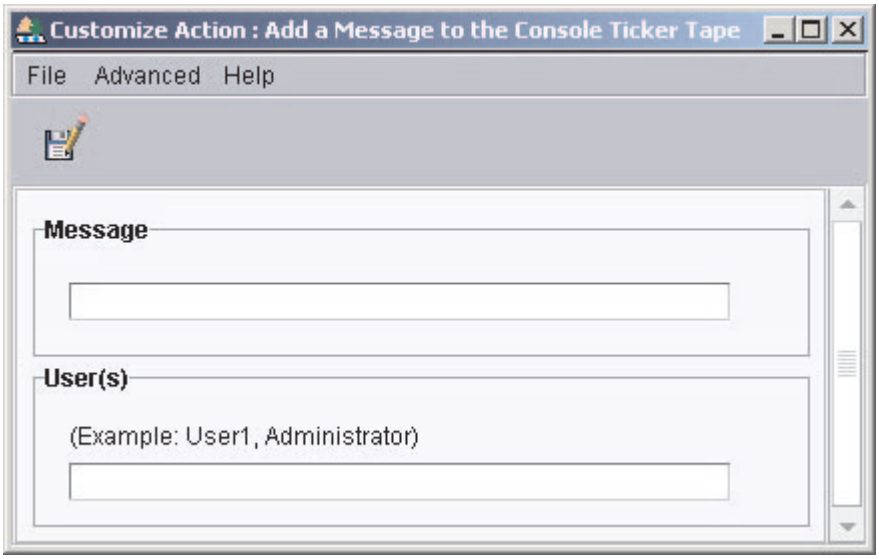

Figure 12. Customize Action window for ticker-tape alert

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 84 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. 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 24 through step 13 on page 24.
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 22. 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.
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.

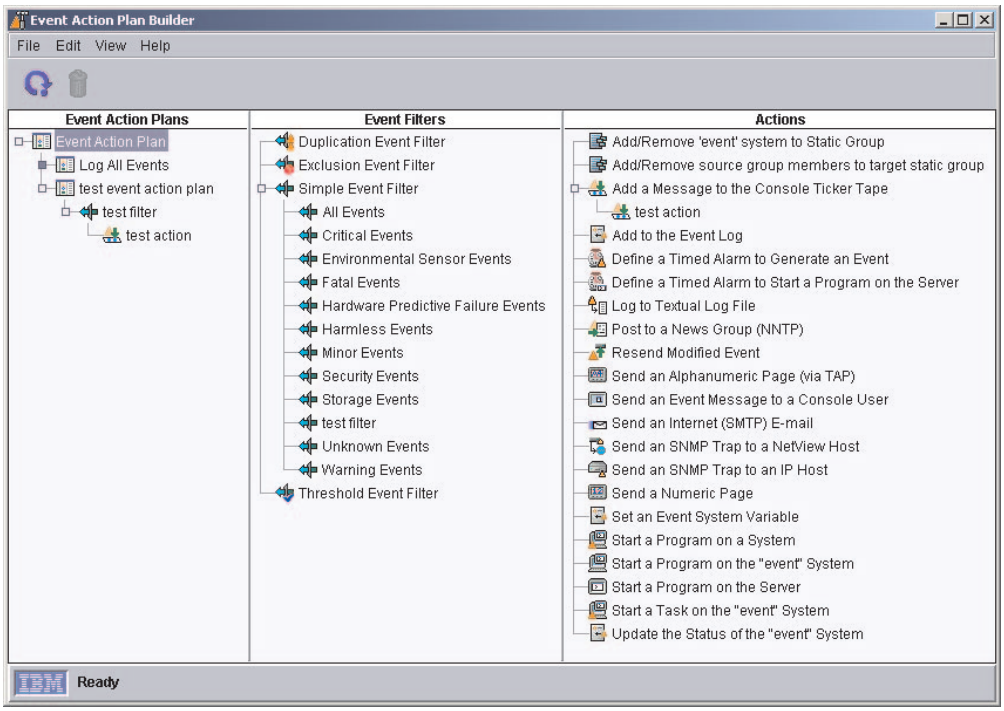

Figure 13. Example of an event action plan with an event filter and event action assigned to it

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 and 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, and `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 79 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 and view the specific event action plans that are assigned 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 every managed system in a group and events received by any managed system in the group, or just the events received by every managed system 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.

Viewing event details in the event log

Using the event log, you can view details on all events or subsets of events that have been received and logged by IBM Director Server.

You can view all events, or by managed system or filter criteria.

To view all events in the event log, in the IBM Director Console Tasks pane, double-click the **Event Log** task. The Event Log window opens.

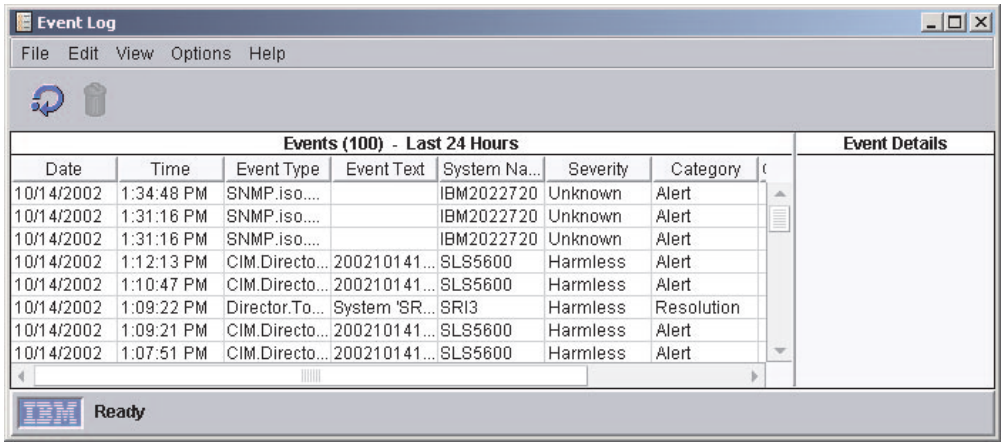

Figure 14. Event Log showing all events for all managed systems

To view the events for a specific managed system or group, drag the **Event Log** task onto the managed system or group. The Event Log window for that managed system or group opens.

To view events by filter criteria, in the IBM Director Console Tasks pane, expand the **Event Log** task tree; then, double-click the filter for which you want to see all the events. The Event Log window opens, and only those events are displayed.

Exporting the event log

You can export an event log to an HTML, XML, or comma-separated value (CSV) file.

To export an event log, in the Event Log window, click **File** → **Export**, and click the format to which you want to export the event log.

Hardware Status

You can use the Hardware Status task to view managed system and device hardware status from the management console. Hardware status 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. Hardware status also adds the system or device in the applicable hardware status group whenever a managed system or device generates a hardware event.

Three hardware status groups are displayed in the Groups pane:

- Hardware Status Critical
- Hardware Status Information
- Hardware Status Warning

When you click a hardware status group, the managed systems or devices that have generated that severity of a hardware event are displayed in the Group Contents pane. An icon is displayed beside the managed system or device in the Group Contents pane. See Figure 15 on page 29 for an example.

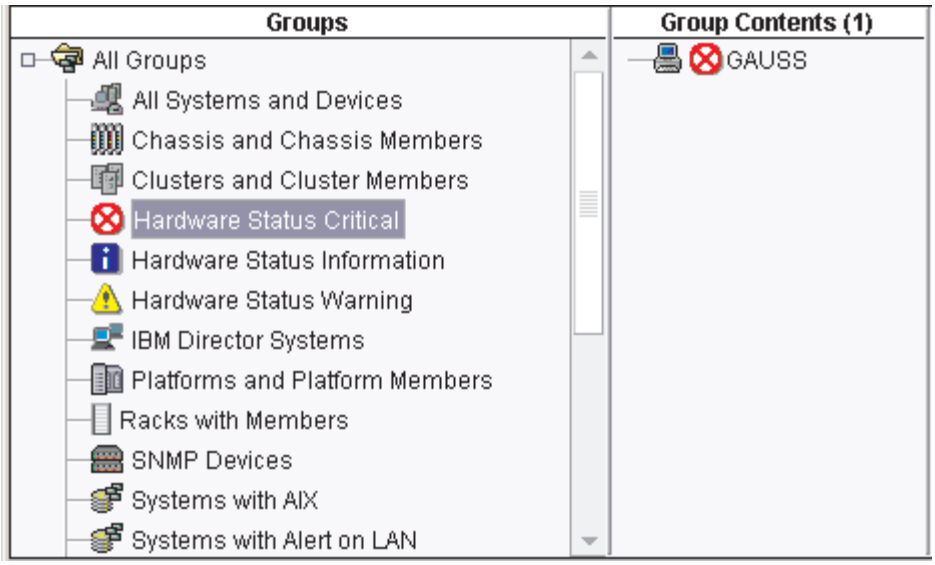

Figure 15. IBM Director Console displaying hardware status groups

The same icon is displayed in the bottom-right portion of the IBM Director Console interface, below the ticker tape, along with the number of managed systems and devices that are included in that hardware status group. If a hardware status group does not contain any managed systems or devices, its icon is unavailable.

Figure 16. Hardware status icons located in the bottom-right portion of IBM Director Console

You also can drag a managed system or device onto the **Hardware Status** task in the IBM Director Console Tasks pane.

You can view the event details for each hardware status group that contains a managed system or device by clicking the applicable icon in the bottom-right portion of IBM Director Console. The Hardware Status window opens.

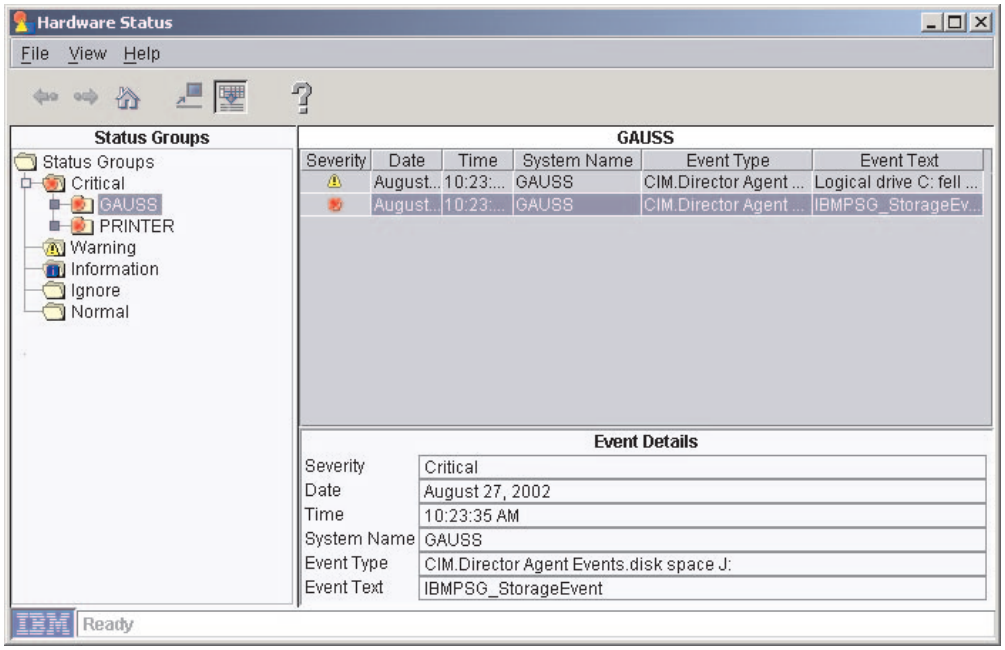

Figure 17. Hardware status window showing all hardware status events

You also can view the event details for an individual managed system or device by double-clicking on the hardware status icon beside the system or device in the Group Contents pane. See Figure 18.

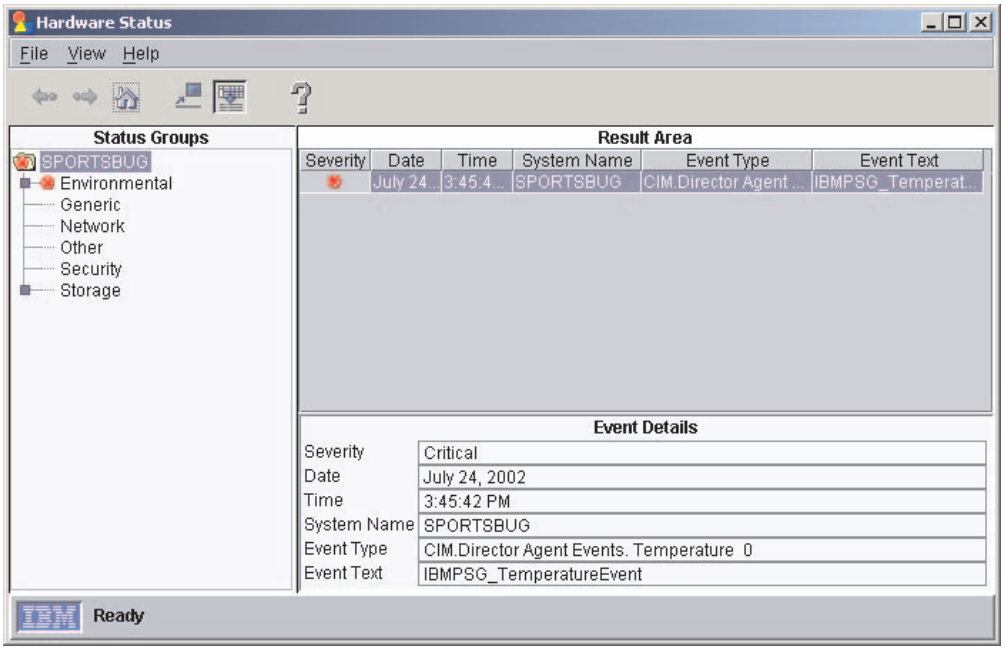

Figure 18. Hardware Status window showing events for a single managed system

To set a managed system or device status to normal and ignore all future hardware events generated by the managed system or device, in the Status Groups pane, right-click the managed system or device and click **Ignore Events** to ignore all

hardware events on the managed system or device. You also can ignore a specified type or types of hardware events by right-clicking an event type and clicking **Ignore Events**.

To set a managed system or device status to normal but allow future hardware events to affect the system status, right-click the managed system or device and click **Clear all Events**. You also can delete specified types of hardware events by right-clicking an event type and clicking **Clear all Events**.

Inventory

You can use inventory to collect data about the hardware and software currently installed on the managed systems in your network. IBM Director collects inventory data when a managed system is discovered initially and during regular intervals, or you can opt to not collect inventory upon initial discovery and instead schedule an inventory collection at a more convenient time using the Scheduler task (see "Scheduler" on page 51 for more information on how to schedule tasks). The default interval for refreshing the database is every 7 days. You can change the refresh interval and other inventory collection parameters using the Inventory Collection Preferences page in the IBM Director Console Server Preferences window. You also can collect inventory data on a managed system or group immediately, or schedule an inventory collection using the Scheduler task.

You can query the inventory database to display details on particular properties of a managed system, such as disk space remaining. You can use a standard query provided, or create your own custom query.

You can use the inventory software dictionary to track the software installed on your managed systems. The software dictionary file contains predefined software profiles that recognize most standard software packages after they are installed. When you install software applications on servers, computers, or devices, the inventory query browser displays the new software after the next inventory collection. 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. Typically, this includes software developed internally in your organization or a new version of software released after this version of IBM Director.

Viewing inventory data

You can use any query from the Available Queries pane in the Inventory Query Browser to view inventory data. The Standard folder contains a number of predefined queries, or you can create your own query, which is then stored in the Custom folder.

Using a predefined query

Complete the following steps to use a predefined query to view inventory data:

1. In the IBM Director Console Tasks pane, drag the **Inventory** task onto a managed system or group. The Inventory Query Browser window opens.

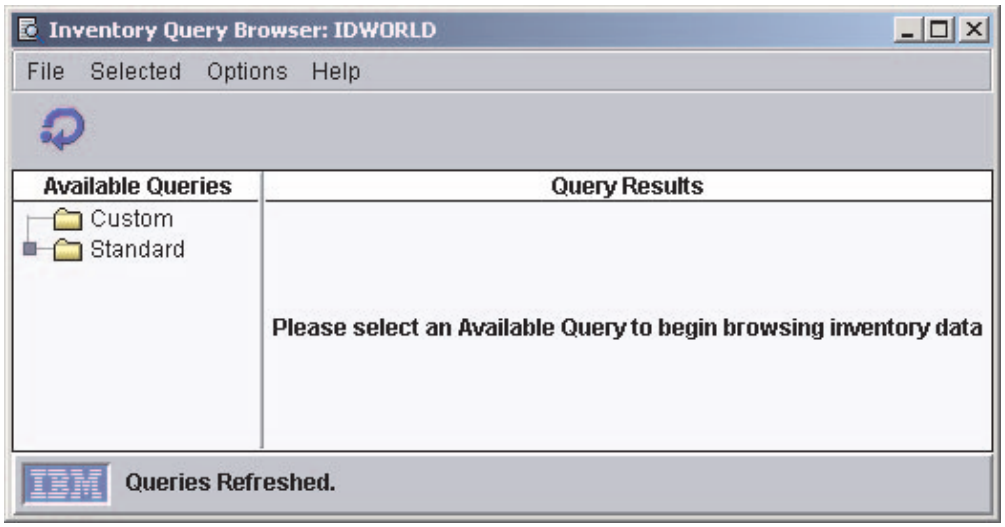

Figure 19. Inventory Query Browser window

The Inventory Query Browser has two panes: Available Queries and Query Results. The Available Queries pane automatically displays predefined queries that are included in IBM Director and any queries that you have created previously. In the Query Results pane, you can view the details of the query for each selected managed system.

2. In the Available Queries pane, expand the Standard folder. Click a query. The results for each managed system are displayed in a table in the Query Results pane. If no information is currently available on that query, a message is displayed.

You can schedule an inventory collection to occur at a specific date and time or regular interval, using the Scheduler task. See “Scheduler” on page 51 for more information about using the Scheduler task. Also, you can configure inventory collection parameters using the Inventory Collection Preferences page in the IBM Director Console Server Preferences window.

