

IBM Director 4.1



# Systems Management Guide

**Note:** Before using this information and the product it supports, be sure to read the general information in Appendix E, "Notices", on page 223.

**First Edition (March 2003)**

**© Copyright International Business Machines Corporation 2003. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Figures</b> . . . . .	ix
<b>Tables</b> . . . . .	xi
<b>Preface</b> . . . . .	xiii
How this book is organized . . . . .	xiii
Notices that are used in this book . . . . .	xiv
IBM Director publications . . . . .	xiv
IBM Director resources on the World Wide Web . . . . .	xv
<b>Chapter 1. Introducing IBM Director 4.1</b> . . . . .	1
IBM Director environment . . . . .	1
IBM Director components . . . . .	2
IBM Director Server . . . . .	3
IBM Director Agent . . . . .	4
IBM Director Console . . . . .	4
IBM Director Agent features . . . . .	5
ServeRAID Manager . . . . .	5
Management Processor Assistant Agent . . . . .	5
IBM Director Remote Control Agent (Windows only) . . . . .	5
Web-based Access (Windows only) . . . . .	5
Web-based Access help files (Windows only) . . . . .	5
System Health Monitoring (Windows only) . . . . .	5
SNMP Access and Trap Forwarding . . . . .	6
Upgrading from previous releases of IBM Director . . . . .	6
IBM Director extensions . . . . .	6
IBM Director Server Plus Pack . . . . .	6
IBM Director Software Distribution Premium Edition . . . . .	8
IBM Director Remote Deployment Manager 4.10 . . . . .	8
Additional IBM Director extensions . . . . .	9
<b>Chapter 2. Understanding IBM Director Console</b> . . . . .	11
Understanding the IBM Director Console interface . . . . .	11
Starting tasks . . . . .	12
Managed systems and managed objects . . . . .	12
Groups . . . . .	13
Associations . . . . .	19
Events and alerts . . . . .	20
Event action plans . . . . .	20
Implementing an event action plan . . . . .	21
Viewing and changing system variables . . . . .	25
Enabling and viewing an event action history . . . . .	26
Viewing event action plan associations . . . . .	26
Restricting event action plans . . . . .	26
Exporting event action plans . . . . .	26
Importing event action plans . . . . .	27
Scheduler . . . . .	27
Starting Scheduler . . . . .	28
Viewing information about scheduled jobs . . . . .	33
Viewing job properties . . . . .	35
Viewing scheduled job history information . . . . .	35
Viewing execution history logs . . . . .	35
Message Browser . . . . .	36

User Administration . . . . .	36
Encryption administration . . . . .	37
<b>Chapter 3. Working with managed systems using IBM Director Console</b>	
<b>tasks</b> . . . . .	39
IBM Director Console tasks and BladeCenter products . . . . .	39
Active PCI Manager . . . . .	40
Fault Tolerant Management Interface (FTMI) . . . . .	41
Slot Manager . . . . .	45
Asset ID . . . . .	53
BladeCenter Assistant . . . . .	54
Starting the BladeCenter Configuration or BladeCenter Management subtask	54
BladeCenter Configuration subtask . . . . .	55
BladeCenter Management subtask . . . . .	57
Deployment wizard . . . . .	60
Switch Management LaunchPad subtask . . . . .	60
Capacity Manager. . . . .	60
Viewing and activating monitors. . . . .	60
Identifying bottlenecks . . . . .	61
Receiving automatic notification of a bottleneck . . . . .	63
Generating a report . . . . .	64
Viewing report details . . . . .	68
Saving and printing a report . . . . .	68
Viewing previously generated reports. . . . .	69
Predicting future performance . . . . .	69
Viewing a performance forecast graph . . . . .	70
Changing settings . . . . .	71
CIM Browser. . . . .	71
Starting the CIM Browser task . . . . .	71
Viewing information in the CIM Browser. . . . .	72
Setting a property value for a CIM class instance . . . . .	72
Executing a method for a CIM class instance. . . . .	73
Creating shortcuts to classes and methods . . . . .	73
Configure Alert Standard Format . . . . .	74
DMI Browser. . . . .	74
Starting the DMI Browser task . . . . .	75
Viewing component information in the DMI Browser . . . . .	75
Setting an attribute value for a DMI group . . . . .	75
Creating a group class shortcut . . . . .	75
Event action plans . . . . .	76
Event Log. . . . .	76
Viewing and changing display options . . . . .	77
Exporting events from the event log . . . . .	77
File Transfer . . . . .	77
Starting the File Transfer task . . . . .	77
Transferring files between managed systems . . . . .	79
Synchronizing files, directories, or drives . . . . .	79
Hardware Status . . . . .	80
Inventory . . . . .	82
Viewing inventory data . . . . .	83
Exporting inventory query results to a file . . . . .	85
Viewing and editing the inventory software dictionary . . . . .	85
Management Processor Assistant . . . . .	88
Starting the Management Processor Assistant task . . . . .	88
Communications Configuration subtask . . . . .	90
Management Processor Configuration subtask . . . . .	91

Server Management subtask . . . . .	92
Microsoft Cluster Browser . . . . .	94
Starting the Microsoft Cluster Browser task . . . . .	94
Process Management . . . . .	96
Viewing and working with processes, services, and device-services information . . . . .	96
Creating and applying a process monitor . . . . .	98
Removing process monitors . . . . .	99
Viewing process monitors . . . . .	99
Creating and running process tasks . . . . .	99
Issuing a command on a managed system . . . . .	100
Restricting anonymous command execution . . . . .	101
Rack Manager . . . . .	102
Starting the Rack Manager task . . . . .	102
Starting a component association . . . . .	104
Canceling a component association . . . . .	104
Creating and configuring a rack . . . . .	104
Adding components to an existing rack . . . . .	105
Removing a rack component . . . . .	105
Remote Control . . . . .	106
Starting a remote-control session . . . . .	106
Changing remote-control states . . . . .	107
Changing the refresh rate . . . . .	107
Recording a remote-control session . . . . .	107
Playing a recorded remote-control session . . . . .	107
Restricting remote-control usage . . . . .	107
Sending key combinations . . . . .	108
Remote Session . . . . .	108
Resource Monitors . . . . .	109
Viewing available resource monitors . . . . .	109
Setting a resource-monitor threshold . . . . .	110
Viewing all resource-monitor thresholds . . . . .	113
Recording a resource monitor . . . . .	113
Viewing a graph of a resource-monitor recording . . . . .	115
Exporting a resource-monitor recording . . . . .	116
Monitoring the same resource on multiple groups or managed systems . . . . .	116
Exporting and importing threshold tasks . . . . .	116
Viewing resource-monitor data on the ticker tape . . . . .	117
Scheduler . . . . .	117
ServeRAID Manager . . . . .	117
Starting the ServeRAID Manager task . . . . .	117
Viewing system or device information . . . . .	118
Viewing ServeRAID alerts . . . . .	118
Locating defunct disk drives . . . . .	118
SNMP devices . . . . .	118
Setting discovery parameters . . . . .	119
Creating a new SNMP device . . . . .	119
Using the SNMP Browser . . . . .	120
Software Distribution . . . . .	121
Understanding software distribution . . . . .	122
Importing software and building software packages . . . . .	123
Importing a previously created software package using Director File Package wizard (Premium Edition only) . . . . .	133
Distributing a software package . . . . .	133
Creating and editing software-package categories . . . . .	134
Working with software packages . . . . .	135

Changing software-distribution server preferences . . . . .	136
Viewing details about file-distribution servers and software packages . . . . .	137
Software Rejuvenation . . . . .	138
Starting the Software Rejuvenation task . . . . .	139
Configuring a service rejuvenation . . . . .	139
Scheduling a software rejuvenation . . . . .	140
Editing a rejuvenation schedule . . . . .	141
Deleting a rejuvenation schedule . . . . .	142
Creating a schedule filter. . . . .	142
Setting rejuvenation options for all managed systems . . . . .	143
Starting the Prediction Configuration wizard . . . . .	143
Viewing resource utilization . . . . .	145
Creating an event filter for software-rejuvenation events . . . . .	145
Using keyboard shortcuts . . . . .	146
System Accounts . . . . .	146
System Availability . . . . .	147
Starting the System Availability task. . . . .	147
Changing the graph dates . . . . .	149
Changing the settings criteria . . . . .	149
Saving the system-availability report . . . . .	150
<b>Chapter 4. Event management . . . . .</b>	<b>151</b>
Planning and designing event action plan implementations . . . . .	151
Grouping managed systems . . . . .	152
Structuring event action plans . . . . .	152
Structuring event filters . . . . .	153
Building an event action plan . . . . .	153
Event filters. . . . .	154
Creating an event filter . . . . .	155
Modifying an event action plan . . . . .	158
Event actions . . . . .	158
Available event action types . . . . .	161
Event data substitution variables . . . . .	162
<b>Chapter 5. Working with management servers using the command-line interface (DIRCMD) . . . . .</b>	<b>165</b>
Installing and accessing DIRCMD . . . . .	165
DIRCMD syntax . . . . .	165
Management . . . . .	166
Options . . . . .	166
Server-management bundle. . . . .	168
Managed-system bundle . . . . .	172
Event-management bundle . . . . .	173
Resource-monitor bundle. . . . .	175
Process-monitor bundle . . . . .	176
SNMP-device bundle . . . . .	177
<b>Chapter 6. Working with managed systems using Web-based Access (Windows only) . . . . .</b>	<b>181</b>
Starting Web-based Access. . . . .	181
Starting Web-based Access using a Web browser . . . . .	181
Starting Web-based Access using MMC . . . . .	183
Understanding the Web-based Access interface . . . . .	184
Viewing Hardware Status using the Director page . . . . .	185
Viewing managed-system information using the Information page . . . . .	186
Inventory services . . . . .	187

Monitor services . . . . .	191
System services . . . . .	194
Working with managed systems using the Tasks page . . . . .	195
Configuration . . . . .	196
Tools . . . . .	200
Web Links . . . . .	200
<b>Chapter 7. Solving IBM Director problems . . . . .</b>	<b>201</b>
<b>Appendix A. Resource-monitor attributes . . . . .</b>	<b>211</b>
<b>Appendix B. Obtaining FRU data files using the GETFRU command . . . . .</b>	<b>215</b>
<b>Appendix C. Terminology summary and abbreviation list . . . . .</b>	<b>217</b>
IBM Director terminology summary . . . . .	217
Abbreviation and acronym list . . . . .	217
<b>Appendix D. Getting help and technical assistance . . . . .</b>	<b>221</b>
Before you call . . . . .	221
Using the documentation . . . . .	221
Getting help and information from the World Wide Web . . . . .	221
Software service and support . . . . .	222
<b>Appendix E. Notices . . . . .</b>	<b>223</b>
Edition notice . . . . .	223
Trademarks . . . . .	224
<b>Glossary . . . . .</b>	<b>225</b>
<b>Index . . . . .</b>	<b>235</b>





---

# Figures

1. Hardware in an IBM Director environment . . . . .	2
2. Software in an IBM Director environment . . . . .	3
3. IBM Director Console interface . . . . .	11
4. IBM Director Console toolbar . . . . .	12
5. A selected group listed in the Group Contents pane . . . . .	14
6. Dynamic Group Editor window . . . . .	15
7. Task Based Group Editor window . . . . .	16
8. Static Group Editor window . . . . .	17
9. Category Editor window . . . . .	18
10. Group Import window . . . . .	19
11. Event Action Plan Builder window . . . . .	21
12. Simple Event Filter Builder window . . . . .	23
13. Customize Action window for ticker-tape alert . . . . .	24
14. Example of an event action plan with an event filter and event action assigned to it . . . . .	25
15. Scheduler window . . . . .	28
16. New Scheduled Job window . . . . .	29
17. Repeat window . . . . .	30
18. Options page in New Scheduled Job window . . . . .	31
19. New Scheduled Job window, when you opt to schedule a task that is activated by dragging it onto a managed system . . . . .	33
20. Selecting a job type in the left pane on the Jobs page in the Scheduler window . . . . .	34
21. Selecting a specific job execution in the left pane on the Jobs page in the Scheduler window . . . . .	35
22. Encryption Administration window . . . . .	37
23. Fault Tolerant Management Interface window . . . . .	42
24. Slot Manager window using Slot view . . . . .	46
25. Slot Manager window using Tree View . . . . .	47
26. Slot Manager window using Table View . . . . .	48
27. Examples of slot error status . . . . .	49
28. Asset ID window . . . . .	53
29. Management Processor Assistant window when activating the BladeCenter Management subtask . . . . .	55
30. Monitor Activator window . . . . .	61
31. Simple Event Filter Builder window . . . . .	64
32. Report Definitions window . . . . .	65
33. Report Viewer window . . . . .	66
34. Lower-right pane in the Report Viewer window displaying a performance forecast graph . . . . .	70
35. CIM Browser window . . . . .	72
36. Event Log showing all events for all managed systems . . . . .	76
37. File Transfer window . . . . .	78
38. File Transfer window when target managed system has IBM Director Agent 3.1 installed . . . . .	78
39. IBM Director Console displaying hardware status groups . . . . .	80
40. Hardware status icons located in the bottom-right portion of IBM Director Console . . . . .	80
41. Hardware Status window showing all hardware status events . . . . .	81
42. Hardware Status window showing events for a single managed system . . . . .	82
43. Inventory Query Browser window . . . . .	83
44. Inventory Query Builder window . . . . .	84
45. Inventory Software Dictionary Editor window . . . . .	86
46. Management Processor Assistant window when activating the Server Management subtask . . . . .	89
47. Microsoft Cluster Browser window . . . . .	95
48. Microsoft Cluster Browser window showing the status of a cluster . . . . .	95
49. Microsoft Cluster Browser window showing cluster resource details . . . . .	96
50. Process Management window . . . . .	97
51. Process Monitors window . . . . .	98
52. Process Task window . . . . .	100

53. Execute Command window . . . . .	101
54. Rack Manager window . . . . .	103
55. Remote Control window . . . . .	106
56. Remote Session window for a managed system running Windows . . . . .	109
57. Resource Monitors window for a managed device . . . . .	110
58. System Threshold window for setting numeric thresholds. . . . .	111
59. System Threshold window for setting text threshold strings . . . . .	112
60. Resource Monitors window. . . . .	114
61. The Resource Monitor Recording window . . . . .	114
62. New Record window . . . . .	115
63. ServeRAID Manager window . . . . .	118
64. SNMP Browser window . . . . .	120
65. SNMP Browser window with a device tree expanded . . . . .	121
66. Software Distribution Manager window (Standard Edition) . . . . .	123
67. Software Distribution Manager window (Premium Edition) . . . . .	124
68. Director Update Assistant wizard . . . . .	124
69. About InstallShield window. . . . .	126
70. InstallShield Package wizard . . . . .	127
71. Microsoft Windows Installer Package wizard . . . . .	129
72. RPM Package wizard. . . . .	130
73. Create Custom Package window . . . . .	132
74. Director File Package wizard . . . . .	133
75. New Package Category window . . . . .	134
76. Server Preferences window . . . . .	137
77. File Distribution Servers Manager . . . . .	138
78. Software Rejuvenation window . . . . .	139
79. Service Rejuvenation window. . . . .	140
80. Repeat Schedule window . . . . .	141
81. Schedule Filter window . . . . .	142
82. Rejuvenation Options window. . . . .	143
83. Prediction Configuration wizard . . . . .	144
84. System Accounts window . . . . .	147
85. System Availability window. . . . .	148
86. Settings window. . . . .	149
87. Simple Event Filter Builder window. . . . .	156
88. Prompt when modifying an existing event action plan . . . . .	158
89. Customize Action window displaying example values . . . . .	160
90. Web-based Access user interface . . . . .	184
91. Director page in the left pane . . . . .	185
92. Hardware Status pane . . . . .	186
93. Information page in the left pane . . . . .	187
94. Task services in the left pane . . . . .	196