Creating and using your own inventory query

In addition to the default queries, you can create your own custom inventory query.

Complete the following steps to create and use a custom query to view inventory data:

1. In IBM Director Console, click **Tasks** → **Build Custom Query**. The Inventory Query Builder window opens.

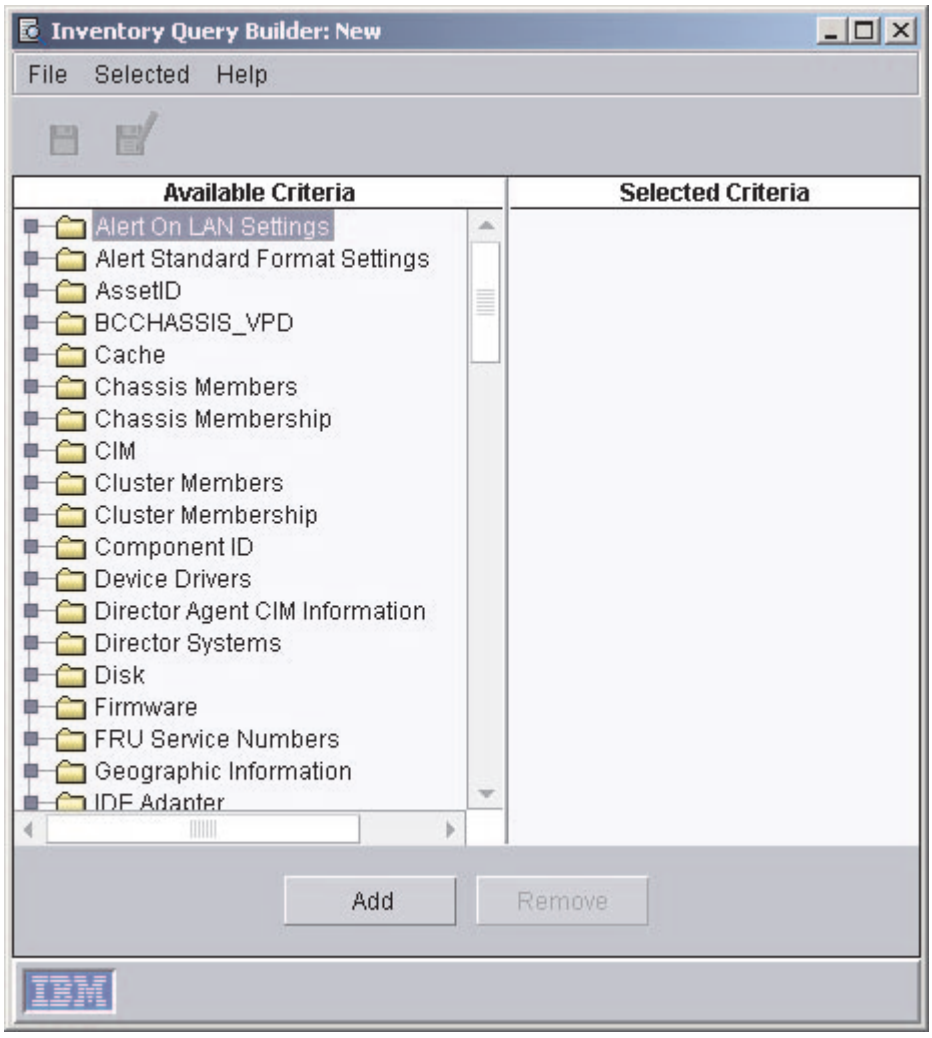

Figure 20. Inventory Query Builder window

2. In the Available Criteria pane, drag the data items you want to add to the query onto the Selected Criteria pane. The order of the criteria in the Selected Criteria pane is the order that the criteria will be displayed in the Inventory Query Browser window.
3. Click **File** → **Save As** to save the query. The new query is displayed under the Custom folder in the Available Queries pane of the Inventory Query Browser window.
4. In the Available Queries pane, expand the Custom folder. Click a query. The results for each managed system are displayed in a table in the Query Results pane. If no information is currently available on that query, a message is displayed.

Editing a custom query

You can modify a query you have already created.

Complete the following steps to edit a custom query:

1. In the IBM Director Console Tasks pane, double-click the **Inventory** task. The Inventory Query Browser window opens.
2. In the Available Queries pane, expand the Custom folder to view the list of custom queries. Right-click the query you want to edit and click **Modify**.

3. Add or delete criteria in the Selected Criteria pane.
4. Click **File** → **Save** to save your changes and update the query.

Exporting inventory query results to a file

You can export inventory query results in CSV, HTML, or XML format.

Complete the following steps to export query results:

1. In the IBM Director Console Tasks pane, double-click the **Inventory** task. The Inventory Query Browser window opens.
2. In the Inventory Query Browser window, click the query.
3. Click **File** → **Export** and click the format to which you want to export the results.
4. Type a file name and specify the location where you want to save the file; then, click **OK**.

Viewing and editing the inventory software dictionary

You can use the inventory software dictionary to track software packages on your managed systems. You can create and modify software dictionary profiles that associate the title of a software package with one or more specific files on a managed system. You can specify exact file sizes, last-modified dates, and so on, to assist in tracking a specific level or release of the software.

Viewing the software inventory

When you collect inventory data on a managed system or group, the software query obtains the inventory software dictionary information.

To view the software inventory, follow the steps for collecting inventory data; then, in the Available Queries pane, expand the Standard folder and click the Software query. The software inventory displays in the Query Results pane.

Adding an entry to the inventory software dictionary

Complete the following steps to add an entry to the inventory software dictionary:

1. In the IBM Director Console Tasks pane, right-click the **Inventory** task; then, click **Edit Software Dictionary**. The Inventory Software Dictionary Editor window opens.

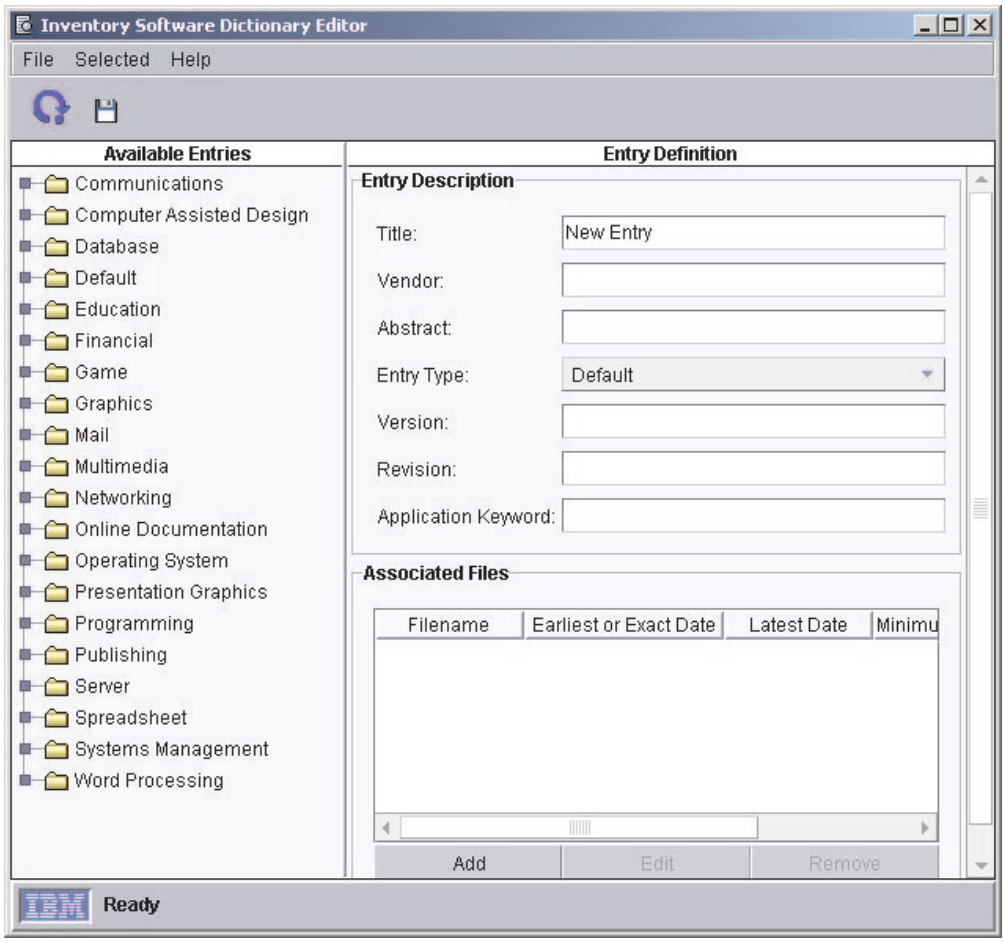

Figure 21. Inventory Software Dictionary Editor window

2. In the Entry Definition pane, `New Entry` is displayed in the **Title** field. In the **Title** field, type a name to identify the entry. In the **Entry Type** field, select which folder in the Available Entries pane the entry will be displayed. In the other fields, type the information you want to use to identify the application.

   The **Title** and **Entry Type** fields are the only required fields. However, any information you type in the Entry Description pane is displayed when you use the Inventory Query Browser window to view software information. It is not used as search criteria when collecting inventory data. The information entered in the Associated Files group box is used as the search criteria.

3. In the Associated Files group box, click **Add**. The Associated File Attributes window opens.
4. Click **Enter File Information Manually** or **Select File From List**; then, click **OK**. The second Associated File Attributes window opens.
5. If you clicked **Enter File Information Manually**, type the file name for which you want the inventory software scanner to search. To further qualify the file, you can type a specific file size, range of file sizes, file date, or range of file dates. Click **OK**.

   If you clicked **Select File from List**, type the file name in the **File Name** field, or select the file. Click **OK**. The corresponding attributes are displayed in the Associated Files group box.

6. (Optional) In the Associated Files group box, click **Edit** to change any of the attributes.

7. (Optional) If you want to add more files to the software dictionary entry definition, repeat step 3 on page 35 through step 6 on page 35.
8. Click the Save Entry icon. The definition is added immediately to the software dictionary. The next time inventory data is collected, the data you have provided in the Associated Files pane is used as a criteria in locating the file.

Inventory software dictionary matches

The inventory software dictionary finds a match for an entry definition only if all associated files for the entry are in the same directory. To locate product suites (such as Microsoft Office) that might not have all applications in the same directory, you can create separate inventory software dictionary entry definitions for each application in the suite and then create a dynamic group to display all managed systems and devices found with the specified application files.

Complete the following steps to create separate inventory software dictionary entries and to create a dynamic group:

1. In the IBM Director Console Tasks pane, right-click the **Inventory** task; then, click **Edit Software Dictionary**. The Inventory Software Dictionary Editor window opens. (See Figure 21 on page 35.)
2. In the Entry Definition pane, use the **Title** and **Entry Type** fields to identify and classify each entry you create in the inventory software dictionary. You also can fill in the other fields as needed.
3. Below the Associated Files group box, click **Add**. The Associated File Attributes window opens.
4. Click **Enter File Information Manually** or **Select File From List**; then, click **OK**. The easiest method is to select the file from a list. When you finish selecting the file name, the corresponding attributes are displayed in the Associated Files group box.
5. (Optional) Click **Edit** to change any of the attributes.
6. (Optional) If you want to add more files to the definition, repeat steps 3 through 5.
7. Click the **Save Entry** icon to save your software dictionary entry. You have now created one entry identifying the file (or set of files, if you specified more than one file) corresponding to one application in a single directory.
8. Click **File** → **New** to add another software dictionary entry. Repeat steps 2 through 7 for each software dictionary entry you want to create, and then click **File** → **Close** to close the Inventory Software Dictionary Editor window.
9. To ensure detection of the installed software packages, perform an inventory collection on the managed system or device with the specific software installed on it.
10. In the IBM Director Console Groups pane, right-click anywhere except on an entry and click **New Dynamic**. The Dynamic Group Editor window opens.
11. In the Available Criteria pane, expand the **Inventory** tree; then, expand the **Software** tree, and then expand the **Program Title** tree to display the list of software dictionary entries from which you can create a new dynamic group.
12. Locate and click the first software dictionary entry you created; then, click **Add** to add the entry to the Selected Criteria pane.
13. Locate and click the second software dictionary entry you created; then, click **Add** to add it to the Selected Criteria pane. Because multiple entries have been selected, the Choose Add Operation window opens.

14. Click **All true (AND)** to create a group that includes a managed system or device only if all of the software dictionary entries you selected are located on that managed system or device.
15. Locate and add the rest of the entries you created. For each subsequent entry you add to the Selected Criteria pane, select the **All true (AND)** option when prompted.
16. When you have finished building your group of entries, click **File** → **Save As**. The Save As window opens.
17. Type the name you want to display in the Groups pane. Click **OK**.
18. Click **File** → **Close Group Editor** to close the Dynamic Group Editor window.
19. Click the new group in the IBM Director Console Groups pane. The managed systems and devices that meet the search criteria for the software entries you created are displayed in the Group Contents pane. In this case, all entries have to be present on the managed system or device for the managed system or device to be displayed.

Process Management

You can use Process Management to manage 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 can issue commands on managed systems also. However, you cannot use the Process Management task or any subtasks on SNMP devices, BladeCenter chassis, or platforms.

In IBM Director Console, the Process Management task has three subtasks:

- Process Monitors
- Process Tasks
- Remove Process Monitors

Viewing and working with processes, services, and device-services information

To view processes, services, and device-services information, in the IBM Director Console Tasks pane, drag the **Process Management** task onto a managed system or group. The Process Management window opens and contains three pages:

Applications
: Shows all processes running on that managed system or group.

Services
: Shows the status of all Windows services that are installed on that managed system or group (only managed systems running Windows operating systems).

Device Services
: Shows all hardware device drivers installed on that managed system or group (only managed systems running Windows operating systems).

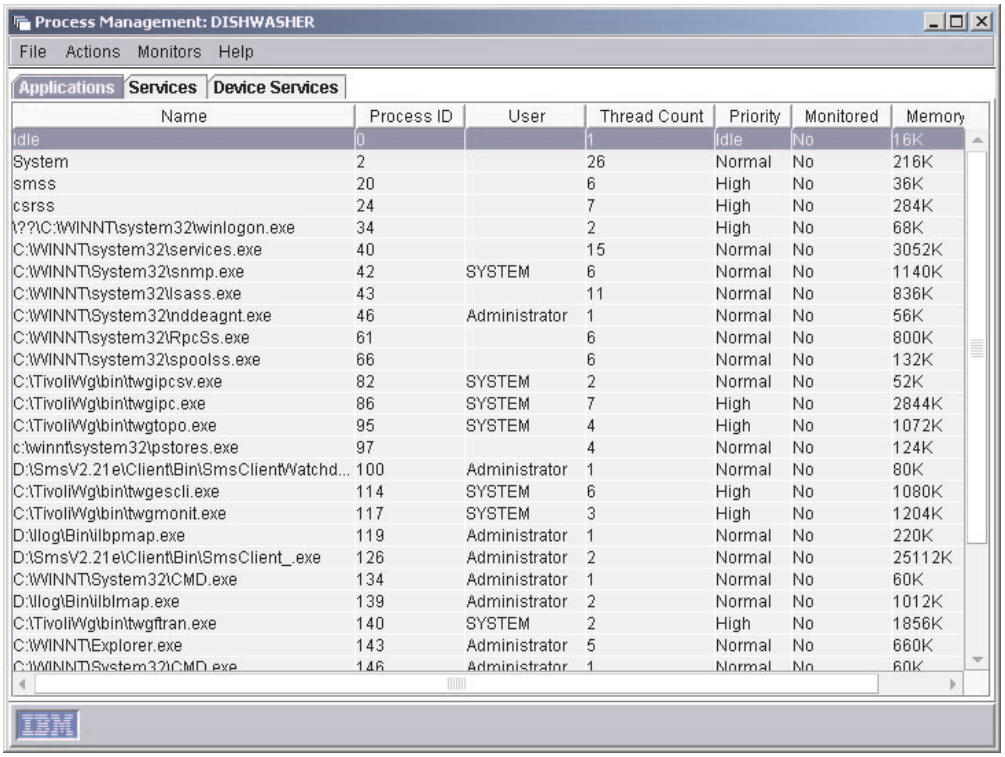

Figure 22. Process Management window

Closing an application (process)

Complete the following steps to close an application (process):

1. In the IBM Director Console Tasks pane, drag the **Process Management** task onto a managed system or group. The Process Management window opens.
2. On the **Applications** page, right-click the application (process) you want to close, and click **Close Application**. A confirmation window is displayed.
3. Click **Yes**.

Starting, stopping, pausing, and resuming Windows services

Complete the following steps to start, stop, pause, or resume a Windows service:

1. In the IBM Director Console Tasks pane, drag the **Process Management** task onto a managed system or group. The Process Management window opens.
2. Click the **Services** tab and right-click the service that you to want to start, stop, pause, or resume; then, click the applicable choice.

Starting and stopping device services

Complete the following steps to start or stop device services:

1. In the IBM Director Console Tasks pane, drag the **Process Management** task onto a managed system or group. The Process Management window opens.
2. Click the **Device Services** tab. Right-click the device that you to want to start or stop and click **Start Service** or **Stop Service**.

Creating and applying a process monitor

You can create a process monitor that generates an event if 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.

After you create a process monitor, you can apply it to one or more managed systems.

Creating a process monitor

Complete the following steps to create a process monitor:

1. In the IBM Director Console Tasks pane, expand the **Process Management** task.
2. Double-click the **Process Monitors** subtask. The Process Monitors window opens.