---

## Tables

1. IBM Director tasks and the BladeCenter components you can use them on . . . . .	39
2. FTMI CIM queries . . . . .	45
3. Performance analysis icon descriptions . . . . .	67
4. Resource-monitor status icons . . . . .	113
5. Event action types . . . . .	161
6. Event data substitution variables . . . . .	162
7. Management commands . . . . .	166
8. DIRCMD options . . . . .	166
9. Server-management bundle syntax. . . . .	168
10. Managed-system bundle syntax . . . . .	172
11. Event-management bundle syntax . . . . .	174
12. Resource-monitor bundle syntax. . . . .	175
13. Process-monitor bundle syntax . . . . .	176
14. SNMP-device bundle syntax . . . . .	178
15. Solving IBM Director problems . . . . .	201
16. Resource-monitor attributes . . . . .	211
17. Abbreviations and acronyms used in IBM Director . . . . .	217



---

## Preface

This book provides instructions for using IBM® Director 4.1 for systems-management tasks. IBM Director consists of the following tools to meet your systems-management needs:

- IBM Director Console is the graphical user interface (GUI) for IBM Director Server. Using IBM Director Console, system administrators can conduct comprehensive systems management using either a drop-and-drag action or a single click.
- Command Line Interface (DIRCMD) is the command-line interface for IBM Director Server. System administrators can use a command-line prompt to access, control, and gather information from IBM Director Server.
- Web-based Access provides access to managed systems using either a Web browser or the Microsoft Management Console (MMC). System administrators can access a managed system and view real-time asset and health information about the managed system.

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

---

## How this book is organized

Chapter 1, “Introducing IBM Director 4.1”, on page 1, contains an overview of IBM Director, including its components, features, and extensions.

Chapter 2, “Understanding IBM Director Console”, on page 11, details the basic functionality of IBM Director Console, including group creation and management, event action plans, and Scheduler.

Chapter 3, “Working with managed systems using IBM Director Console tasks”, on page 39, describes the tasks that you can perform using IBM Director Console.

Chapter 4, “Event management”, on page 151, contains information about planning, designing, and building event action plan implementations.

Chapter 5, “Working with management servers using the command-line interface (DIRCMD)”, on page 165, describes the tasks that you can perform using the command-line interface to IBM Director Server.

Chapter 6, “Working with managed systems using Web-based Access (Windows only)”, on page 181, contains information about using Web-based Access to view real-time asset and health information on a managed system.

Chapter 7, “Solving IBM Director problems”, on page 201, lists solutions to problems you might encounter with IBM Director.

Appendix A, “Resource-monitor attributes”, on page 211, details the resource-monitor attributes available when using the Resource Monitors task.

Appendix B, “Obtaining FRU data files using the GETFRU command”, on page 215, details how to obtain field-replaceable unit (FRU) data files using the GETFRU command on managed systems.

Appendix C, “Terminology summary and abbreviation list”, on page 217, contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

Appendix D, “Getting help and technical assistance”, on page 221, contains information about accessing IBM Support Web sites for help and technical assistance.

Appendix E, “Notices”, on page 223, contains product notices and trademarks.

The glossary on page 225 provides definitions for terms used in IBM Director publications.

---

## 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 4.1 Installation and Configuration Guide* (dir41\_install.pdf)
- *IBM Director 4.1 Systems Management Guide* (dir41\_sysmgt.pdf)

You also can obtain these publications from the IBM Support Web site. The *IBM Director 4.1 Events Reference* is available from the Web site only. Check this Web site regularly for new or updated IBM Director publications. For additional information about downloading materials from the IBM Support Web site, see “IBM Director resources on the World Wide Web” on page xv.

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

- *Advanced System Management PCI Adapter, Software User's Guide*
- *Advanced System Management PCI Adapter, Installation Instructions*
- *Remote Supervisor Adapter, User's Guide*
- *Remote Supervisor Adapter, Installation Guide*
- *Remote Supervisor Adapter II, User's Guide*
- *Remote Supervisor Adapter II, Installation Guide*

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

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

- *Implementing Systems Management Solutions using IBM Director* (SG24-6188-01)
- *IBM @server BladeCenter Systems Management* (REDP3582)
- *The Cutting Edge: IBM @server BladeCenter* (REDP3581)

- *IBM eServer BladeCenter Type 8677 Planning and Installation Guide (SG24-6196-00)*
- *IBM eServer xSeries 440 Planning and Installation Guide (SG24-6196-00)*
- *Server Consolidation with the IBM eServer xSeries 440 and VMware ESX Server (SG24-6852-00)*
- *Managing IBM TotalStorage NAS with IBM Director (SG24-6830-00)*
- *IBM Director Security (REDPO417)*
- *Integrating IBM Director with Enterprise Management Solutions (SG24-5388-01)*
- *Using Active PCI Manager (REDP0446)*
- *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](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](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.

### 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 ServerProven<sup>®</sup> page**

<http://www.ibm.com/pc/us/compat/index.html>

This Web page provides information about IBM hardware compatibility with IBM Director 4.1.

**IBM Director Agent page**

[http://www.ibm.com/pc/ww/eserver/xseries/systems\\_management/nfdir/agent.html](http://www.ibm.com/pc/ww/eserver/xseries/systems_management/nfdir/agent.html)

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

**IBM Support page**

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

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

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<sup>®</sup>, 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 UpdateXpress<sup>™</sup> to update your server, on the right click **UpdateXpress CD** for the latest release of UpdateXpress.



---

## Chapter 1. Introducing IBM Director 4.1

IBM Director is a comprehensive systems-management solution. Based on industry standards, it can be used with most Intel-microprocessor-based systems. IBM Director has features designed expressly to work with the hardware in the following currently marketed IBM systems and products:

- IBM @server™ xSeries™ servers
- IBM @server BladeCenter™ chassis
- IBM @server blade servers
- IBM NetVista™ desktop computers
- IBM IntelliStation® workstations
- IBM ThinkPad® mobile computers
- IBM TotalStorage™ Network Attached Storage (NAS) products
- IBM SurePOS™ point-of-sale systems

A powerful suite of tools and utilities, IBM Director automates many of the processes required to manage systems proactively, including capacity planning, asset tracking, preventive maintenance, diagnostic monitoring, troubleshooting, and more. It has a graphical user interface that provides easy access to both local and remote systems.

IBM Director can be used in environments with multiple operating systems (heterogeneous environments) and integrated with robust workgroup and enterprise management software from IBM (such as Tivoli®), Computer Associates, Hewlett-Packard, Microsoft, NetIQ, and BMC Software.

---

### IBM Director environment

IBM Director is designed to manage a complex environment that contains numerous servers, desktop computers, workstations, mobile computers (notebook computers), and assorted devices. IBM Director can manage up to 5,000 systems.

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*.
- Servers, workstations, desktop computers, and mobile computers that are managed by IBM Director. Such systems are called *managed systems*.
- Network devices, printers, or computers that have SNMP agents installed or embedded. Such devices are called *SNMP devices*.

Figure 1 shows the hardware in an IBM Director environment.

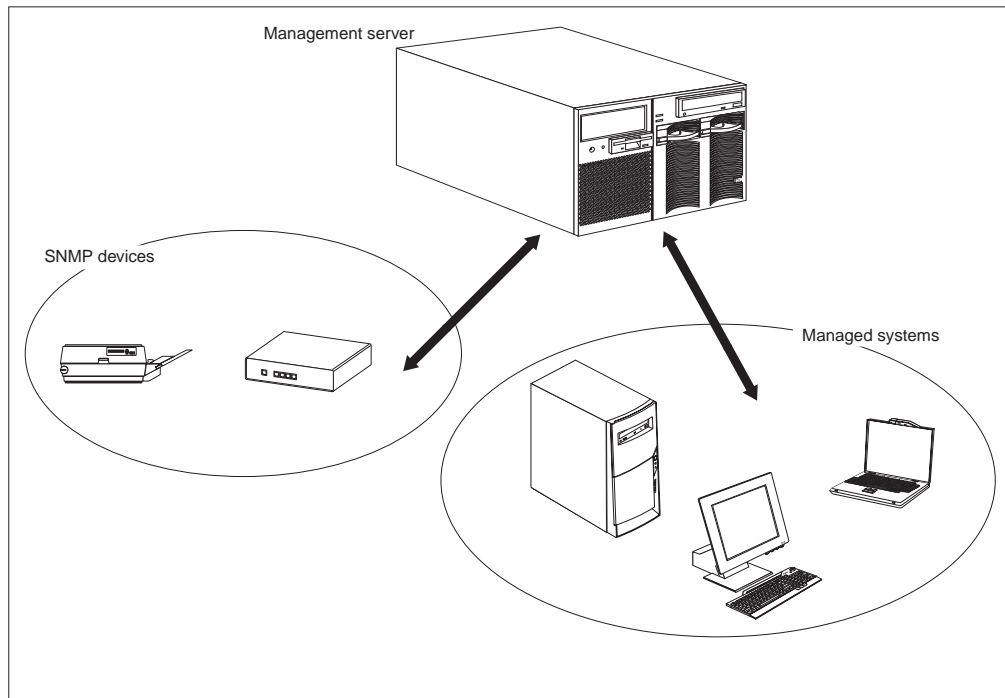


Figure 1. Hardware in an IBM Director environment

For information about IBM hardware supported by IBM Director 4.1, see the hardware compatibility list located on the IBM ServerProven Web site at [www.ibm.com/eserver/xseries/serverproven](http://www.ibm.com/eserver/xseries/serverproven).