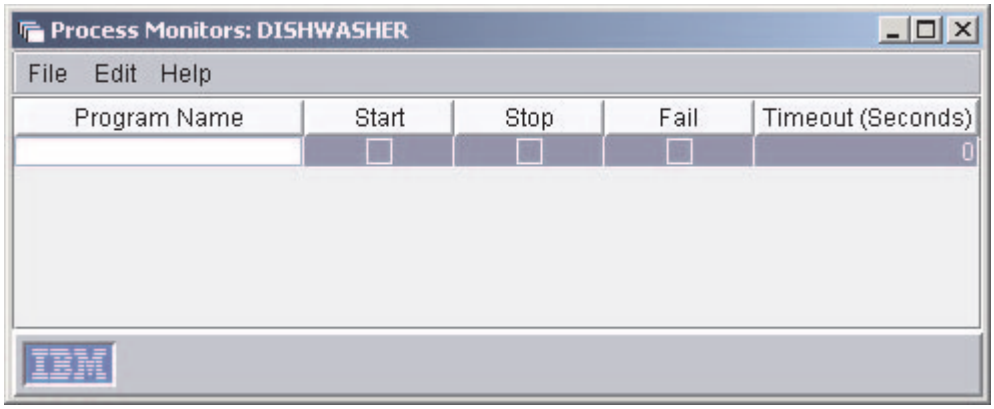

Figure 23. Process Monitors window

3. Type the executable file name of the application process you want to monitor.
4. Select any combination of the **Start**, **Stop**, and **Fail** check boxes, to specify which action or actions you want to monitor.
5. If you selected the **Fail** check box, type a timeout setting. This is the number of seconds that the process monitor will wait for the application process to start before generating a fail event.
6. To monitor additional processes with the same Process Monitors subtask, click **Edit** → **New Row**.
7. Repeat steps 3 through 5 until you have listed the executable file names of all the processes you want to monitor.
8. Click **File** → **Save As** to save the process monitor. The Save As window opens.
9. Type a name to identify the process monitor; then, click **OK**. The new process monitor is displayed as a subtask under the **Process Monitors** task in IBM Director Console.

Applying a process monitor

Complete the following steps to apply a process monitor:

1. Drag the process monitor onto the managed system or group that has a process you want to monitor. The Process Monitor window opens.
2. Click **Execute Now**, or click **Schedule** to schedule it for a later time. See “Scheduler” on page 51 for more information about how to schedule tasks.

Removing process monitors

When you no longer need to monitor a process on a managed system, you should remove the process monitor task. Doing so will avoid wasting managed-system resources.

You can remove monitors individually from a single managed system, or you can use the **Remove Process Monitors** subtask to remove all current process monitors on a managed system or group.

Removing process monitors individually

Complete the following steps to remove process monitors individually:

1. Drag the managed system or group from which you want to remove the process monitor onto the **Process Monitors** task. The Process Monitors window opens.
2. Right-click the process monitor you want to remove and click **Delete Row**.
3. Click **File** → **Save**. A confirmation message is displayed.
4. Click **Yes**. The monitor is removed from the managed system or group.

Removing all monitors from a system or group of systems

Complete the following steps to remove all process monitors from a managed system or group:

1. Drag the **Remove Process Monitors** subtask onto the managed system or group from which you want to remove all process monitors.
2. Click **Execute Now**, or click **Schedule** to schedule the removal for a later time. See “Scheduler” on page 51 for more information about how to schedule tasks.

Viewing process monitors

To view a list of the process monitors running on a managed system or group, drag the **Process Monitors** task onto the managed system or group. The Process Monitors window opens, and the list of process monitors running on that managed system is displayed.

Creating and running process tasks

You can use the Process Tasks subtask 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. These process tasks can be issued immediately, scheduled to run at a specific time and date, or scheduled to run on a repeating schedule (see “Scheduler” on page 51 for more information about scheduling tasks).

Remember that because you are running a command-line program on a managed system, anything that a system-account user can do from a command line can be done to the managed system regardless of the user that is logged in on the managed system.

Consider naming the process tasks you create appropriately. The name for a process task should include the following information:

- Type of process task to be run
- Name of the process task to be run
- Types of managed systems with which the process task will work properly

All process tasks are alphabetized in the list.

Creating a process task

Complete the following steps to create a process task:

1. In the IBM Director Console Tasks pane, expand the **Process Management** task.
2. Double-click the **Process Tasks** subtask. The Process Task window opens.

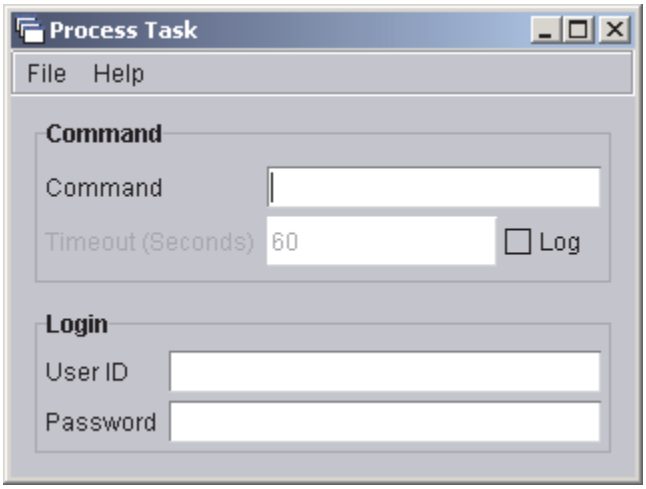

Figure 24. Process Task window

3. Type the command-line program to be run.
4. If the command produces text-based output (for example, a directory listing), select the **Log** check box and type a timeout value, in seconds. Make sure that the timeout value is long enough to complete the running of the command.
5. (Optional) If you want to run this process using another user ID, specify a user ID and password.
6. Click **File** → **Save As** to save the process task. The Save As window opens.
7. Type a name and click **OK**. The new process task is displayed under **Process Tasks** in IBM Director Console.

Running a process task

Complete the following steps to run a process task:

1. Drag the process task onto the managed system or group on which you want to run the process task. The Process Task window opens.
2. Click **Execute Now**, or click **Schedule** to run the process task at a later time. (See "Scheduler" on page 51 for more information about scheduling tasks.)

   If you chose to run the process task now, the Execution History window opens, indicating the status of the process task.

Execution History window

IBM Director Server maintains a history of the process tasks that are run on managed systems. The Execution History window opens automatically when you run a process task. Through this window, you can run a previously run task immediately, or export the execution history.

Issuing a command on a managed system

You can use the Process Management task to issue a command-line program on a managed system.

Complete the following steps to issue a command:

1. In the IBM Director Console Tasks pane, drag the **Process Management** task onto a managed system or group. The Process Management window opens.
2. Click **Actions** → **Execute Command**.
3. The Execute Command window opens.

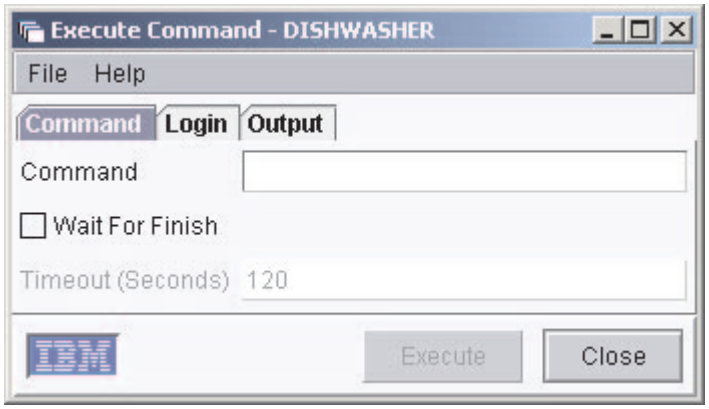

Figure 25. Execute Command window

It has three pages:

Command
Type a command to be issued on the managed system.

Login Specifies a different user for the command to run on the managed system.

Output
Displays any output the command would normally provide.

Note: When using this option, you can set a timeout value for the command you specify on the Command page.

4. Click **Execute** to run the command.

Restricting anonymous command execution

By default, commands are executed on the 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.

For managed systems running Windows, complete the following steps to require a user ID and password:

1. In a command line, type
   ```
   regedit
   ```
2. Navigate to the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Director\CurrentVersion.
3. Double-click **RestricAnonCmdExec**.
4. In the **Value data** field, change **0** to **1**.
5. Click **OK**.

For managed systems running Linux, complete the following steps to require a user ID and password:

1. Change to the directory where the IBM Director Agent is installed, which by default is opt/IBMdirector/data. To do this, at a command prompt, type
   ```
   cd opt/IBM/director/data
   ```
   then
   ```
   vi ProcMgr.properties
   ```

2. Change the line

   ```
   RestrictAnonCmdExec=false
   ```

   to

   ```
   RestrictAnonCmdExec=true
   ```

3. Save the file. The changes take effect immediately.

Resource Monitors

You can use resource monitors to view statistics about critical system resources, such as processor, disk, and memory usage. With resource monitors, you can also set thresholds to detect potential problems with managed systems or devices. When a threshold is met or exceeded, an event is generated. You create event action plans to respond to resource-monitor events (see “Event action plans” on page 21 for more information about how to do this). You can apply resource monitors to individual managed systems and devices and to groups.

In IBM Director Console, under the **Resource Monitors** task, two subtasks are displayed:

- All Available Recordings
- All Available Thresholds

You can use these subtasks to view information about previously configured resource-monitor recordings and previously configured resource-monitor thresholds, respectively.

Viewing available resource monitors

You can view the resource monitors available for a managed system, device, or group. (For more information on resource-monitor attributes, see Appendix A, “Resource-monitor attributes” on page 93.)

Complete the following steps to view resource monitors available for a managed system, device, or group:

1. In the IBM Director Console Tasks pane, drag the **Resource Monitors** task onto the managed system, device, or group that you want to monitor. The Resource Monitors window opens.
2. In the Available Resources pane, expand the tree to view which resource monitors are available.

Setting a resource-monitor threshold

If you set a resource-monitor threshold for an attribute on a managed system or device, an event is generated when the threshold is met or exceeded. Most resource-monitor thresholds are numeric values, although for some resource monitors you can set text-string thresholds, where a text string is monitored and an event is generated if the text changes.

Complete the following steps to set a resource-monitor threshold:

1. In the IBM Director Console Tasks pane, drag the **Resource Monitors** task onto the managed system, device, or group that you want to monitor. The Resource Monitors window opens.

2. In the Available Resources pane, expand the tree; then, double-click the resource you want to monitor. The resource is displayed in the Selected Resources pane.

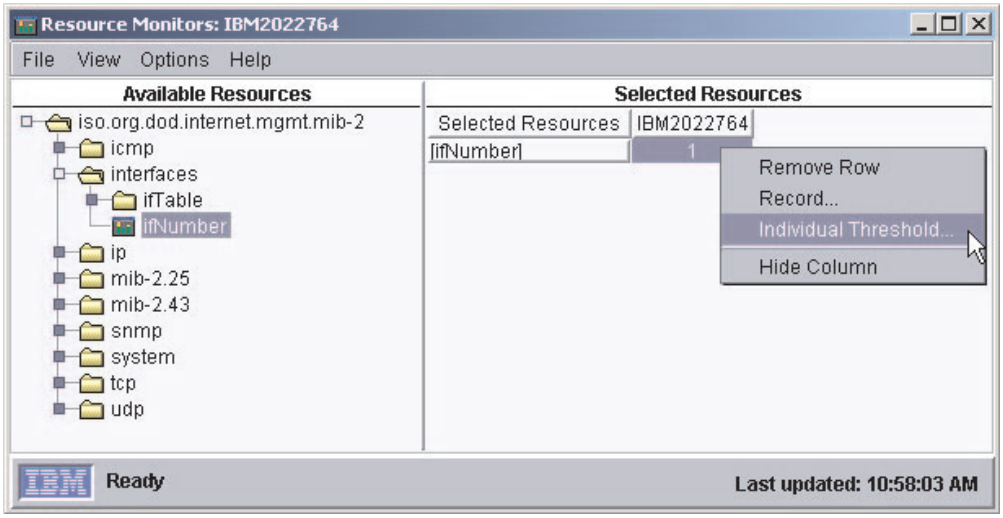

Figure 26. Resource Monitors window for a managed device

3. In the Selected Resources pane, right-click the resource attribute you want to monitor; then, click **Individual Threshold** if you dropped the Resource Monitors task onto an individual managed system or device. Or, click **Group Threshold** if you dropped the Resource Monitors task onto a group. The System Threshold window opens, and depending on whether the resource-monitor threshold is numeric (Figure 27 on page 45) or a text string (Figure 28 on page 46), you see the applicable window.

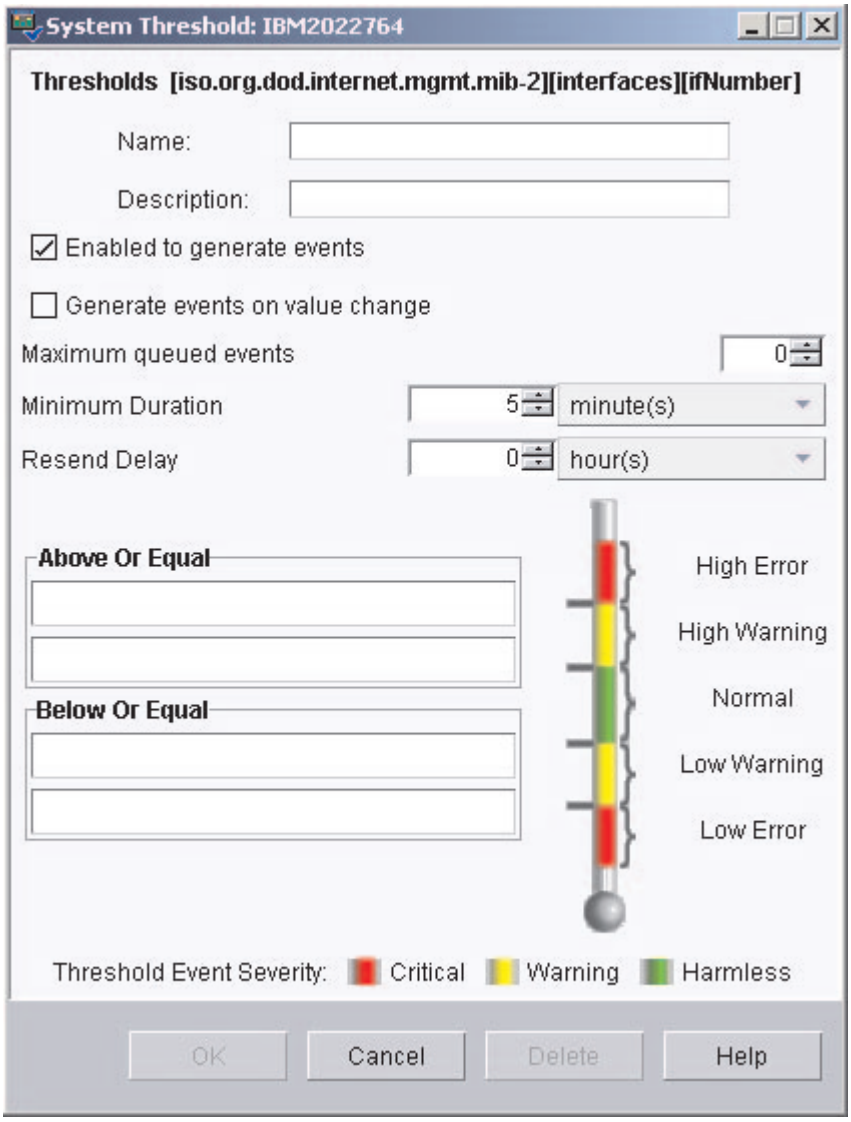

Figure 27. System Threshold window for setting numeric thresholds

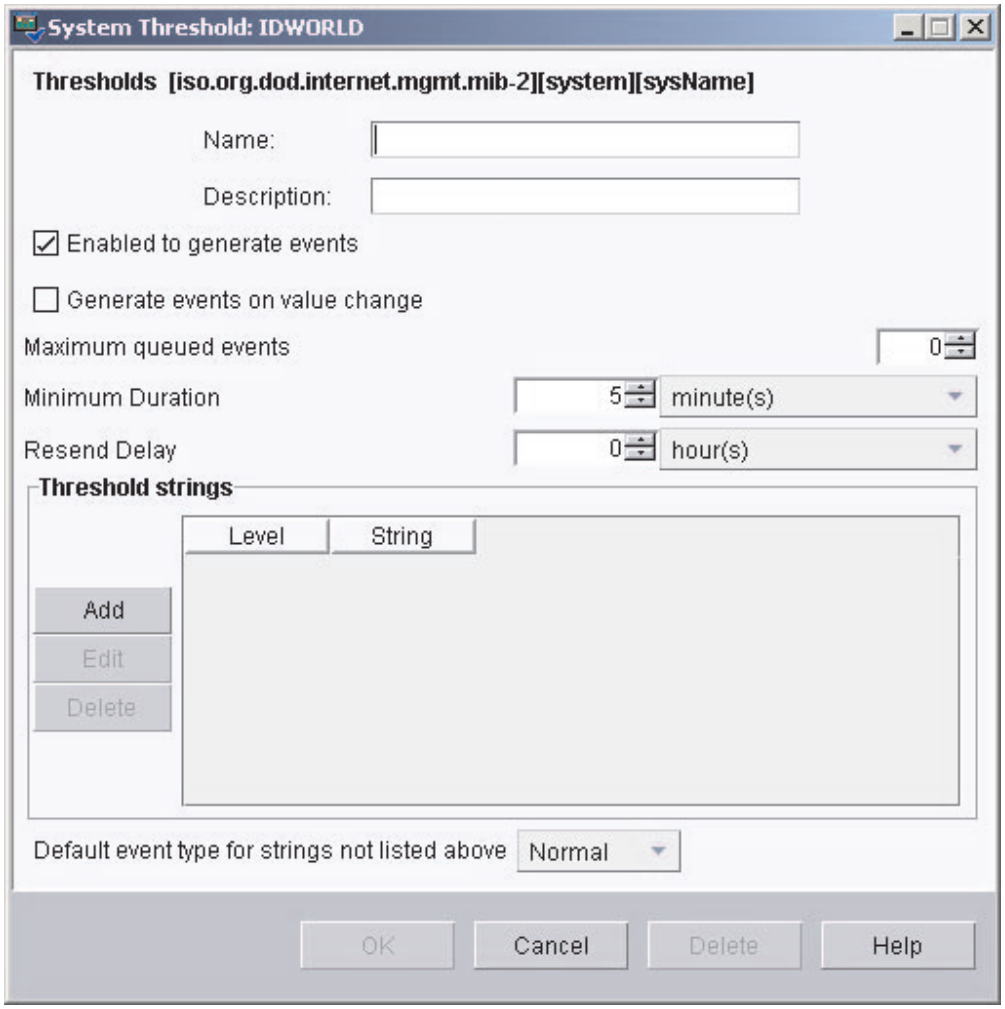

Figure 28. System Threshold window for setting text threshold strings

4. Type a name for the threshold and complete the applicable fields. The **Enabled to generate events** check box is selected by default, so if the threshold you set in this window is met or exceeded, an event is generated. To be alerted when an event is generated, you must set up an event action plan that uses a threshold event filter (see "Event action plans" on page 21 for more information).