---

## IBM Director components

The IBM Director software has three components:

- IBM Director Server
- IBM Director Agent
- 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 a 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.

Figure 2 on page 3 shows where the IBM Director software components are installed in a basic IBM Director environment.

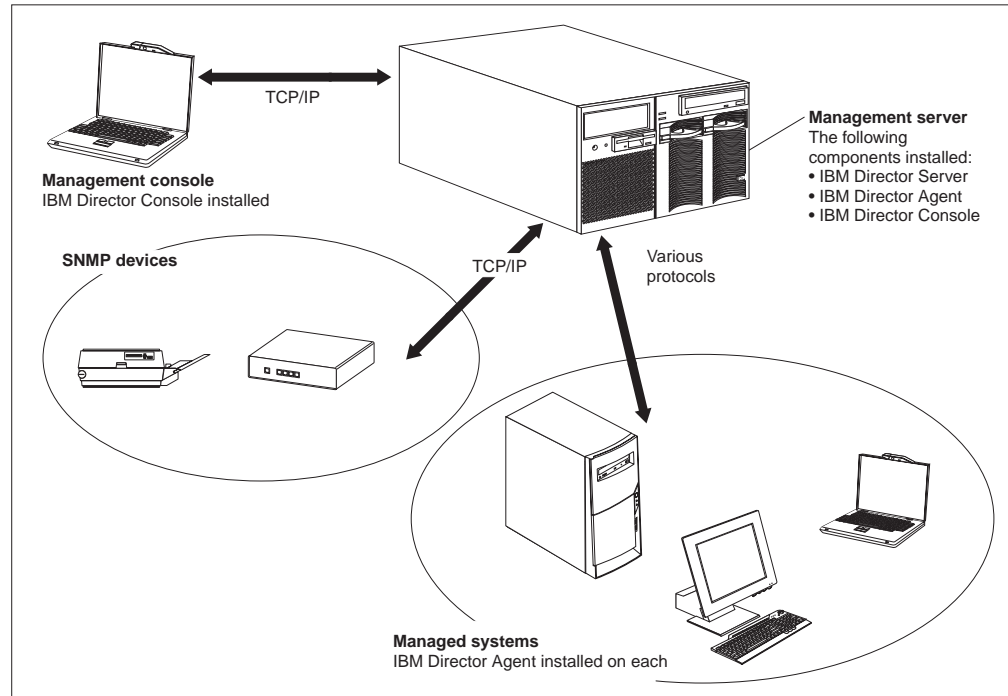


Figure 2. Software in an IBM Director environment

## 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 Windows® 2000. For large-scale IBM Director solutions, you must 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:

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

IBM Director Server requires a license. Every IBM xSeries server and @server BladeCenter chassis comes with an IBM Director Server license. You can purchase additional IBM Director Server licenses for installation on non-IBM servers.

## 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 XP Professional (Service Pack 1 recommended)
- Windows 2000 Professional, Server, Advanced Server, and Datacenter Server (Service Pack 3 required)
- Red Hat Linux, versions 7.1, 7.2, and 7.3
- Red Hat Linux Advanced Server, version 2.1
- SuSE Linux, versions 7.2, 7.3, and 8.0
- Novell NetWare 6.0
- Caldera Open UNIX®, version 8.0
- VMware ESX Server 1.5.2

The IBM Director Agent features vary according to the operating system on which it is installed. For example, you can enable Web-based Access to IBM Director Agent only on Windows operating systems.

All IBM *@server* BladeCenter HS20 servers, IBM NetVista desktop computers, IBM IntelliStation workstations, IBM ThinkPad mobile computers, IBM TotalStorage NAS products, and IBM SurePOS point-of-sale systems come with a license for IBM Director Agent. You can purchase additional licenses for non-IBM systems.

## 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 drag-and-drop 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 XP Professional (Service Pack 1 recommended)
- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3 required)
- Red Hat Linux, version 7.3
- SuSE Linux, version 8.0

You can install IBM Director Console on as many systems as needed. IBM Director includes an unlimited-use license for IBM Director Console.

---

## IBM Director Agent features

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

### ServeRAID Manager

ServeRAID™ Manager works with IBM servers that contain a ServeRAID adapter or an integrated SCSI controller with RAID capabilities. Using ServeRAID Manager, system administrators can monitor and manage RAID arrays without taking a server offline.

### Management Processor Assistant Agent

Management Processor Assistant (MPA) Agent works with IBM servers that contain one of the following service processors or adapters:

- Advanced System Management processor (ASM processor)
- Advanced System Management PCI adapter (ASM PCI adapter)
- Integrated system management processor (ISMP)
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

The MPA Agent handles in-band communication between service processors and IBM Director Server. In addition, it provides in-band alert notification for managed systems running Linux, NetWare, or Caldera Open UNIX (when supported by the service processor).

Using the MPA task in IBM Director Console, system administrators can configure, monitor, and manage the service processors in xSeries servers.

### IBM Director Remote Control Agent (Windows only)

You can use IBM Director Remote Control Agent to perform remote desktop functions on a managed system. From IBM Director Console, you can control the mouse and keyboard of a managed system on which IBM Director Remote Control Agent has been installed. This feature is available only on Windows operating systems.

### Web-based Access (Windows only)

You can use Web-based Access to access a managed system using either a Web browser or the Microsoft Management Console (MMC). When you install Web-based Access on a managed system, system administrators can access IBM Director Agent and view real-time asset and health information about the managed system. This feature is available only on Windows operating systems.

### Web-based Access help files (Windows only)

These are the help files for the Web-based Access interface. They provide information about the managed-system data available to a system administrator using Web-based Access, as well as instructions for performing administrative tasks. Web-based Access is available only on Windows operating systems.

### System Health Monitoring (Windows only)

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

operating-system event log, IBM Director Server, and other management environments. System Health Monitoring is available only on Windows operating systems.

**Note:** For managed systems running Windows, you *must* install System Health Monitoring if you want to monitor the system hardware and send in-band alerts.

## SNMP Access and Trap Forwarding

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

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

---

## Upgrading from previous releases of IBM Director

If you are running IBM Director 3.x, you can upgrade to IBM Director 4.1. Earlier versions of IBM Director are not compatible with IBM Director 4.1.

IBM Director Server 4.1 can manage systems running IBM Director Agent 3.x. This is useful for managed systems running operating systems that are not supported by IBM Director 4.1:

- Windows NT<sup>®</sup> Server, Extended Edition, and Workstation
- Windows 98, Millennium Edition (Me), and 95
- Red Hat Linux 6.2
- SuSE Linux 7.1
- Caldera Linux 2.3.1
- Turbolinux 6.05
- Novell NetWare 5.x
- SCO UnixWare 7.1.1
- OS/2 WARP<sup>®</sup> Server for e-business

---

## IBM Director extensions

*Extensions* are tools that extend the functionality of IBM Director. IBM Director extensions include the IBM Director Server Plus Pack, IBM Director Software Distribution Premium Edition, IBM Director Remote Deployment Manager, and others.

### IBM Director Server Plus Pack

The IBM Director Server Plus Pack contains a portfolio of tools that extend the functionality of IBM Director. These advanced server-management tools are specifically designed for use on xSeries and Netfinity servers. The Server Plus Pack contains the following extensions:

- Active<sup>™</sup> PCI Manager
- Capacity Manager
- Rack Manager
- Software Rejuvenation

- System Availability

To use the Server Plus Pack extensions, you must install them on the management server, the management console, and any managed systems that are xSeries and Netfinity servers. If you do not have IBM xSeries or Netfinity servers in your IBM Director environment, you do not need to install Server Plus Pack extensions.

The Server Plus Pack components that accompany an installation of IBM Director Server and IBM Director Console are located on the *IBM Director* CD. The Server Plus Pack components for an IBM Director Agent installation are located on the *IBM Director Server Plus Pack* CD.

**Note:** To finish installing Rack Manager on the management server, you also must install the Rack Manager server component located on the *IBM Director Server Plus Pack* CD.

The *IBM Director Server Plus Pack* CD is offered without charge to customers using IBM Director 3.1 or 3.1.1; other customers can purchase it for an additional fee. For more information, contact your IBM marketing representative.

Unless otherwise noted, the extensions work with all currently offered xSeries servers.

### **Active PCI Manager**

Active PCI Manager works with the xSeries 235, 255, 345, 360, and 440 servers, as well as the RXE-100 Remote Expansion Enclosure.

Using Active PCI Manager, system administrators can manage peripheral component interconnect (PCI) and peripheral component interconnect-extended (PCI-X) adapters. Active PCI Manager contains two subtasks: Fault Tolerant Management Interface (FTMI) and Slot Manager (previously released as Active PCI Manager). FTMI allows system administrators to view network adapters that are members of fault-tolerant groups; it also can be used to perform offline, online, failover, and eject operations on the displayed adapters. Using Slot Manager, system administrators can display information about PCI and PCI-X adapters, analyze PCI and PCI-X performance, and determine the best slots in which to install PCI and PCI-X adapters.

#### **Notes:**

1. Active PCI Manager is supported only on managed systems running Windows 2000 Server, Advanced Server, and Datacenter Server.
2. Before you install IBM Director 4.1, ensure that you have uninstalled any Active PCI Manager components. Earlier versions of Active PCI Manager, versions 1.0, 1.1, and 3.1.1, are not compatible with IBM Director 4.1.
3. IBM Active PCI Software for Microsoft Windows, version 5.0.2.0 or later, must be installed. You can download the software from [www.ibm.com/support/](http://www.ibm.com/support/). In the **Search** field in the upper-right corner of the window, type ActivePCI.

### **Capacity Manager**

Using Capacity Manager, system administrators can monitor critical resources such as processor utilization, hard disk capacity, memory usage, and network traffic. Capacity Manager can identify current or latent bottlenecks for an individual server or a group of servers. It generates performance-analysis reports that recommend ways to prevent diminished performance or downtime; it also forecasts performance trends.

## **Rack Manager**

Using the Rack Manager drag-and-drop interface, system administrators can build a realistic, visual representation of a rack and its components. By clicking on an element in the visual representation, system administrators can access detailed information (such as system health and inventory data) for the rack component.

## **Software Rejuvenation**

Using Software Rejuvenation, system administrators can avoid unplanned system outages due to resource exhaustion. As software runs over long periods of time, operating systems steadily consume resources and might fail to relinquish them properly. This phenomenon (known as resource exhaustion or software aging) can eventually lead to ineffective operation or even system failure. Software Rejuvenation monitors operating-system resources, predicts system outages, and generates resource exhaustion events; once notified, system administrators can take corrective action before a failure occurs.

System administrators also can use Software Rejuvenation to automate the process of restarting operating systems, applications, and services at convenient times and in advance of actual failures. Since Software Rejuvenation is cluster aware, it can restart a node without taking the cluster offline.

## **System Availability**

Using System Availability, system administrators can document and track server availability. System Availability accurately measures server uptime and downtime and provides several graphical representations of this information. It helps system administrators to notice patterns concerning system availability.

## **IBM Director Software Distribution Premium Edition**

IBM Director Software Distribution Premium Edition adds several new functions to the IBM Director Software Distribution task. The IBM Director Software Distribution task enables you to import IBM software, build software packages using the Update Assistant wizard, and distribute the packages to managed systems. When you purchase and install IBM Director 4.1 Software Distribution Premium Edition, you can accomplish the following additional tasks:

- Import non-IBM software and build software packages using the following wizards:
  - InstallShield Package wizard (Windows)
  - Microsoft Windows Installer wizard (Windows)
  - RPM Package wizard (Linux)
- Import IBM or non-IBM software and build a software package using the Custom Package Editor
- Export a software package for use on another management server
- Import a software package created by another management server, using the Director File Package wizard

## **IBM Director Remote Deployment Manager 4.10**

Remote Deployment Manager (RDM) is a flexible and powerful tool for configuring, deploying, and retiring systems. Using RDM, system administrators can accomplish the following deployment tasks:

- Update system firmware
- Modify configuration settings
- Install operating systems
- Back up and recover primary partitions



- Securely erase data from disks

RDM supports both customized and scripted deployments. In addition, since it uses industry-standard protocols to wake and discover target systems, RDM does not require an agent component.

## Additional IBM Director extensions

IBM provides additional IBM Director extensions that you can download from the IBM Support Web site:

### **Real Time Diagnostics**

Enables you to run industry-standard diagnostic utilities on servers while they are running.

### **Cluster Systems Management**

Enables you to manage IBM Cluster Systems Management (CSM) clusters using IBM Director Console.

Check the Systems Management Web page for information about these extensions. See “IBM Director resources on the World Wide Web” on page xv for more information.

**Note:** IBM can add or withdraw extensions on the IBM Support Web site without notice.

In addition, other companies have developed extensions for IBM Director:

### **APC PowerChute Extension for IBM Director**

Enables you to manage PowerChute data and events from IBM Director Console or a Web browser.

### **Electronic Service Agent**

Tracks and captures system inventory data, and if the system is under a service agreement or within the warranty period, automatically reports hardware problems to IBM.

### **Application Workload Management (Aurema)**

Manages how multiple applications use server resources.

For more information about these third-party extensions, see the Redbooks publication *Implementing Systems Management Solutions Using IBM Director* (SG24-6188-01).



## Chapter 2. Understanding IBM Director Console

You can use IBM Director Console to group managed objects, view associations, start tasks, and set IBM Director options and preferences. This chapter covers how to use IBM Director Console to accomplish these activities, how to use IBM Director tasks that are used on other tasks, such as Scheduler, and how to build and use event action plans.

### 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.

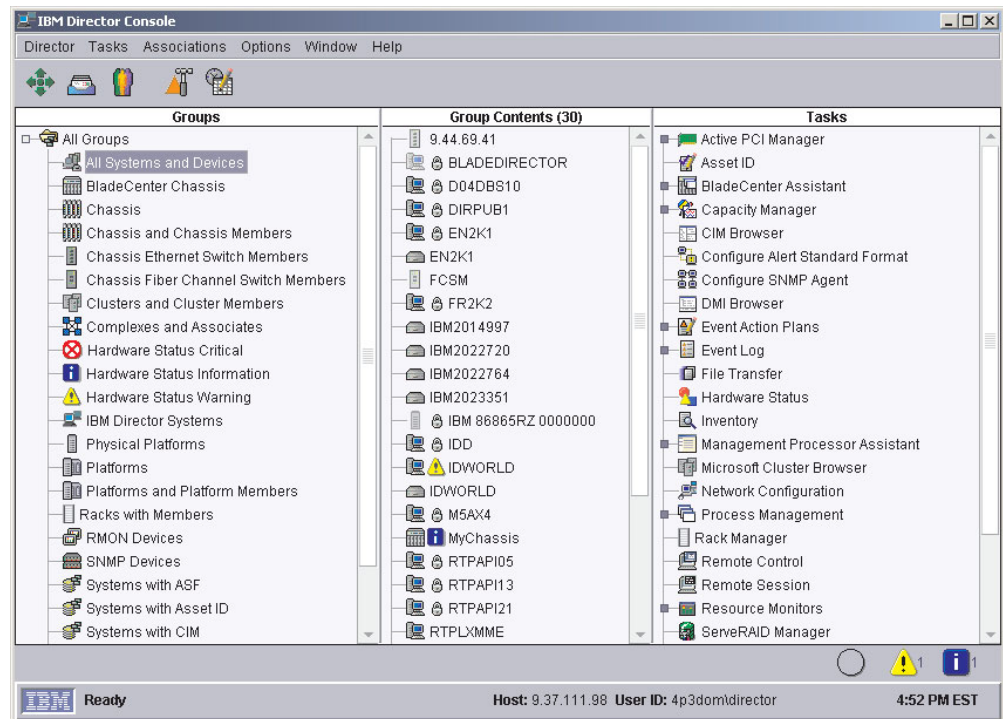


Figure 3. IBM Director Console interface

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 secured by a 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 that has local administrative rights to that managed system and password, you can access the system.