   If you select the **Generate events on value change** check box, you cannot specify a threshold value. An event is generated if the value changes for the specified attribute and the **Enabled to generate events** check box is selected.

   To monitor a text-string threshold, in the "Threshold strings" group box, click **Add**. The "Add string threshold setting" window opens. Type the text you want to monitor, and select an event type from the list; then, click **OK**. The text string and event type are displayed in the "Threshold strings" group box.
5. Click **OK**. The threshold is set immediately.

If you set an individual threshold, in the Resource Monitors window, a threshold icon is displayed in the data cell of the attribute you selected. In IBM Director Console, an icon is displayed beside the managed system in the Group Contents pane. If the threshold state changes from Normal to Met or Exceeded, the icon changes to reflect the change.

If you set a group threshold, a threshold icon is displayed in the Selected Resources attribute cell in the Selected Resources pane. If a threshold is met or exceeded on a managed system or device in the selected group, the data cell for the managed system that meets the criteria displays an icon indicating that the threshold has been met.

The following table lists the resource-monitor status icons and what each icon indicates.

Table 2. Resource-monitor status icons

Icon	Description
	The threshold was set successfully and is in the Normal state.
	The threshold was met and has generated an event.
	Statistics are being recorded.
	The monitor has been disabled.

Viewing all resource-monitor thresholds

To view all previously created resource-monitor thresholds, in the IBM Director Console Tasks pane, expand the **Resource Monitors** task; then, double-click the **All Available Thresholds** subtask. The All Available Thresholds window opens, displaying all the thresholds created.

To view all the thresholds set on an individual managed system or group, drag the **All Available Thresholds** subtask onto a managed system or group. The All Available Thresholds window opens, displaying all the thresholds created for that system or group.

Recording a resource monitor

Note: You cannot record a resource monitor for a group. You can set and record resource monitors for individual managed systems or devices only.

You can record a resource monitor to capture statistics about a managed system. Complete the following steps to start recording a resource monitor:

1. In the IBM Director Console Tasks pane, drag the **Resource Monitors** task onto the managed system that has the resource you want to record. The Resource Monitors window opens.
2. In the Available Resources pane, expand the tree; then, double-click the resource you want to record to add it to the Selected Resources pane.
3. Right-click the attribute cell relating to the resource and the managed system you want to monitor and click **Record**.

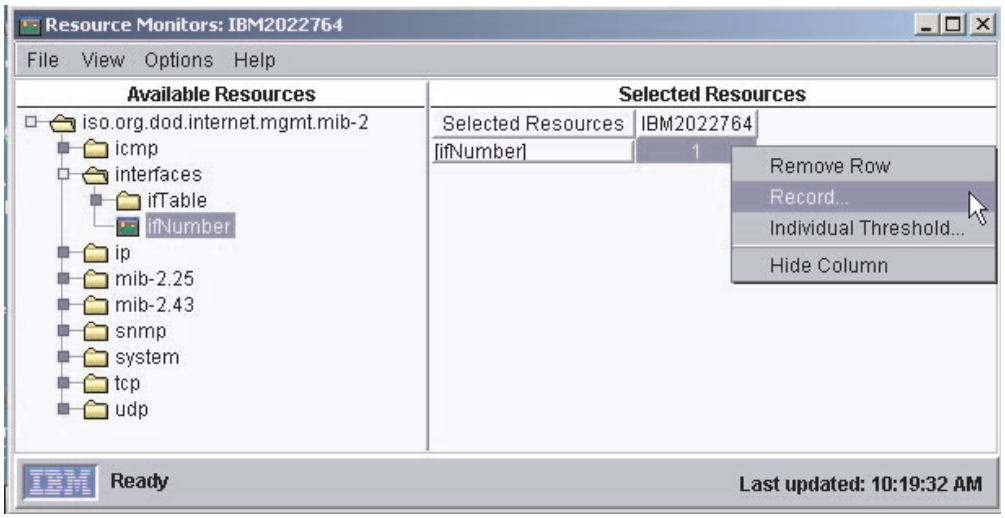

Figure 29. Resource Monitors window

The Resource Monitor Recording window opens.

Figure 30. The Resource Monitor Recording window

4. Click **File** → **New**. The New Record window opens.

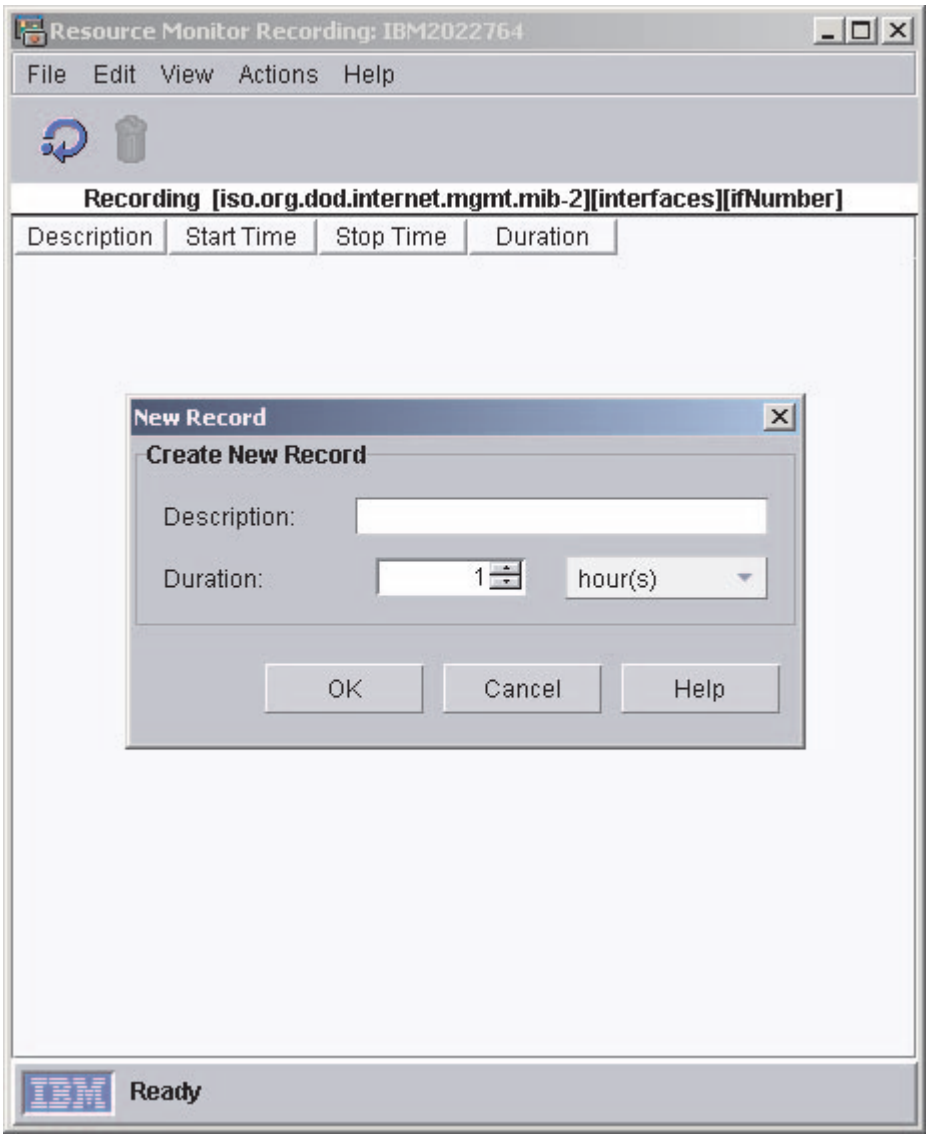

Figure 31. New Record window

5. Type a description and select the length of time to record the resource monitor.
6. Click **OK** to start recording. The Resource Monitors Recording window is updated to include the recording you just created. Click **View** → **Refresh** to update the status of the recording.

Viewing a graph of a resource-monitor recording

Complete the following steps to view a graph of a resource-monitor recording:

1. In the IBM Director Console Tasks pane, expand the **Resource Monitors** task.
2. Drag the **All Available Recordings** task onto the managed system or group for which you want to review the recordings. The All Available Recordings window opens.
3. Locate the recording you want to review; then, right-click the cell and click **Graph**. The Recorded Data window opens, displaying a graph of the recorded data.

Exporting a resource-monitor recording

You can export a resource-monitor recording to a file in CSV, TXT, HTML, or XML format for the purpose of archiving statistics.

Complete the following steps to export a resource-monitor recording:

1. In the IBM Director Console Tasks pane, expand the **Resource Monitors** task.
2. Drag the **All Available Recordings** task onto the managed system that has a resource-monitor recording you want to export. The All Available Recordings window opens.
3. Right-click the recording you want to export and click **Export**. The Export window opens.

   Note: You can save the file to a local directory on the management server only.
4. Type a name for the file, and click **OK**.

Monitoring the same resource on multiple groups or managed systems

You can apply a threshold task, which is a resource-monitor threshold that you have already created, to individual managed systems or groups to monitor the same resource for a given set of conditions on multiple groups or managed systems. A threshold task is created by taking a resource monitor that is configured already and exporting it to a task.

Complete the following steps to create a threshold task:

1. Create an individual or group threshold.
2. In the IBM Director Console Tasks pane, expand the **Resource Monitors** task.
3. Drag the **All Available Thresholds** subtask onto one of the managed systems. The All Available Thresholds window opens.
4. Right-click the threshold you want to export to a task and click **Export to Task**. The Export Task window opens.
5. Type a descriptive name for the task, and click **OK**.

The new task is displayed in IBM Director Console under the Resource Monitors task. You can drag this new task onto other managed systems or groups to set identical threshold alerts.

Viewing resource-monitor data on the ticker tape

You can view the resource-monitor data for a managed system or group continually in IBM Director Console using the ticker-tape display feature.

Complete the following steps to view resource-monitor data through the ticker tape:

1. In the IBM Director Console Tasks pane, drag the **Resource Monitors** task onto the managed system or group that has the resource monitor you want to view using the ticker tape. The Resource Monitors window opens.
2. In the Available Resources pane, expand the tree and locate the resource monitor for which you want to display the data.
3. Right-click the resource monitor and click **Add to Ticker Tape on IBM Director Management Console**. The managed system name or group name and the resource-monitor data are displayed on the ticker tape.

Stopping the ticker-tape message display of data

To stop all resource-monitor data from being displayed in the ticker-tape area of the management console, in IBM Director Console, right-click the ticker-tape message, click **Remove All Monitors**.

Scheduler

You can use the Scheduler task to schedule a single noninteractive task or sets of noninteractive tasks to occur at a later time. You can specify an exact date and time you want the task to be started, or you can schedule a task to repeat automatically at a specified interval. Scheduled tasks are referred to as jobs.

IBM Director does not permit saving changes to an existing job; you must always save it as a new job.

Starting the Scheduler task

You can start the Scheduler task in either of two ways:

- Scheduling a task directly
- Dragging a task to a managed system or group

To schedule a task using the second technique, see “Dragging a task onto a managed system or group” on page 56.

Scheduling a task directly

Complete the following steps to schedule a task directly in Scheduler:

1. In IBM Director Console, click **Tasks** → **Scheduler**. The Scheduler window opens.

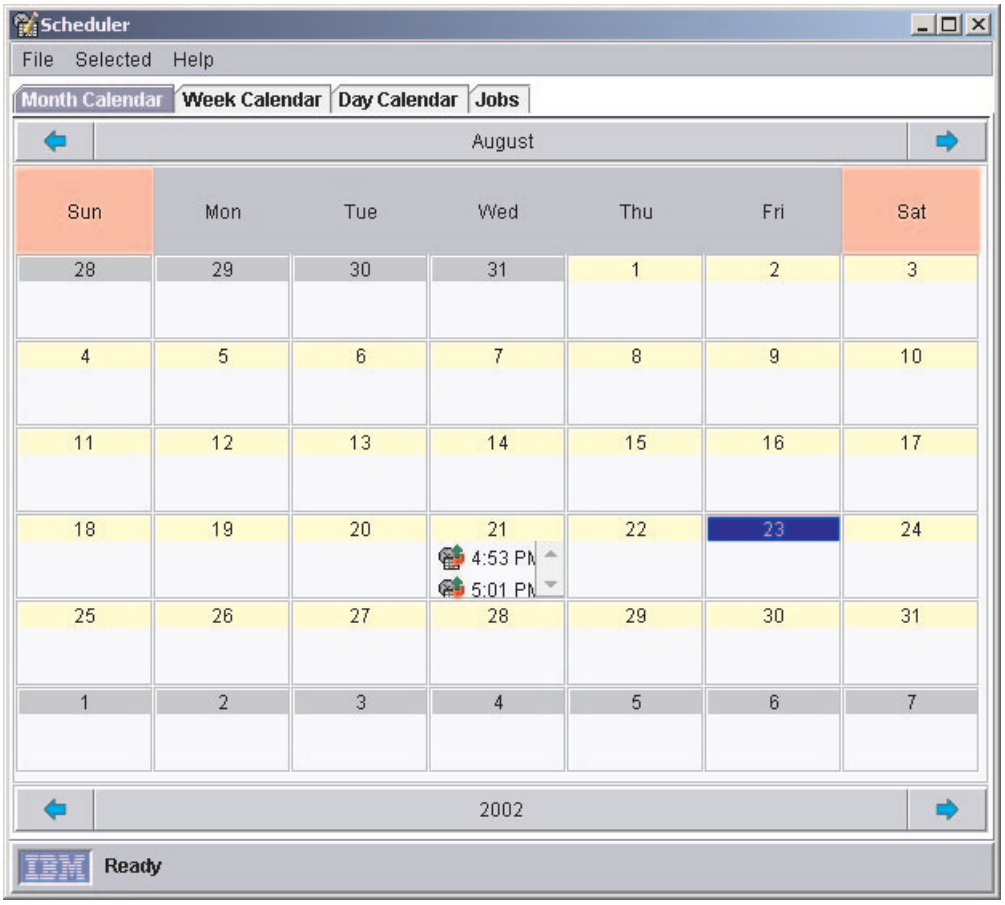

Figure 32. Scheduler window

2. Double-click the date on which you want the new job to start. The New Scheduled Job window opens.

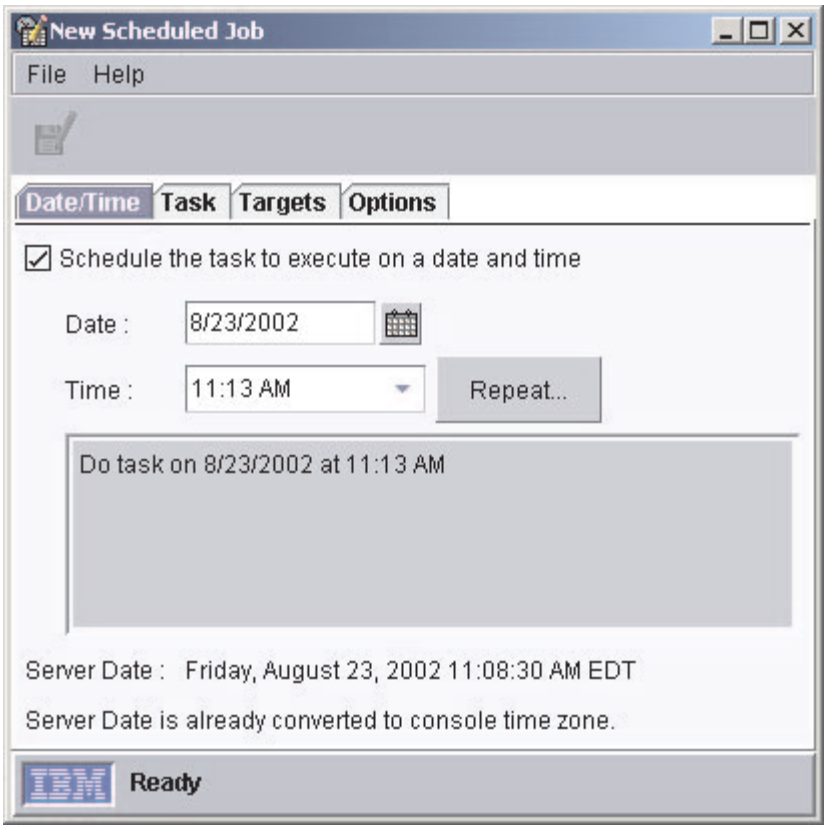

Figure 33. New Scheduled Job window

The New Scheduled Job window has four pages:

- **Date/Time**
- **Task**
- **Targets**
- **Options**

3. In the Date/Time page, specify a date and time for your scheduled job to be activated.

   Note: If you are using IBM Director Console on a system running Windows, ensure that the Windows system time matches the IBM Director Console time; otherwise, the scheduled job will not run at the correct time.

   Select the **Schedule the task to execute on a date and time** check box to activate the job. If you do not select this check box, you cannot assign a date and time to the job. The job is added to the jobs database, but it is not activated automatically. You must activate it manually when you want to execute the job.

   If you want the job to repeat, click **Repeat** to create a repeating schedule for re-executing a job. The Repeat window opens.