For BladeCenter chassis and physical platforms, the padlock icon is displayed if a valid login profile does not exist for the service processor. You can request access using the above method.

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 inventory.

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.

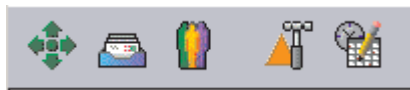


Figure 4. IBM Director Console toolbar

From left to right, the icons represent:

- Discover All Managed Systems (see the *IBM Director 4.1 Installation and Configuration Guide*)
- Message Browser (see “Message Browser” on page 36)
- User Administration (see “User Administration” on page 36)
- Event Action Plan Builder (see “Event action plans” on page 20)
- Scheduler (see “Scheduler” on page 27)

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.

## Starting tasks

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

- 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.

There are also other IBM Director functions, such as the Event Action Plan Builder and Scheduler, that can be started in one of two ways:

- From the menu bar
- From the toolbar

## Managed systems and managed objects

One key to using IBM Director is understanding the concept of managed systems, managed devices, and managed objects. IBM Director recognizes all three, although each term refers to different types of hardware. Managed systems have

IBM Director Agent installed, whereas managed devices are SNMP devices such as network devices, printers, desktop computers, or servers that have SNMP agents installed or embedded. The term managed object can refer to a managed system or device or a Windows cluster, BladeCenter chassis, management processor, multi-node server (complex), static partition, physical platform, remote I/O enclosure, or a rack created using the Rack Manager task.

A management processor is an IBM Director managed object that represents an optional service processor that has been added to an xSeries or Netfinity server that has an ASM service processor. A remote I/O enclosure is an IBM Director managed object that represents an RXE-100 Remote Expansion Enclosure. It is associated with the physical platform representing the xSeries server to which it is connected.

A physical platform is an IBM Director managed object that represents a single physical chassis or server that has been discovered through the use of the service location protocol (SLP). A physical platform can also be created when:

- A deployable system is discovered through an RDM scan
- IBM Director Server determines that a physical platform does not already exist for a blade server in a BladeCenter unit
- IBM Director Server first discovers and gains access to a managed system that meets the following criteria:
  - IBM Director Agent installed and the optional MPA agent installed
  - MPA agent detects a supported service processor
- IBM Director Server gains IP access to an Remote Supervisor Adapter service processor. It will query the Remote Supervisor Adapter service processor for the topology of its associated RS-485 network, and for each ISMP system found, a physical platform is created.

A physical platform can identify some managed systems before an operating system or IBM Director Agent is installed.

## Groups

Groups are logical sets of managed objects. An example might be a group that contains managed systems that have Linux installed. When you start 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.

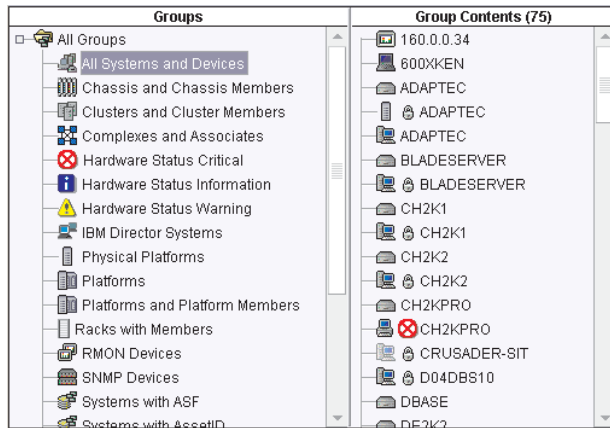


Figure 5. A selected group listed in the Group Contents pane

You can select one group at a time. To perform tasks simultaneously on multiple groups, create a new group and include each desired managed system from the multiple groups, or combine several separate existing groups into one new 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” or “Creating a static group” on page 16.

### 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, affecting their match to 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.

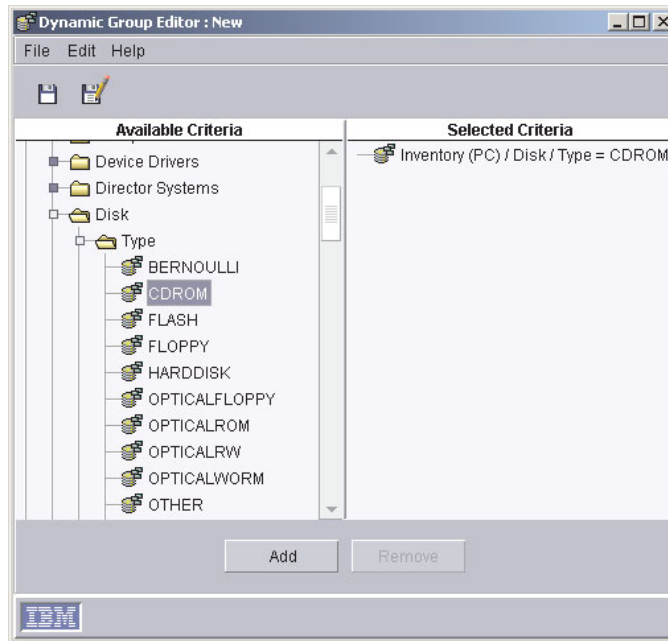


Figure 6. Dynamic Group Editor window

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**; then, 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.
5. Click **OK**. The group is displayed under **All Groups** in the Groups pane.
6. Click **File** → **Close Group Editor** to close the Dynamic Group Editor window.

**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.

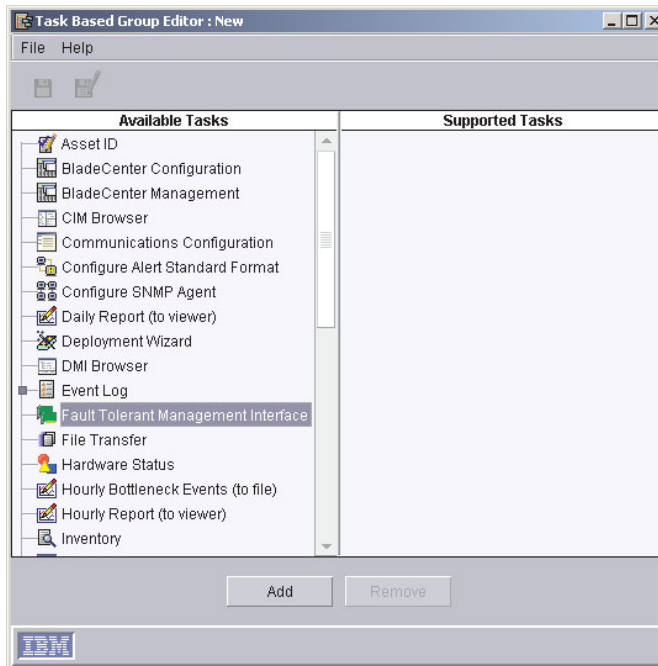


Figure 7. Task Based Group Editor window

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. This is the group name that will be listed in the Groups pane.
5. Click **OK**. The group is displayed under **All Groups** in the Groups pane.
6. 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.



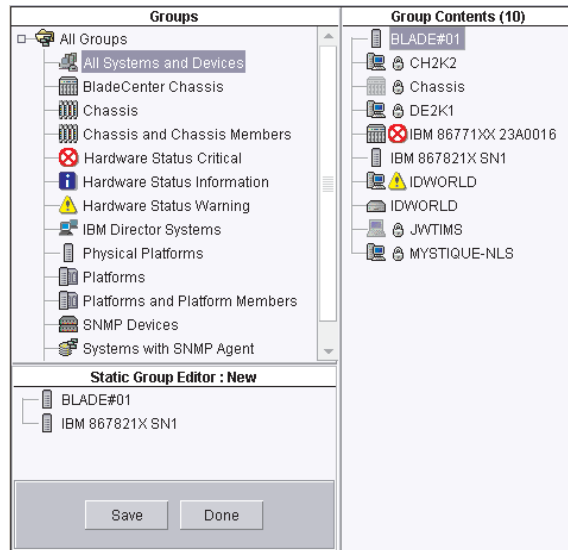


Figure 8. Static Group Editor window

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. This is the group name that will be listed in the Groups pane.
5. Click **OK**. The group is displayed under **All Groups** in the Groups pane.
6. 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.

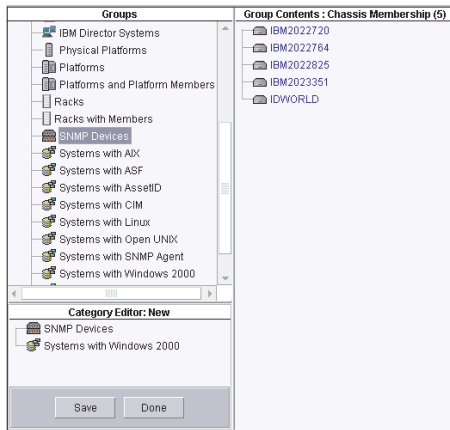


Figure 9. Category Editor window

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. This is the group name that will be listed in the Groups pane.
5. Click **OK**. The new group category is displayed in the Groups pane.
6. Click **Done** to close the Category Editor.

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

### 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.

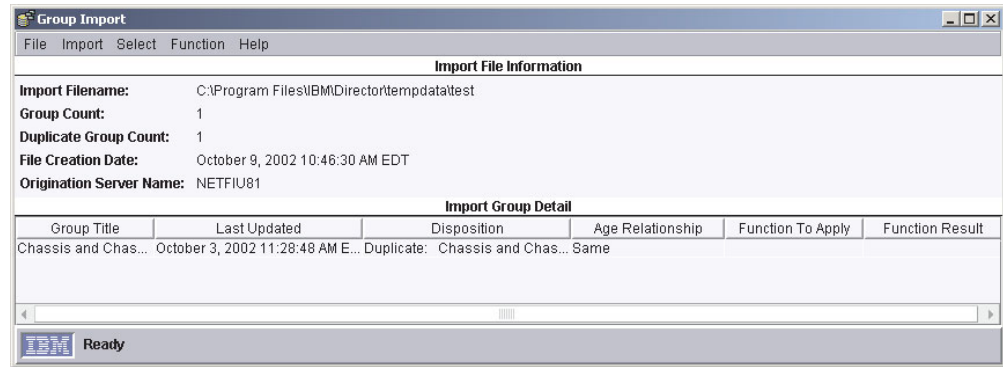


Figure 10. Group Import window

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.

## 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 objects 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. The following is a list of all options available:

- Object Type
- TCP/IP Addresses
- TCP/IP Host Names
- IPX Network IDs
- Domains/Workgroups
- Chassis Membership
- Cluster Membership
- Complex Membership
- Physical Platform—Remote I/O Enclosures
- Platform Membership
- Rack Membership
- System Partition Membership
- TCP/IP Routers/DNS
- Status

Selecting the Platform Membership association shows the relationship between IBM Director managed systems and platforms. This is particularly useful if you have multiple managed objects that represent a single system with IBM Director Agent installed. Depending on the IBM Director task you want to perform, the managed object that you target will differ.

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. The names of any systems not meeting the Associations criteria are displayed in blue type.

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 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 a managed system using the Software Distribution task.

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

**Activations**

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

**Resource Monitors**

Shows the resource monitors, if any, that have been applied to a managed system.

**Event Action Plans**

Shows the event action plans, if any, that have been applied to a managed system.

---

## Events and alerts

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

---

## Event action plans

By creating event action plans and applying them to specific managed systems, you can be notified by e-mail or pager, for example, when a specified threshold is reached or a specified event occurs. Or, you can configure an event action plan to start a program on a managed system and change a managed system variable when a specific event occurs. You can use process-monitor events and resource-monitor events to build an event action plan. See “Process Management” on page 96 and “Resource Monitors” on page 109 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 151. Also, for more information about events, event types, and extended attributes, see the *IBM Director 4.1 Events Reference*.

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

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

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

## Implementing an event action plan

Complete the following steps to implement an event action plan:

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

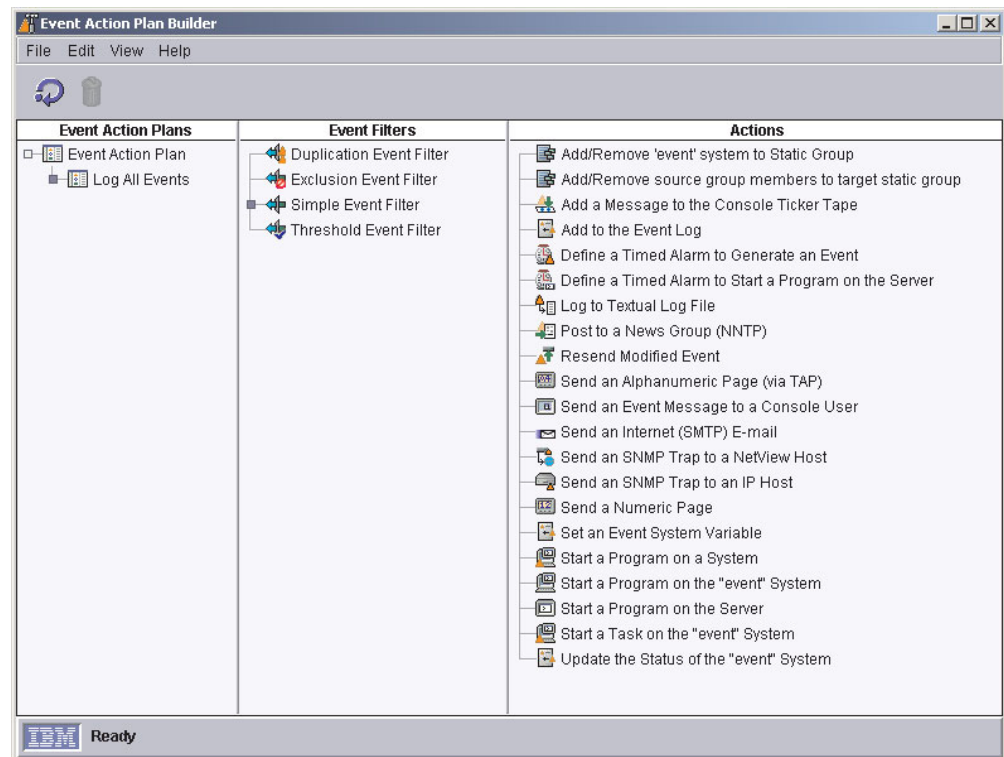


Figure 11. Event Action Plan Builder window

The Event Action Plan Builder interface contains three panes:

### Event Action Plans pane

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

### **Event Filters pane**

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

### **Actions pane**

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

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

#### **Simple Event Filter**

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

#### **Duplication Event Filter**

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

#### **Exclusion Event Filter**

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

#### **Threshold Event Filter**

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

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

The applicable Event Filter Builder window opens.