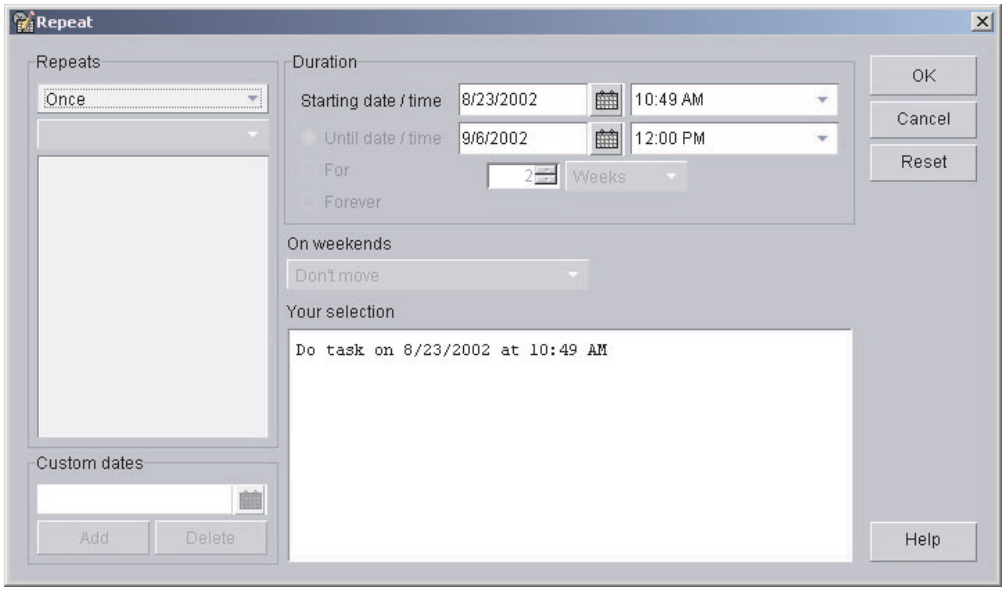

Figure 34. Repeat window

In the **Repeats** group box, use the two lists to specify how often the job is repeated. Use the first list to specify hourly, daily, weekly, monthly, or yearly intervals and the second list to specify incremental hours, days, and so on. If you click **Custom** in the first list, the **Custom Dates** group box is enabled. Type the discrete dates on which to repeat the scheduled job.

In the **Duration** group box, type a specific start and stop date, or click **Forever**. This action sets limits on how many times the job repeats. To opt for special handling if a scheduled job falls on a weekend, click an option from the **On weekends** list. Click **OK**.

4. Click the **Task** tab. In the Available pane, double-click a task you want the job to perform from a list of all the tasks that can be scheduled. The task is added to the Selected Task pane. You can select multiple tasks for a single job. Each task is processed in the order in which it is displayed on the Selected Tasks pane.
5. Click the **Targets** tab. If you want to use an entire managed group as the job target, click **Use a group as the target**. In the Available pane, double-click the group. The group is added to the Selected Group pane. You can select only one group as a target for any job.

   If you want to specify a list of managed systems as the target, click **Specify a list of systems as targets**. In the Available pane, double-click a managed system. The managed system is added to the Selected Group pane. Repeat until you have added all the managed systems on which you want to execute the job.
6. Click the **Options** tab. The Options page has three group boxes:
   - **Special Execution Options**
   - **Execution History**
   - **Events**

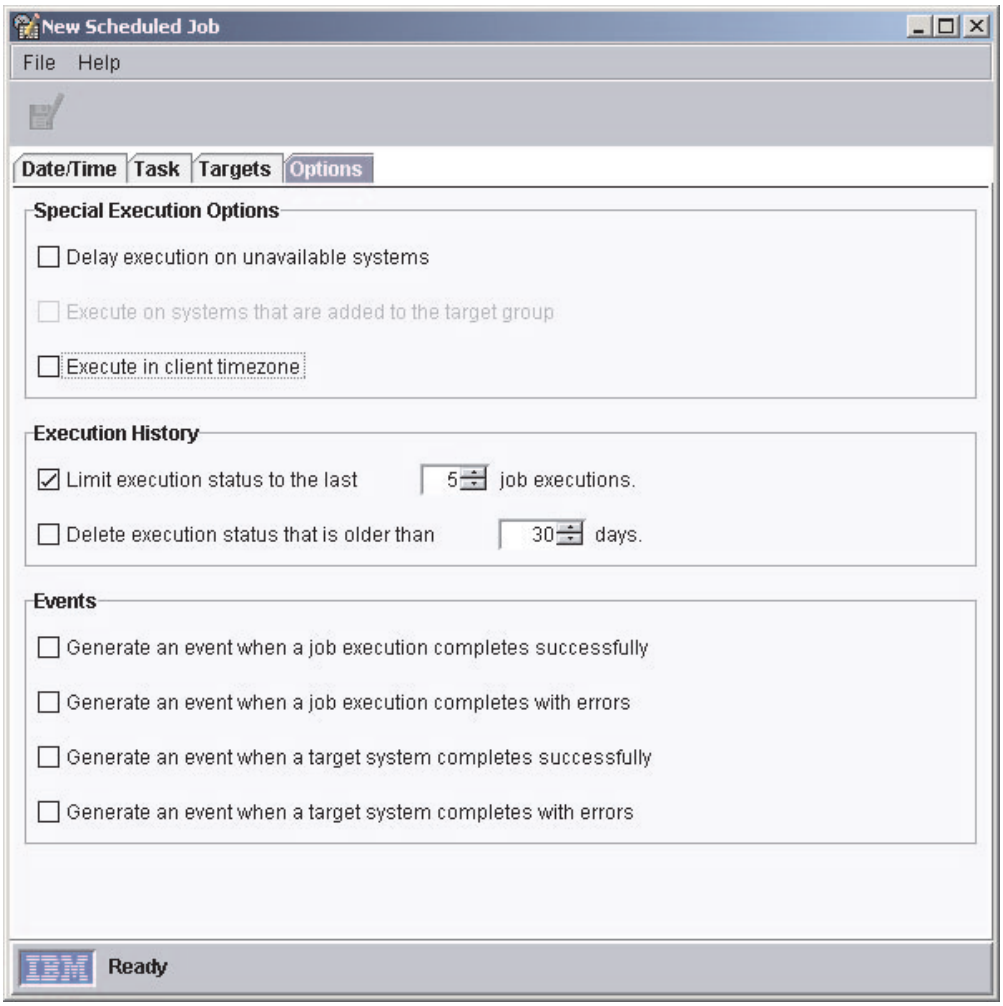

Figure 35. Options page in New Scheduled Job window

The following three special execution options are available:

Delay execution on unavailable systems

If you select this check box, targeted systems that are offline at the time of job activation will have the task performed on them when they are online again. For example, if a managed system was offline at the time of job execution and comes online at a later time, the task will be executed on that managed system as soon as it comes back online.

If you do not select this check box and a targeted system is offline at the time of job activation, the job returns an error status.

Execute on systems that are added to the target group

If you select this check box, any new managed systems that are added to the target group are detected, and the scheduled job is activated on the managed systems that have just been added.

Selecting this check box also causes the execution of a one-time job to stay active until you explicitly cancel it. This option is available only if the target is a managed group, not a list of specific managed systems.

Execute in client time zone

If you select this check box, tasks are executed according to the time zone in which the target managed system resides.

You cannot schedule a job to repeat hourly and be executed in the time zone of the target managed system. Also, if the first scheduled time zone start date occurs before the target managed system date, the job cannot be created.

In the **Execution History** group box you can limit the number of job executions included in the execution history. If you want to limit this information, select the applicable check box.

The **Events** group box has four options:

- **Generate an event when a job execution completes successfully**
- **Generate an event when a job execution completes with errors**
- **Generate an event when a target system completes successfully**
- **Generate an event when a target system completes with errors**

Select the applicable check box to generate an event in the case of successful completion or completion with errors in the execution of a scheduled job, either on all of the target systems or on individual target systems. For example, if a target system does not respond, the target system completes with errors.

7. Click **File** → **Save As**. The Save Job window opens.
8. Type a descriptive name for the scheduled job. Click **OK**. A confirmation message is displayed indicating you have successfully saved the job.
9. Click **OK** to close the message window.

Dragging a task onto a managed system or group

Certain tasks you perform, such as starting a process task, support scheduling by dragging the task onto a managed system or group.

Complete the following steps to schedule a task by dragging the task onto a managed system or group:

1. Drag a noninteractive task (certain tasks you perform using Process Monitors and Process Tasks, for example, support scheduling this way) onto a managed system or group. You are prompted to choose whether to perform the task immediately or to schedule it.
2. Click **Schedule**. The New Scheduled Job window opens.

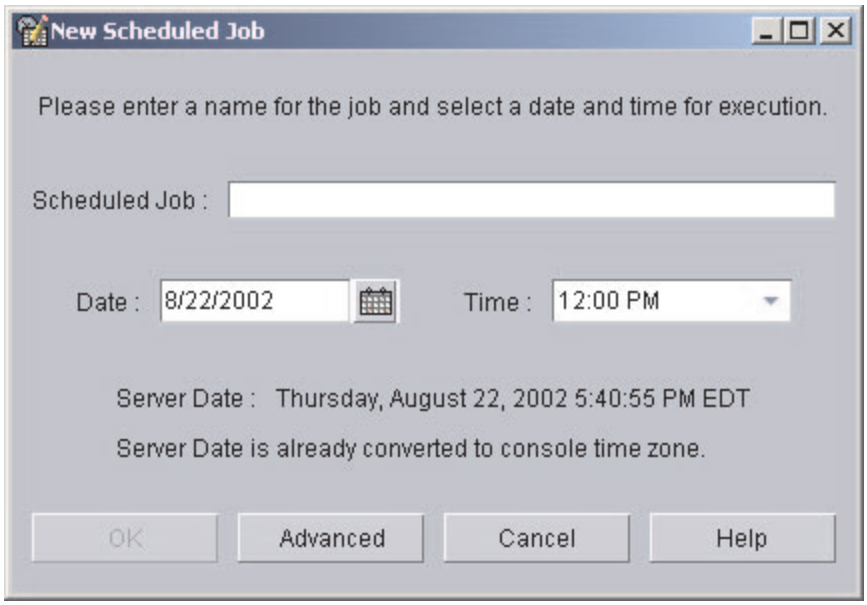

Figure 36. New Scheduled Job window, when you opt to schedule a task that is activated by dragging it onto a managed system

3. In the New Scheduled Job window, type a title for the scheduled job, the date you want the job to be executed, and the time you want the job to start.
4. To save the job, complete the following steps:
   a. Click **OK**. The Save Job window opens.
   b. Type a descriptive name for the scheduled job. Click **OK**. A confirmation message is displayed indicating you have successfully saved the job.
   c. Click **OK** to close the message window.

   To set additional options, such as setting special job properties, generating events when the job is completed, or specifying when the job repeats, complete the following steps:
   a. Click **Advanced** to open another New Scheduled Job window.
   b. Go to step 3 on page 53 to continue.

Viewing information about scheduled jobs

You can view information about previously scheduled jobs. In IBM Director Console, click **Tasks** → **Scheduler**. The Scheduler window opens (see Figure 32 on page 52).

The Scheduler window has four pages:

- **Month Calendar**
- **Week Calendar**
- **Day Calendar**
- **Jobs**

The first three pages are calendar pages; the **Jobs** page lists all the scheduled jobs.

Using the Calendar pages

The three calendar pages, Month, Week, and Day, show when all jobs have been scheduled to be executed. To view the execution history for a job, right-click a job and click **Open Execution History**.

Note: The calendars are independent of each other. This means that changing the date on one calendar does not change the date on another calendar. Also, selecting a job on one calendar does not select it on other calendars.

Viewing job information

The Jobs page displays a list of all scheduled jobs and status information for job executions. Clicking a scheduled job type in the left pane displays information about that job type, such as number of executions that are active or complete, the next date the job will be executed, the tasks that the job will perform, and any options that have been specified for the job, in the right pane (see Figure 37).

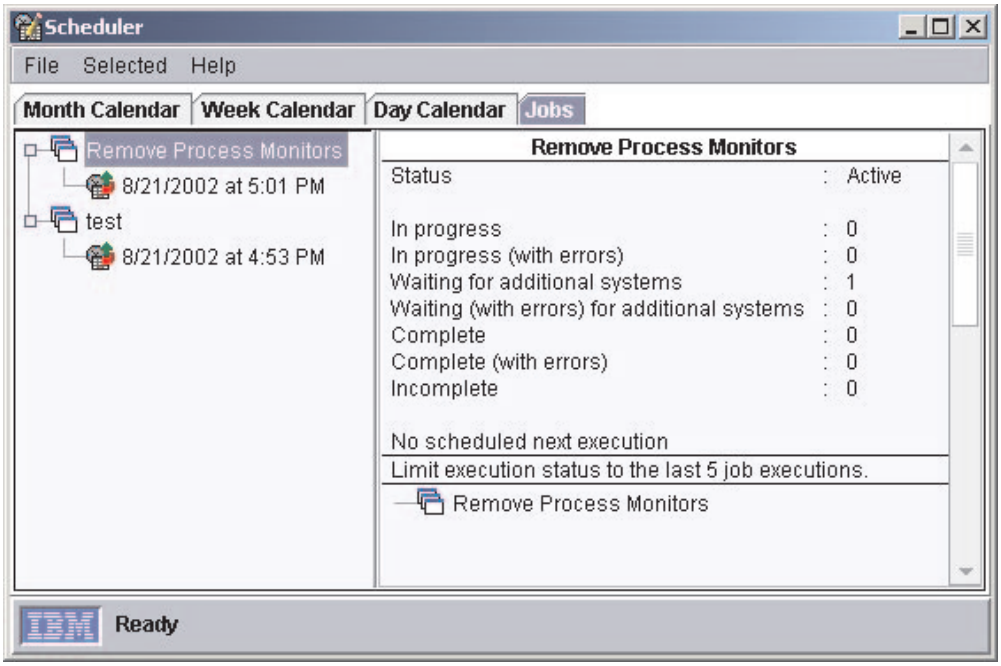

Figure 37. Selecting a job type in the left pane on the Jobs page in the Scheduler window

Clicking a specific execution of a scheduled job in the left pane displays information about that job execution in the right pane. The information that is displayed is identical to the information in the Execution History window.

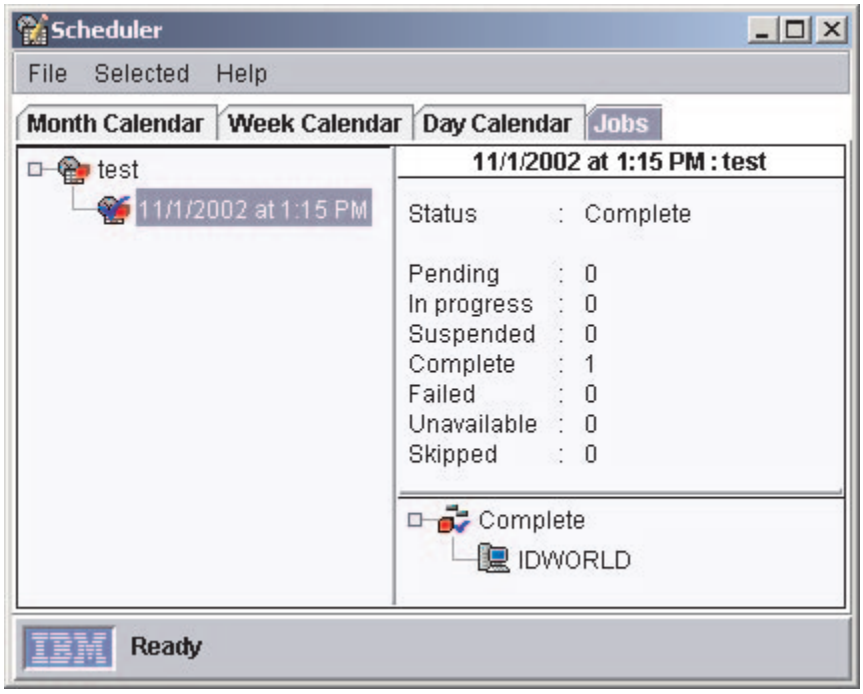

Figure 38. Selecting a specific job execution in the left pane on the Jobs page in the Scheduler window

Viewing job properties

To view the properties of a scheduled job in the Scheduler window, right-click a job and click **Open Job Properties**. The Scheduled Job window opens for the job, with four pages, Date/Time, Task, Targets, and Options.

You can use the Scheduled Job window to change the properties of a job and save it as another scheduled job. IBM Director does not permit saving changes to an existing job; you always must save it as a new job.

Viewing scheduled job history information

To view information about the execution of a scheduled job in the Scheduler window, right-click a job and click **Open Execution History**. Scheduler maintains the execution history information for immediate executions and scheduled jobs.

The Execution History window displays the overall status of the job. The top pane shows a summary of the status (for example, Complete) for the target systems. Target systems are grouped together based on the status of each target for an execution and are displayed in the bottom pane of the window.

Viewing execution history logs

To view the entire log for an execution history in the Scheduler window, right-click a job and click **View Log**.

SNMP devices

IBM Director discovers SNMP devices in your network according to discovery parameters that you can specify. The process used to discover SNMP devices in your network uses lists of initial IP addresses, community names, and subnet masks.

IBM Director works with SNMPv1 and SNMPv2c for all communications and recognizes Management Information Bases (MIBs) in System Management Information (SMI) version 1 and 2 formats.

SNMP devices and agents use community names to control their access. A community name can be any case-sensitive text string. By default, the community name of an SNMP device is set to `public`. If specific SNMP devices in your network have unique community names to restrict access, you can specify the correct name to gain access to the device.

The subnet mask allows you to further refine the scope of the discovery process, limiting the search to certain subnets in the network. The default subnet mask is set to the subnet of each corresponding IP address.

Using your lists of IP addresses, community names, and subnet masks, a series of SNMP GET statements are performed against port 161 of the IP address to determine if the address is associated with a valid SNMP device. A valid SNMP device for IBM Director has the following values accessible: sysName, sysObjectID, sysLocation, sysContact, and sysUpTime. If the object is determined to be a valid SNMP device, another series of SNMP GET statements are sent to obtain information in the atTable, where additional IP addresses can be used to discover even more SNMP devices. The search continues until no new addresses are located. Newly discovered or created SNMP devices managed object names will default to the value of sysName. If this value is blank, then the hostname of the device is used. If hostname is blank, the IP address is used.

All SNMP traps configured with IBM Director Server as the destination are forwarded as an event to the event log. Therefore, by dragging the Event Log task onto the SNMP managed device that originated the trap, you can view any events received. If a trap is received corresponding to an SNMP device that has not been discovered, then IBM Director creates the device automatically if you selected the **Auto-add unknown agents which contact server** check box on the SNMP Discovery page in the Discovery Preferences window.

Setting discovery parameters

Complete the following steps to set discovery parameters for SNMP devices:

1. In IBM Director Console, click **Options** → **Discovery Preferences**. The Discovery Preferences window opens.
2. Click the **SNMP Discovery** tab. Use the **Add**, **Replace**, and **Remove** buttons to create your lists of IP addresses, corresponding subnet masks, and community names.

Creating a new SNMP device

Complete the following steps to create a new SNMP device:

1. In IBM Director Console, right-click the Group Contents pane and click **New SNMP Devices**. The Add SNMP Devices window opens.

2. Type the network address and the community name. Select the **Use as a discovery seed** check box if you want to use this device address as an initial address for discovering additional SNMP devices.
3. Click **OK** to add the SNMP device to the Group Contents pane.

SNMP browser

You can use the SNMP browser to view and configure the attributes of SNMP devices, for example, hubs, routers, or other SNMP-compliant management devices. You can use the SNMP browser for SNMP-based management, troubleshooting problems, or monitoring the performance of SNMP devices.

Before you use the SNMP browser, you must compile any MIB files, so you can view the SNMP data correctly in the SNMP browser.

Compiling a MIB file

The SNMP browser initially displays a tree view of the MIB structure for the SNMP devices selected. If no compiled MIBs are available on IBM Director Server to format the information, or if the device returns information not found in a compiled MIB, then the information is displayed in a dotted-decimal numerical format. IBM Director ships with various MIBs normally needed for SNMP browsing for commonly defined devices. They are located in the Director\data\snmp directory.

MIB data is stored in its own persistent storage file, snmpmib.bag, located in the Director\data directory. By deleting this file and snmpfilename.bag, you can remove all MIB data in IBM Director, but not lose other persistent storage data.

Complete the following steps to compile a MIB file:

1. In the IBM Director Console Groups pane, right-click **SNMP Devices Group** and click **Compile New MIB**.
2. Specify the directory and file name of the MIB file you want to compile and click **OK**. The status messages window indicates the progress of the compilation.

To start the SNMP browser, in the IBM Director Console Tasks pane, drag the **SNMP Browser** task onto an SNMP device. The SNMP Browser window opens.

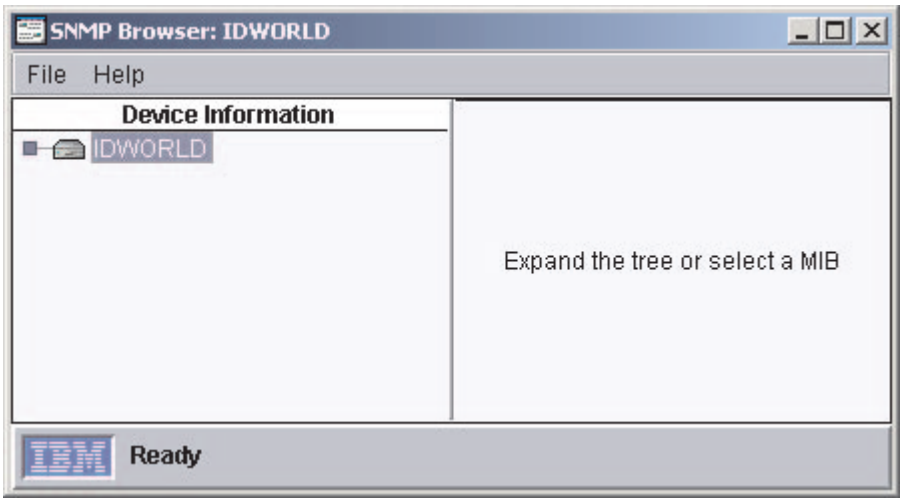

Figure 39. SNMP Browser window

In the SNMP Browser window Device Information pane, expand the tree to view the SNMP information.

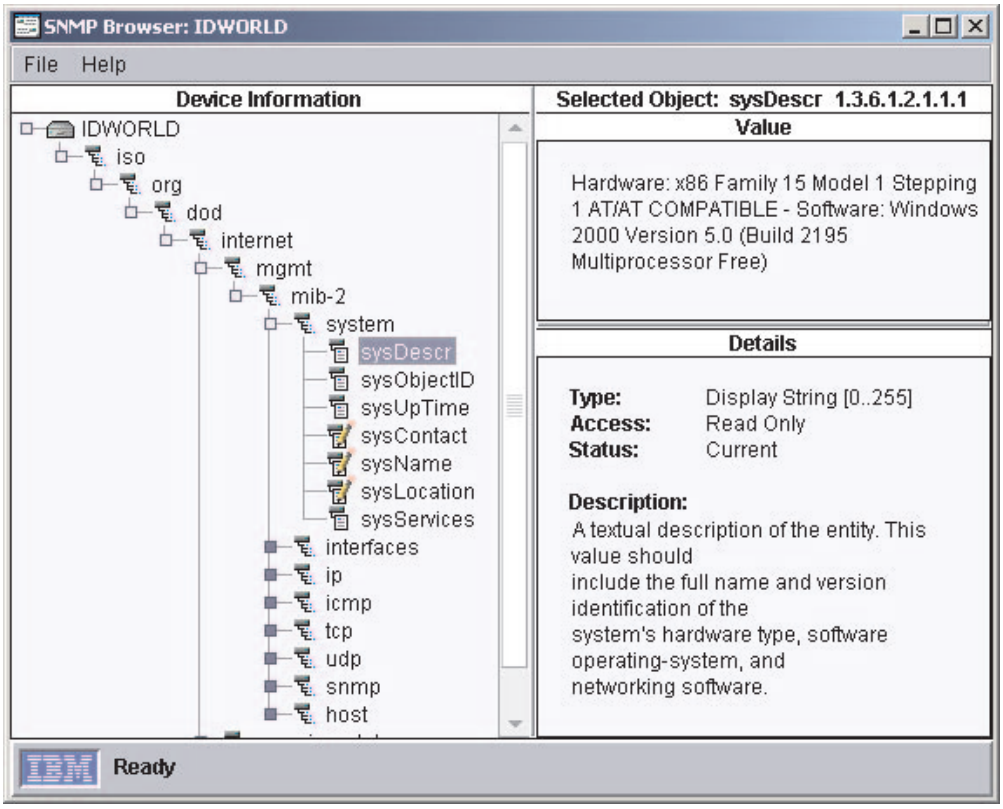

Figure 40. SNMP Browser window with a device tree expanded

The Value pane displays the value of the selected attribute. The Details pane displays the characteristics of the selected attribute, including, for example, the type and access status of the device attribute and a description of the device attribute. If a snap-in is available for the selected attribute, it is displayed in the Selected Object pane in place of the default value and characteristics information.

Setting an attribute value

You can set a user-defined value on an attribute displaying a  icon. Those attributes displaying a  icon are read-only.

To set a value for an SNMP attribute, expand the tree and select a settable attribute. The current value displays in the Value pane. Type the new value and click **Set**.

Software distribution

Using the Software Distribution task, you can import and distribute only IBM software-distribution packages to an IBM Director managed system or systems.

To use software distribution, you must understand the methods IBM Director uses to distribute software and, if you choose to use the redirected distribution method, set up file-distribution servers.

You must follow three steps to distribute software packages to IBM Director managed systems:

1. Obtain the IBM software. The most common method is using the Update*Xpress* CD.
2. Import the software to IBM Director Server and build the software-distribution package using the Package Builder.
3. Distribute the software-distribution package to the IBM Director managed system using one of these methods:
   - Streaming to the managed system from a share (or redirected distribution)
   - Streaming to the managed system from the management server

Redirected distribution

Many software packages are tens or hundreds of megabytes in size. Distributing software of this size across a large network can cause bottlenecks in network data transmission. To avoid this problem, on a server you can set up a shared subdirectory (share) that you specify in the Server Preferences window, on the **File Distribution Servers** page (see “Configuring IBM Director Server to use a file-distribution server” on page 64 for specific instructions on how to do this). You can use either an FTP-based share or a UNC-based share. IBM Director Server streams software-distribution packages to the network share. Then, they are streamed to the managed system.

Note: You cannot use a UNC-based file-distribution server with a managed system running Linux.

While redirected distribution greatly reduces the software distribution traffic in your network, it has one definite limitation. If a redirected distribution of a software-distribution package is interrupted (for example, if the network connection is lost), the installation must begin again.

To use redirected distribution to distribute software-distribution packages, IBM Director must be set up to use a file-distribution server. See “Setting up file-distribution shares” on page 64.

Streaming from the management server

Using this method, software-distribution packages are copied directly from the management server to the managed system.

Streaming from the management server has one advantage. If a network connection is broken during the transmission, IBM Director attempts to resume the connection from the point at which the transmission was interrupted. If the streaming operation can be resumed, retransmission time is saved.

You might prefer to stream a software-distribution package from the management server in the following situations:

- You have an unreliable or slow network link.
- You have a managed system connected to the IBM Director environment through a dial-up connection.

Setting up file-distribution shares

IBM Director 4.0 supports UNC-based and FTP-based file distribution software. You do not need to install IBM Director software on the file distribution server. See your server documentation for information about setting up a shared subdirectory. The share must allow full read/write access to the management server and allow read access to all managed systems.

Configuring security for UNC-based server shares

To access a share, IBM Director Agent presents a user ID and password to the server where the share is located (file-distribution server). You must configure security on the file-distribution server to authorize IBM Director Agents to access it.

You now can specify a user ID and password to access server shares using Distribution Preferences.

Configuring IBM Director Server to use a file-distribution server

Complete the following steps to configure IBM Director Server to use a file-distribution server:

1. In IBM Director Console, click **Options → Server Preferences**. The Server Preferences window opens.
2. Click the **File Distribution Server** tab. A list is displayed of all configured file-distribution servers.
3. Click **Add**. The Add Share Name window opens.
4. In the **Share Name** field, type the name of the file-distribution server using universal naming convention (UNC) notation.
5. In the **Maximum Disk Space** field, type the maximum amount of disk space (MB) that can be allocated on the file-distribution server for software distribution.
6. In the **Maximum Managed Systems** field, type the maximum number of managed systems that can receive a software distribution package at the same time.
7. To limit the bandwidth that can be used to send packages between IBM Director Server and the file-distribution server, select the **Limit bandwidth between server and share (kbps)** check box. In the entry field, type the maximum bandwidth that can be used to send packages between IBM Director Server and the file-distribution server.

   Note: You might want to limit the bandwidth when a dedicated connection, such as ISDN, is used for copying the files from IBM Director Server to the share.
8. If you specified an FTP-based server in step 4, you must type additional information in the following fields:

   User ID on FTP server
   Type a user ID authorized to access the FTP server installed on the share.

   Password
   Type the password associated with the user ID.

   Confirm password
   Confirm the password associated with the user ID.
9. Press **OK**. The Server Preferences window reopens. The data you entered in the Add Share window is now displayed.

If you have multiple file-distribution servers, repeat this procedure for each server.

Importing software and building software-distribution packages using Director Update Assistant

The Director Update Assistant is a wizard within the Software Distribution task that imports the software into IBM Director and creates the software-distribution package or packages. If you want to use the Software Distribution task to distribute drivers from Update*Xpress*, you must use this wizard to import and create software-distribution packages.

When using Update Assistant, two files are required: an XML file that describes the update, and the actual data, which is usually a software bundle. An XML file can describe one or more updates. For example, on the Update*Xpress* CD there is one XML file that describes all the updates on the CD, and an XML file for each update, so you can choose to do a bulk update, or just individual updates.

To import the software and create a software-distribution package or packages, complete the following steps:

1. In the IBM Director Console Tasks pane, double-click the **Software Distribution** task. The Software Distribution Manager window opens.

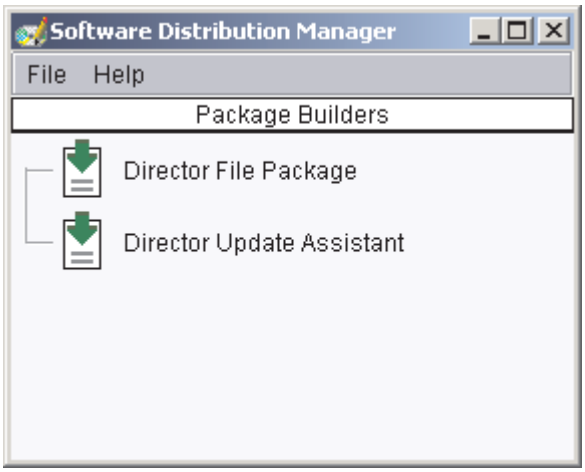

Figure 41. Software Distribution window

2. Double-click **Director Update Assistant**. The Update Assistant wizard starts.

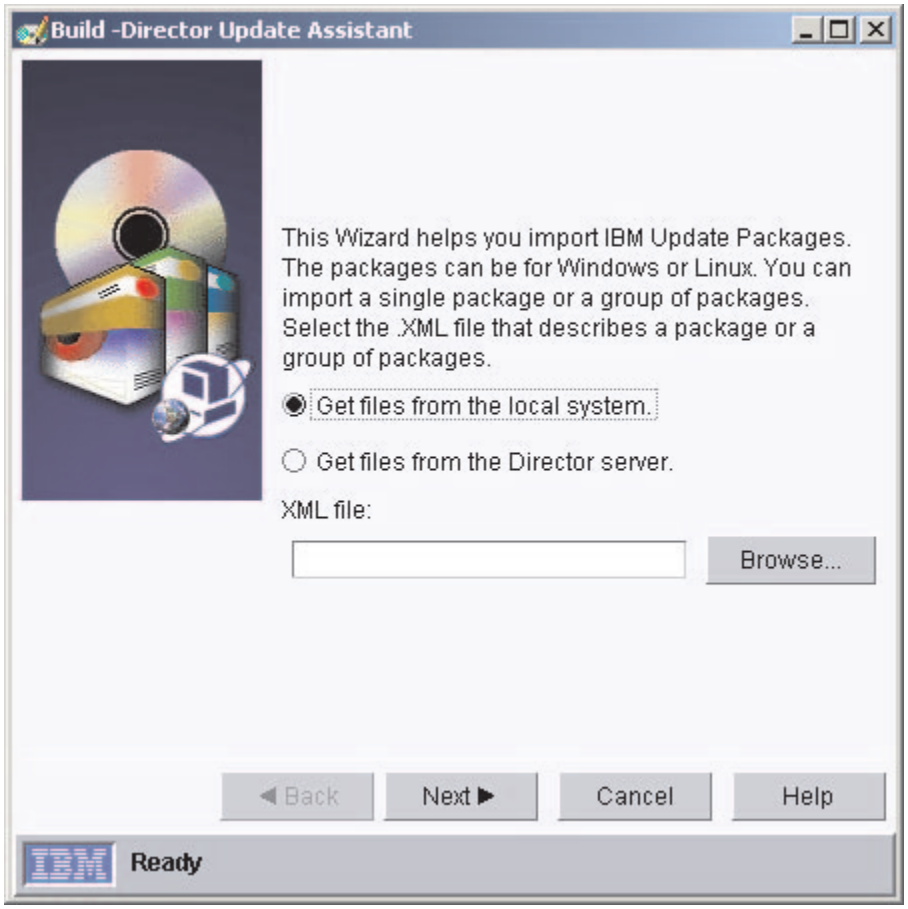

Figure 42. Director Update Assistant wizard

3. Specify whether the files reside on the local managed system or on the server on which IBM Director Server is installed by clicking the appropriate button. Then, type the location of the XML file or, click **Browse** to locate the file. Click **Next**.

   If one update package is specified in the XML file, the package is displayed in a tree structure in the Packages pane. If more than one update package is specified, a folder is displayed in the Packages pane for each managed-system type specified in the XML file. Under each folder, a list of the update packages that apply to the specific managed system is displayed.

   In the Details pane, a description of the software update selected in the Packages pane is displayed.

4. If you want to import a package, double-click the package in the Packages pane to select it. A green check mark is displayed beside all packages selected for import.

   In the Options pane, for managed systems running Windows, select the **Reboot after package installed** check box to restart (reboot) the managed system after the last package is installed. For managed systems running Windows and if the package uses InstallShield, if you want the managed system to respond to the installation other than by restarting, you can specify an alternative response file to run by typing the path name in the **Alternate response file** field. Click **Finish**.

For each update package imported, a package name is displayed in the IBM Director Console Tasks pane under **All Software Distribution Packages**. If more than one update package is imported, a software-distribution category is created for each folder that you imported. Individual software-distribution packages are displayed under a category. To edit these categories, see “Creating and editing software-distribution package categories” on page 68.

You can distribute the software package or software-package category that contains the packages you want to distribute now, or schedule a later time for distribution. See “Distributing a software package” on page 68 for more information.

Importing a software-distribution package using Director File Package wizard

The Director File Package wizard imports signed package (.bfp) format software into IBM Director. Signed packages are another way IBM uses to provide software updates. If you want to import a signed package format software-distribution package, you must use this wizard.

Complete the following steps to import a software-distribution package using this method:

1. Double-click the **Software Distribution** task in the IBM Director Console Tasks pane. The Software Distribution window opens.
2. Double-click **Director File Package**. The File Package wizard starts.

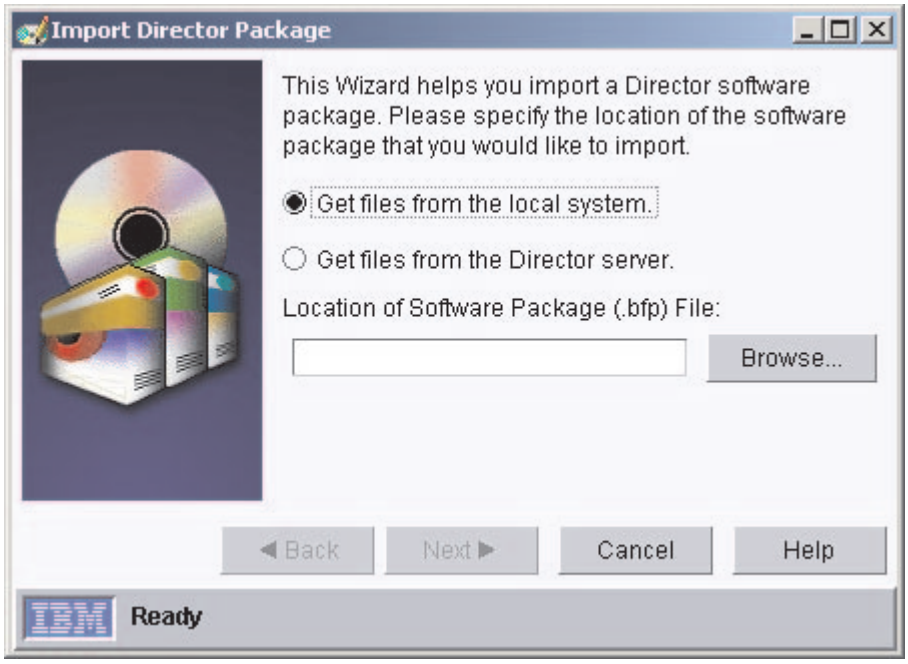

Figure 43. Director File Package wizard

3. Specify whether the files reside on the local managed system or on the server on which IBM Director Server is installed by clicking the appropriate button. Then, type the location of the BFP file, or click **Browse** to locate it. Click **Next**.
4. (Optional) Type a package category.
5. Click **Finish**.

The package name is displayed in the IBM Director Console Tasks pane under **All Software Distribution Packages**. You can distribute the software-distribution package or software-package category that contains this package now, or schedule a later time for distribution. See “Distributing a software package” for more information.

Distributing a software package

Complete the following steps to distribute a software package:

1. In the IBM Director Console Tasks pane, drag the software-distribution package or software-distribution category onto the managed system or group that you want to distribute the package to.
2. Click **Execute Now**, or click **Schedule** to schedule the distribution for a later time. (For more information about scheduling tasks, see “Scheduler” on page 51.)

Note: Group Distribution Preferences and individual managed system Distribution Preferences are independent of each other. That is, when you distribute a software package to a group, the group Distribution Preferences apply to all the managed systems within the group. If you distribute a software package to an individual managed system, the managed system Distribution Preferences apply.

Creating and editing software-distribution package categories

You can use the package category function in Software Distribution to create new categories of software-distribution packages or to edit existing categories of software-distribution packages.

To use the package category function, right-click the **Software Distribution** task and click **New Package Category**. The New Package Category window opens.

Double-clicking a package in the left pane adds the package to the category. The order in which the packages are displayed in the right pane specifies the order of delivery when that category is executed. You can modify the order in which packages are delivered by dragging a package onto the right pane. You can set the managed system to restart (reboot) between each package delivery by selecting the **Reboot Option** check box. You also can set the managed system to restart (reboot) after the last package in a category has been distributed by selecting the **Reboot at end of Category Distribution** check box.

Working with software-distribution packages

After you create a software-distribution package, you can view, edit, restrict access, export a package, and more.

Viewing package contents

You can view the contents of a software-distribution package, including the package files, the managed-system type for which the package was created, and whether a restart on the target system is set to occur after package installation.

To view the contents of a package, in the IBM Director Console Tasks pane, expand the **Software Distribution** task to view the list of software distribution packages. Then right-click the package for which you want to see the contents, and click **Package Information**. The Package Summary window opens.

Editing a package

You can edit an existing software-distribution package by double-clicking the package. The appropriate package editor for the package starts.

When you attempt to open a package, you might receive a message indicating that the package is locked by another process. This means that another user is editing the package, or it is being copied to a file-distribution server. The package remains locked until the other process is completed. However, it is possible for a package to remain locked when no process or user is using it. For example, if a computer was turned off while a package was being edited, the package will remain locked for 5 to 10 minutes.

Restricting package access

You can restrict access to a software-distribution package by specifying a user name and password combination that must be typed to gain access to the package. To enable this option, right-click the package and click **Security**.

Exporting a package

You can export a software-distribution package for use on another IBM Director Server.

Complete the following steps to export a software-distribution package:

1. Right-click a package and click **Export**. The Export Software Distribution window opens.
2. Type a file name and click **Save**.

Viewing software distribution history

Complete the following steps to view the distribution history for a selected software-distribution package:

1. In the IBM Director Console Tasks pane, expand the **Software Distribution** task to view the list of software-distribution packages.
2. Right-click the package for which you want to view the history, and click **Distribution History**. The Software Distribution History window opens.

Viewing package creation and distribution status

Using the Package Audit Log, you can determine the status of software-distribution package creation and distribution. Three levels of detail are provided to assist you in tracking and troubleshooting.

To access the log, in the IBM Director Console Tasks pane, right-click the **Software Distribution** task and click **Package Audit Log**.

Changing software-distribution server preferences

You can change your software-distribution server preferences, such as the maximum number of managed systems on which streaming can occur concurrently, streaming bandwidth, and redirected distribution options. Click **Options** → **Server Preferences**. The Server Preferences window opens. (See Figure 44 on page 70.) Click the **Software Distribution** tab. Change the appropriate selections, and then click **OK**.

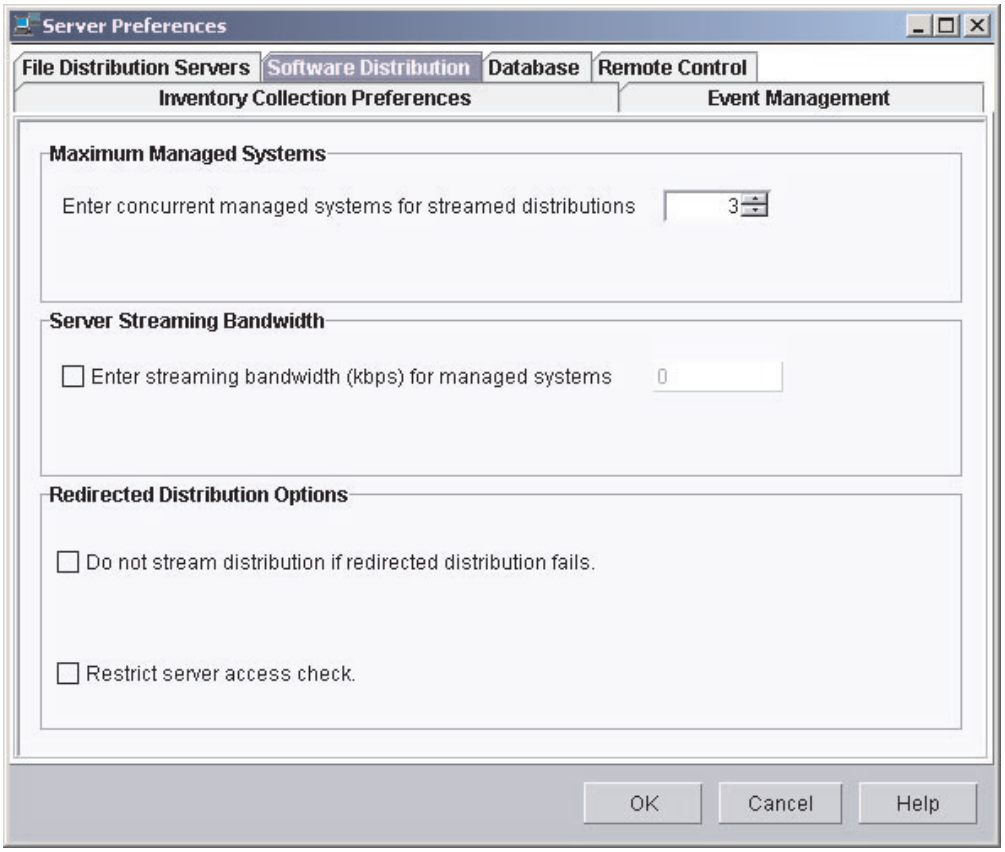

Figure 44. Server Preferences window

Viewing details about file-distribution servers and software packages

Using File Distribution Servers Manager you can view details about file-distribution servers and software packages.

To access the File Distribution Servers Manager, in the IBM Director Console Tasks pane, right-click the **Software Distribution** task; then, click **File Distribution Servers Manager**. You can perform the following tasks in the File Distribution Servers Manager window:

- View the file-distribution maintenance log by clicking **File** → **Maintenance Log**.
- Test access to the file-distribution servers by clicking **Actions** → **Test Access to All File Distribution Servers**.
- Refresh a package from the file-distribution server by clicking **Actions** → **Refresh Package on File Distribution Server**.
- Delete a package from the file-distribution server by clicking **Actions** → **Remove Package from File Distribution Server**.

Configuring software distribution preferences

Complete the following steps to configure software distribution preferences:

1. In IBM Director Console, click **Options** → **Server Preferences**. The Server Preferences window opens.
2. Click the Software Distribution tab.

3. In the **Maximum Managed Systems** field, type the maximum number of managed systems to which IBM Director Server or a file-distribution server can concurrently stream software packages. (The default value is three.)
4. To limit the bandwidth used to stream packages, select the **Enter streaming bandwidth (kbps) for managed systems** check box. In the entry field, type the bandwidth (kbps) for streaming packages from either IBM Director Server or a file-distribution server to the managed system.

   Note: To specify values less than 1 kbps, type a decimal. The minimum acceptable value is 0.25 (256 bytes per second).
5. To avoid streaming a package in the event that a redirected distribution fails, select the **Do not stream distribution if redirected distribution fails** check box.
6. Click **OK**.

Chapter 4. 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 or any related parameters
- One or more event actions, which will 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.

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 Resource Monitor thresholds, which are sent only to the management server where the thresholds are configured).
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 specific monitors
- 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 controller 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 event action plan.
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 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**.

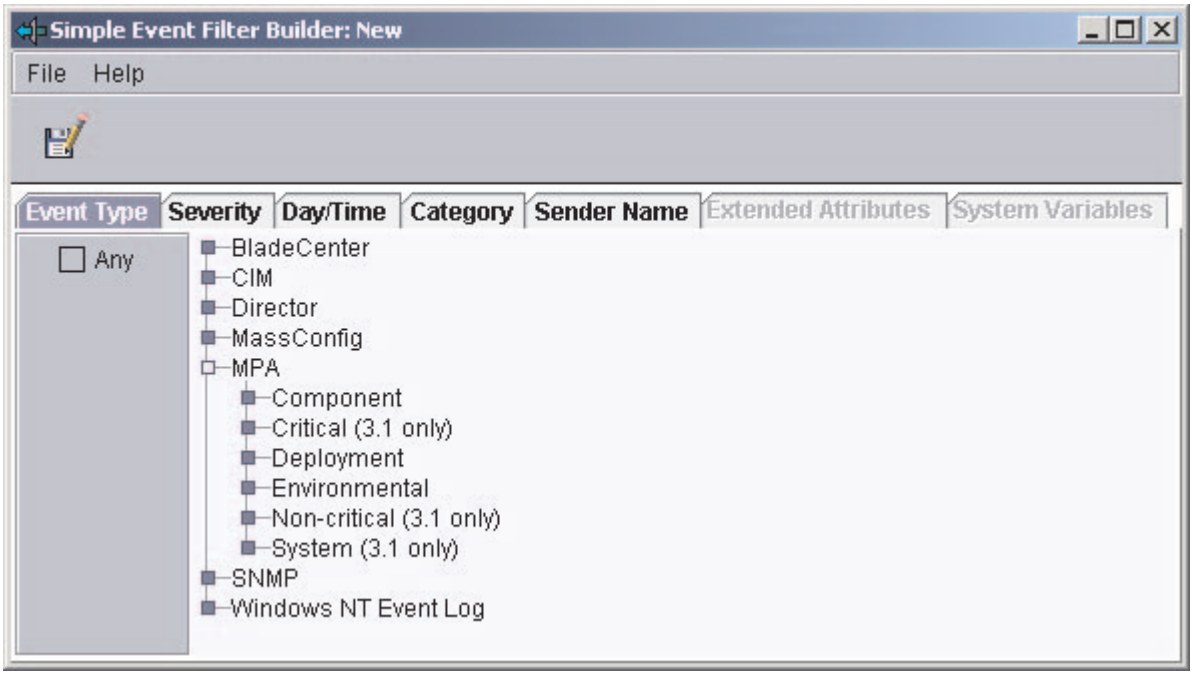

Figure 45. Simple Event Filter Builder window

Note: When you select an option, all suboptions are selected as well. For example, selecting **MPA** in the Simple Event Filter Builder window also selects all Component, Deployment, and Environmental 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 alert 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 event 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 drop-down 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 alerts, you also can manually type managed-system or 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 deselect 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 84.

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:

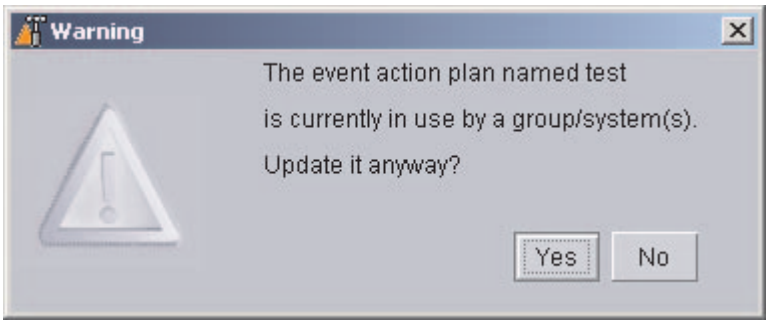

Figure 46. Prompt when modifying an existing event action plan

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 an IBM Director user.

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.

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

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 84 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. See “Event data substitution variables” on page 84 for more information.
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 47 on page 82 for example values.

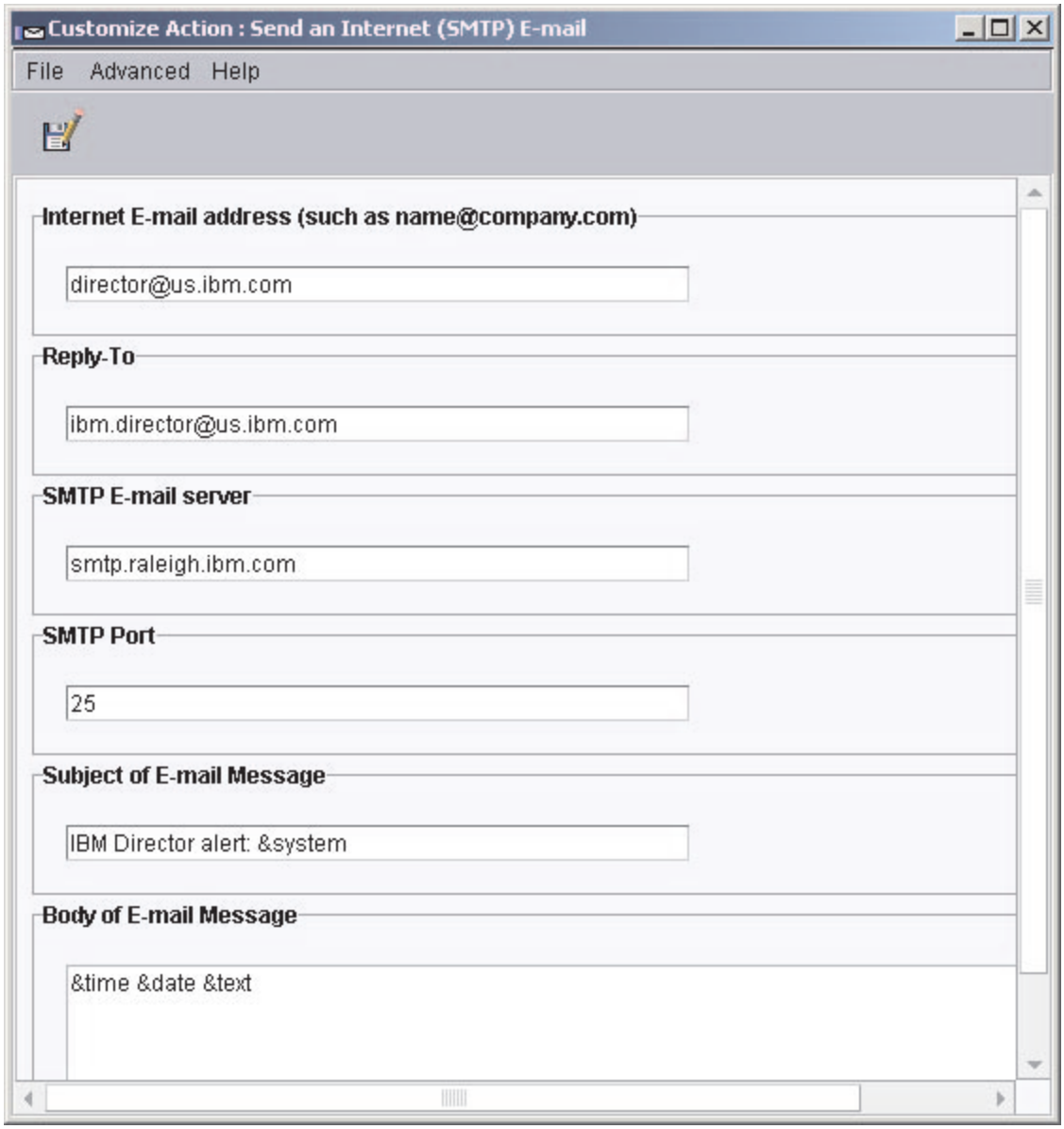

Figure 47. Customize Action window displaying example values

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.

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 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.
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.

Event	Description
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.

Variable	Description
&date	Specifies the date the event occurred.
&time	Specifies the time the event occurred.
&text	Specifies the event details, if supplied by the event.
&type	Specifies 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	Specifies the severity level of the event.
&system	Specifies the name of the managed system for which the event was generated. The system name is either the name of the IBM Director Agent, or in the case of an SNMP device, the TCP/IP address.
&sender	Specifies the name of the managed system from which the event was sent. This keyword returns null if unavailable.
&group	Specifies the group to which the target system belongs and is being monitored. This keyword returns null if unavailable.
&category	Specifies 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	Specifies a dotted representation of the event type using internal type strings.
&timestamp	Specifies the coordinated time of the event.
&rawsev	Specifies the nonlocalized string of event severity (Fatal, Critical, Minor, Warning, Harmless, Unknown).
&rawcat	Specifies the nonlocalized string of event category (Alert, Resolve).
&corr	Specifies the correlator string of the event. Related events, such as those from the same monitor-threshold activation, will match this.
&snduid	Specifies the unique ID of the event sender.
&sysuid	Specifies the unique ID of the managed system associated with the event.
&prop:*filename*#*propname*	Specifies the value of the property string *propname* from property file *filename* (relative to IBM\Director\classes).

Variable	Description
&sysvar:*varname*	Specifies the event system variable *varname*. This keyword returns null if a value is unavailable.
&slotid:*slot-id*	Specifies the value of the event detail slot with the nonlocalized ID *slot-id*.
&md5hash	Specifies the MD5 (message digest 5) hash code (CRC) of the event data (good event-specific unique ID).
&hashtxt	Specifies a full replacement for the field with an MD5 hashcode (32-character hex code) of the event text.
&hashtxt16	Specifies a full replacement for the field with a short MD5 hashcode (16-character hex code) of the event text.
&otherstring	Specifies the value of the detail slot with the localized label that matches otherstring. This keyword returns OTHERSTRING if unavailable.

Chapter 5. Solving IBM Director problems

The following table lists some of the problem symptoms and suggested solutions for IBM Director 4.0.

Symptom	Suggested action
Databases	
The Microsoft Jet database is full.	Migrate to a larger database such as IBM DB2®, Oracle, or Microsoft SQL.
Errors appear during the Database Configuration process when an Oracle database is used.	Configure and start the Oracle TCP/IP listener before starting the Database Configuration dialog. If a failure occurs, the database administrator must check the configuration of the TCP/IP listener.
Dialog boxes	
Tables appear too small in a pane.	Change the table settings to enlarge the table in the pane. **Note:** Modified table settings are not saved.
Dynamic groups criteria	

When a dynamic group is created using certain criteria such as the not equal to operator as part of the selected criteria, not all of the managed systems that do not possess that criterion are returned.	Verify that you are using the correct criteria when you create the dynamic group. Each criterion searches only the rows in the table with which it is associated. For example:
	• If you select a criterion of
	`Inventory (PC)/SCSI Device/Device Type=TAPE`
	only the managed systems that appear in at least one row in the SCSI_DEVICE table that also have a value of TAPE in the DEVICE_TYPE column are returned.
	• If you select a criterion of
	`Inventory (PC) / SCSI Device/Device Type ^= TAPE`
	only the managed systems that appear in at least one row of the SCSI_DEVICE table, of which none of those rows have a value of TAPE in the DEVICE_TYPE column, are returned. This does not necessarily return all managed systems that do not have SCSI tape drives. Only managed systems that appear in a particular table and that meet the criteria for that table are returned.

Event action plans	
Group event action plans do not appear.	Verify that a managed system or group has an event action plan assigned to it: 1. In IBM Director Console, click **Associations** → **Event Action Plans**. 2. In the Groups pane, click **All Groups**. 3. In the Group Category Contents pane, expand each group that has an event action plan applied to it to view the event action plans that are applied to the group. Event action plan associations are not displayed in the Groups pane, nor are event action plans that have been applied to a group displayed as being associated with each individual managed system that is a part of that group. The event action plan is displayed as being applied to the group only.

Symptom	Suggested action
Event log message	
An event ID 2003 warning message appears in the application event log.	If you are using Windows 2000 with Internet Information Services (IIS) installed, an event ID 2003 warning message might appear in the application event log when you start System Monitor and add counters. The event ID 2003 warning message might appear as follows: `The configuration information of the performance library "C:\WINNT\system32\w3ctrs.dll" for the "W3SVC" service does not match the trusted performance library information stored in the registry.` The functions in this library are not recognized as trusted. Microsoft previously identified that this is a problem in these products.
Field replaceable unit (FRU)	

FRU information does not appear when inventory is collected.	Verify that the FTP client (director\cimom\bin\getfru.exe) is able to reach the IBM FRU information site through your firewall. For the copy to succeed, the managed system must have firewall access through a standard FTP port. By default, it tries to reach ftp://ftp.pc.ibm.com/pub/pccbbs/bp_server on port 21. If the managed system cannot access the IBM Support FTP site, you can copy the FRU files to your network manually. Use the program getfru.exe which is in the %SystemRoot%\system32 directory. Type the following command from a command prompt:
	`getfru -s ftp.pc.ibm.com -d /pub/pccbbs/bp_server`
	
	Copy the FRU data files to a server and directory on your network. Then, write a script to retrieve these files automatically. To use the getfru.exe program in your script, observe the following syntax:
	`getfru -s <ftp_server_name> -d <directory_of_fru_files>`
	
	where:
	• *ftp_server_name* is the FTP address of the network server where you copied the FRU data files.
	• *directory_of_fru_files* is the directory that stores the FRU data files.
	
	Then, use the Process Management task to run the FRU data files located on your network. See “Process Management” on page 37 for more information. If the FRU Numbers service does not detect the presence of the FRU data files, some FRU information might be available from other sources for the FRU Numbers service to display.

Hard disk drives geometry reporting	
The following report is created indicating that an insufficient amount of space is available on a hard disk drive: `Win32_DiskDrive.Size is less than Win32_DiskPartition.Size for a removable medium that has been formatted as a single partition.`	The following hard disk drives are not supported by a Microsoft operating system: • Optical • Iomega • Jaz This is previously identified by Microsoft as a Windows Management Instrumentation (WMI) problem.

Symptom	Suggested action
IBM Director Console	
Managed systems are unavailable on the management console.	• Verify that: – The system is turned on. – IBM Director Agent is running. – The network connection is reliable. • Check or modify the network timeout value. Click **Start** → **Programs** → **IBM Director** → **Network Configuration**. • Check the network timeout value for the management server or the managed system. To change the network timeout value using: – **Windows**: Open the twgipccf.exe file, and change the timeout value. – **Linux**: In the data directory, under the products install root, edit the ServiceNodeLocal.properties file. Add `ipc.timeouts=`*x* where *x* is the specified number of seconds. The default setting is 15 seconds. If you are using UNIX or Linux and IBM Director Agent is installed in the default directory, you must restart the managed system. From a command prompt, type `/opt/IBM/director/bin/twgend -r` to stop and restart the managed system.
An input/output error connecting-to-server message appears when IBM Director Console is started.	Make sure that IBM Director Server is running before starting IBM Director Console. A green circle icon in the task bar is displayed to indicate that you can start IBM Director Console. Do not attempt to start IBM Director Console if the red diamond icon (indicating that the server is not responding) or the green triangle icon (indicating that the server is still in the process of starting) appear in the task bar.
Errors appear during attempts to log on to the management server using IBM Director Console.	Verify that: • The management server name, user ID, and password are valid. • The management server is running.
A request for access fails, and the managed systems remain locked.	• Determine whether the managed system and management server accept encrypted communications only. • Ensure that the server has encryption enabled through the Encryption Administration window. • If the managed system has a UNIX or Linux operating system, ensure that the password encryption method is set to Message Digest 5 (MD5). • Make sure that you have a connection from the management console to port 2033 on the management server.
Through the use of imaging, a system was added and appears on the management console as a duplicate of a system that was previously added.	Verify that the Unique ID attribute is enabled through the operating system.

Symptom	Suggested action
IBM Director Server	
IBM Director Server is not starting.	• Determine whether a service is failing that might prevent IBM Director Server from starting. Double-click the IBM Director icon on the task bar to determine whether there are any failing services. • Verify that the IBM Director Server service ID password and user account are valid. You must always use the same administrator password and user account for IBM Director Server and IBM Director Server service. To change the user account or password for the service, complete the following steps: 1. Click **Start** → **Programs** → **Administrative Tools**. 2. Double-click **Services**. 3. Right-click **IBM Director Server**. 4. Select **Properties**. Click **Log On**. 5. Select the **This account** check box, and modify and confirm the password. 6. Click **OK**, and then restart the IBM Director Server service.
Java® Runtime Environment (JRE) exceptions	
Intermittent JRE exceptions occur.	Verify that you have sufficient system memory. Intermittent JRE exceptions might occur when you run IBM Director Console on systems that are memory constrained. Sun Microsystems previously identified that this is a problem in some products. For more information about memory requirements, see the *IBM Director 4.0 for BladeCenter products Installation and Configuration Guide.*
SNMP browser	
Opening the SNMP browser for a device does not display the specific requested MIB.	Verify that: • IBM Director is using a community name that allows read access to the MIB that you want to view. With certain SNMP devices you can hide MIBs behind community names. • The SNMP device or agent implements the MIB in question.
SNMP devices	
SNMP devices are not being discovered.	Verify that: • The management server is running the SNMP service. If it is not, another system on the same subnet must be running an SNMP agent and must be added as a seed device. Remove the management server as the seed device. • The seed devices or other devices to be discovered are running an SNMP agent. • The community names specified in the IBM Director Discovery Preferences window allow IBM Director to read the mib-2.system table of the devices to be discovered and the mib-2.at table on seed devices. • The correct network masks have been configured for all managed systems that must be discovered. • The correct addresses have been entered for the seed devices. The most effective seed devices are routers and domain name servers. To configure these devices, from IBM Director Console, click **Options** → **Discovery Preferences**. SNMP discovery does not discover 100% of the devices. If a device has not communicated with other managed systems, the device might not be discovered.

Symptom	Suggested action
An attribute value for a MIB file cannot be changed.	Verify that: • IBM Director is using a community name that allows write access to the MIB file that has a value that you want to change. • The MIB file is writable. • The MIB file has a value you can set to be displayed in the SNMP browser. • The compiled MIB file is associated with the value to change.
When a MIB file attribute value is set to a hexadecimal, octal, or binary value, the file fails.	Verify that all values have been converted and are being added in a decimal format.
SNMP traps	
Trap destinations are missing from the SNMP agent table. **Note:** IBM Director sends and receives SNMP traps using TCP/IP only.	A table displays only the first trap destination in the SNMP configuration interface when there are multiple communities and traps associated with each community. The IBM Director CIM-based inventory stores only the first value of an array-valued property (such as the SNMP trap destination).
Security	
Load All Events does not function.	When the security log gets very large (approximately 4000 records), clicking **Load All Events** produces the `Loading data...please wait` message. After approximately 5 minutes, the message stops, and only the 30 most recent events are displayed. The **Load All Events** button is not enabled.
Software Distribution	
The software distribution package creation fails.	Check the available disk space on the management server. Packages are created on the management server before being written to the target system. If disk space is insufficient on the management server, the package creation fails.
An error message appears when a software package is distributed using a redirector share.	The error message is: `Managed System (system name) has detected that software package (package name) was not found on share (\\server\share).` You can delete software-distribution packages from the management server. The redirector cache can be maintained only through the File Distribution Server Managers interface. This is accessed by right-clicking the **Software Distribution** task. Errors occur if you manipulate the cache through any means other than IBM Director Console.
Software-distribution packages are not using the file-distribution servers.	Ensure that the file-distribution server is a member of the same domain as the management server or has a trust relationship with that domain.
The software-distribution package installation failed, and the location of the package needs to be changed.	Reinstall IBM Director Agent, and specify a different drive and directory.
Redirected software distributions are not working properly.	If Norton AntiVirus is installed on the management server, redirected distributions fail. Complete the following steps: 1. Uninstall Norton AntiVirus. 2. Delete the failed software distribution packages. 3. Recreate the packages.
Time zone	
The wrong time zone is displayed.	When the time zone is changed, a managed system does not adjust the time shown in the event viewer. Start the managed system again to show the correct time for the new time zone.

Appendix A. Resource-monitor attributes

You can use the Resource Monitor task to monitor critical system resources on managed systems. The resources that you can monitor are different depending on the operating system that is installed on the managed system. Use this table to identify the resource-monitor attributes that you want to monitor if you are:

- Planning your IBM Director installation or configuration
- Adjusting your resource-monitoring strategy

Resource monitor data-collection rates vary depending on the managed system or device. In general, using the default settings, data collections occur every 5 to 10 seconds, and the display refreshes every 10 to 20 seconds.

Note: (Windows only) The attributes for the following resource monitors can vary depending on the features and functions you have configured on the managed system:

- CIM monitors
- DMI monitors
- Device, performance, and service monitors
- Registry monitors

To view the resource-monitor attributes available for a particular managed system or device, see “Viewing all resource-monitor thresholds” on page 47.

When referring to this table, be sure to select the applicable column for the operating system installed on the managed system. For more information about resource monitors, see “Resource Monitors” on page 43.

Attribute	Windows 2000	Linux
CPU monitor		
CPU utilization	X	X
CPU ’x’ utilization (on SMP devices)	X	
Process count	X	X
Thread count		
Disk monitor **Notes:** 1. The disk drive monitor attributes are repeated for each local nonremoveable logical drive found. 2. (Linux only) The list of file-system attributes is displayed first; then, the disk monitor attributes are displayed under each file system.		
Disk 1 workload	X	
Drive C: % space used	X	
Drive C: Space remaining	X	
Drive C: Space used	X	
Blocks available		X
Blocks used		X
Inodes available		X
Inodes used		X

Attribute	Windows 2000	Linux
Percentage blocks available		X
Percentage blocks used		X
Percentage Inodes available		X
Percentage Inodes used		X
Percentage space available		X
Percentage space used		X
Space available (MB)		X
Space used (MB)		X
Volume SYS: space remaining		X
Volume SYS: space used		X
File monitor File monitor attributes can be files or directories. See the rows for the applicable file monitor attributes. **Notes:** 1. For compatible file-system types, the “Directory exists” or “File exists” attribute (depending on which is applicable) is always valid data. 2. (Linux only) If there are additional directories, additional subelements are displayed. 3. (Linux only) Directories can contain hundreds of subelements. If so, a directory might take 5 seconds or longer to open.		
Directory		
Directory exists	X	X
Last modified	X	X
Directory attributes		X
Directory owner		X
Directory size (bytes)		X
Last modified		X
Object type		X
File		
Checksum	X	X
File exists	X	X
File size	X	
Last modified	X	X
File attributes		X
File owner		X
File size (bytes)		X
Object type		X
File system monitor		
/		X
/bin		X
/dev		X
/etc		X
/home		X

Attribute	Windows 2000	Linux
/lib		X
/lost+found		X
/sbin		X
/tmp		X
/usr		X
/var		X
List of directory contents		
Directory attributes		X
Directory exists		X
Directory owner		X
Directory size (bytes)		X
Last modified		X
Object type		X
Memory monitor		
Locked memory	X	
Memory usage	X	
Available (bytes)		X
Used (bytes)		X
Cache blocks in use		
Percent of cache in use		
TCP/IP monitor		
Interface *x* - Broadcast packets received	X	
Interface *x* - Broadcast packets sent	X	
Interface *x* - Bytes received	X	
Interface *x* - Bytes sent	X	
Interface *x* - Unicast packets received	X	
Interface *x* - Unicast packets sent	X	
IP packets received	X	
IP packets received with errors	X	
IP packets sent	X	
TCP connections	X	
UDP datagrams received	X	
UDP datagrams sent	X	
Process monitor **Note:** The number of applications or executable files that a process monitor checks can vary. The IBM Director user configures the processes monitored using the Process Monitor task in IBM Director Console. Each of the process monitor attributes is displayed for each executable file that is monitored.		
Current active processes	X	X
Maximum running at once	X	X
Maximum running yesterday	X	X
New executions counted	X	X
Times failed to start	X	X

Attribute	Windows 2000	Linux
Time started	X	X
Time stopped	X	X
Total execution time	X	X
Yesterday's execution time	X	X
Yesterday's new executions	X	X

Appendix B. Terminology summary and abbreviation list

This appendix provides a summary of IBM Director terminology and a list of abbreviations 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 *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	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
CSV	comma-separated value
DBCS	double-byte character set
DES	data encryption standard
DIMM	dual inline memory module
DMI	Desktop Management Interface
DNS	Domain Name System
EEPROM	electrically erasable programmable read-only memory
FRU	field replaceable unit
FTMI	fault tolerant management interface

Abbreviation	Definition
GB	gigabyte
Gb	gigabit
GUI	graphical user interface
GUID	globally unique identifier
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPX	internetwork packet exchange
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
LAN	local area network
LED	light-emitting diode
MAC	media access control
MB	megabyte
Mb	megabit
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
NIC	network interface card
NNTP	Network News Transfer Protocol
NVRAM	nonvolatile random access memory
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PFA	Predictive Failure Analysis
RAM	random access memory
RDM	Remote Deployment Manager
RPM	Red Hat Package Manager
SID	Security identifier

Abbreviation	Definition
SMBIOS	System Management BIOS
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
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
UIM	Upward Integration Module
UNC	universal naming convention
UUID	universal unique identifier
VPD	vital product data
VRM	voltage regulator module
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation

Appendix C. 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:

- Use the troubleshooting information in your system and software 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/. If you click **Profile** from the support page, you can create a customized support page. The support page has many sources of information and ways for you to solve problems, including:

- Diagnosing problems, using the IBM Online Assistant
- Downloading the latest device drivers and updates for your products
- Viewing Frequently Asked Questions (FAQ)
- Viewing hints and tips to help you solve problems
- Participating in IBM discussion forums
- Setting up e-mail notification of technical updates about your products

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.

Appendix D. Notices

This publication 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 jurisdictions 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 publication 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

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Trademarks

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

BladeCenter	Predictive Failure Analysis
DB2	Redbooks
e-business logo	ServeRAID
IBM	TotalStorage
IntelliStation	Update*Xpress*
Light Path Diagnostics	Wake on LAN
Netfinity	xSeries
NetView	

Lotus and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT 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.

Linux is a registered trademark of Linus Torvalds.

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

Index

Part Number: 01R0514

Printed in U.S.A.

(1P) P/N: 01R0514

SC01-R051-40