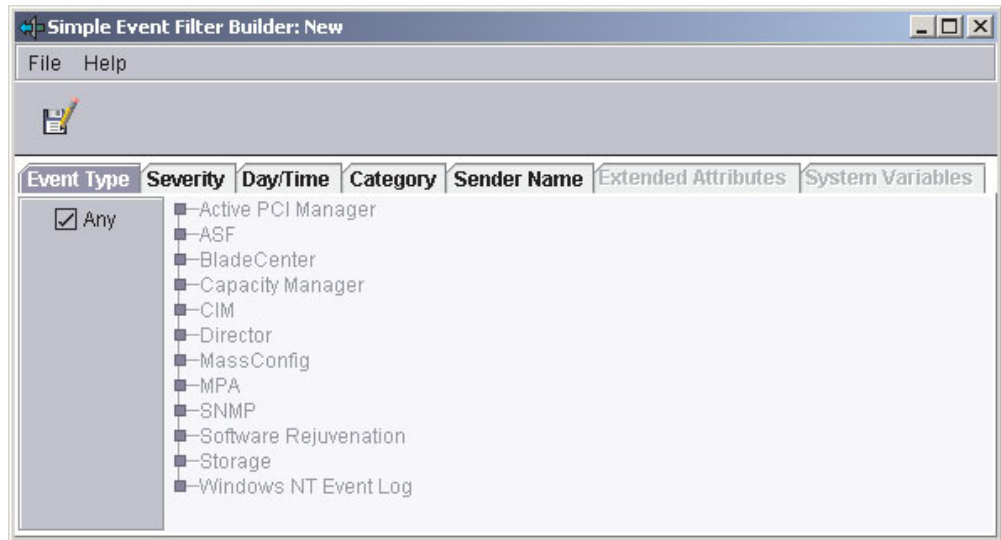


Figure 12. Simple Event Filter Builder window

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

#### Event Type

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

#### Severity

Specifies the urgency of events that are received.

#### Day/Time

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

#### Category

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

#### Sender Name

Specifies the managed system to which the filter applies.

#### Extended Attributes

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

#### System Variables

Specifies user-defined pairings of a keyword and value that are known only to the local management server. The **System Variables** tab is available only if one or more system variables exist. See “Viewing and changing system variables” on page 25 for more information.

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

- Complete the fields as appropriate for the event filter you want to create.
6. Click **File** → **Save As**. The Save Event Filter window opens.
  7. Name the filter and click **OK** to save the filter. The new filter is displayed in the Event Filters pane under the applicable filter type.
  8. (Optional) You can create additional event filters for use in a single event action plan. Repeat step 4 on page 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 13 is for ticker-tape alerts.

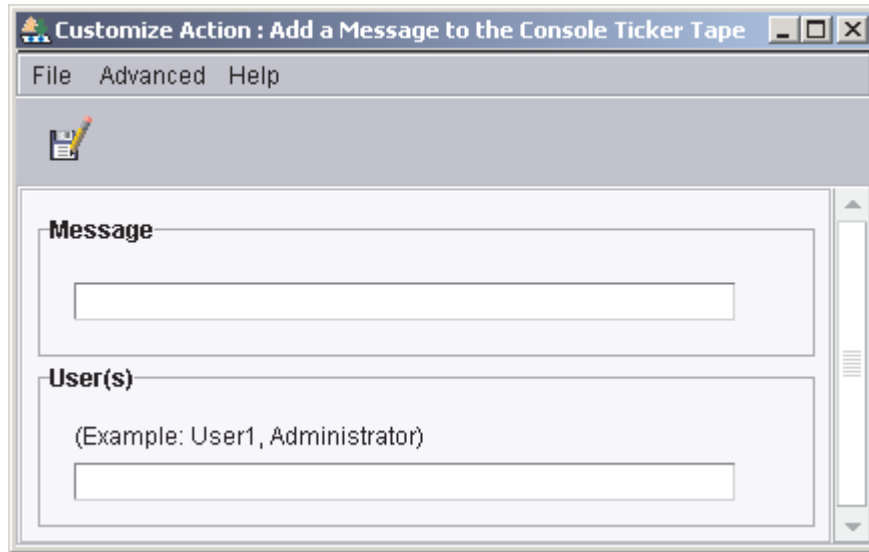


Figure 13. Customize Action window for ticker-tape alert

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 162 for more information).
11. Click **File** → **Save As**. The Save Event Action window opens.
12. Name the action and click **OK** to save the action. The new action is displayed in the Actions pane under the applicable action type.
13. (Optional) Test the event action to verify that it works as you intended. For example, you can create a message using the Add a Message to the Console Ticker Tape action type and specify \* in the **User** field to indicate all users. When you test this action, the ticker tape displays the message on your IBM Director Console.  
Complete the following steps to test an event action:
  - a. Locate the event action under the corresponding event action type in the Actions pane of the Event Action Plan Builder window.
  - b. Right-click the event action, then click **Test**. The action occurs.
14. (Optional) You can customize additional event actions for use in a single event action plan. Repeat step 9 through step 13.
15. In the Event Filters pane, drag the event filter onto the event action plan (located in the Event Action Plans pane) that you created in steps 2 through 3 on page 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.

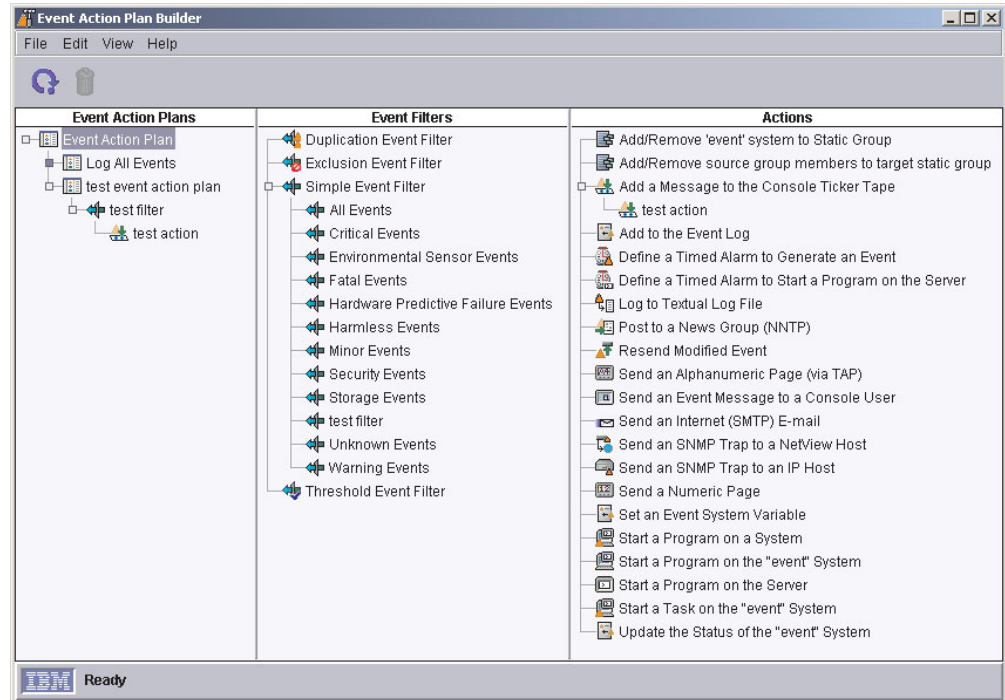


Figure 14. Example of an event action plan with an event filter and event action assigned to it

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

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

## Viewing and changing system variables

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

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

Then, if 10 seconds elapse before IBM Director Server receives the event that triggers this event action or before the management server stops and restarts, the NetStatus system variable is reset to Normal. You can reference system variable

names and values wherever event data substitution is allowed. See “System Variables page” on page 157 for more information about system variables and how they can be used in event action plans.

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

## Enabling and viewing an event action history

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

## Viewing event action plan associations

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

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

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

## Restricting event action plans

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

Complete the following steps to restrict an event action plan:

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

## Exporting event action plans

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

**Archive**

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

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

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

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

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

Complete the following steps to export an event action plan:

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

## Importing event action plans

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

Complete the following steps to import an event action plan:

1. Transfer the archive file that you want to import to a drive on the management server.
2. In IBM Director Console, click **Tasks** → **Event Action Plan Builder**. The Event Action Plan Builder window opens.
3. Click **File** → **Import** → **Archive**. The Select File for Import window opens.
4. Select the archive file from step 1.
5. Click **OK** to begin the import process. The Import Action Plan window opens, displaying the event action plan to import.
6. Click **Import** to complete the import process. If the event action plan had previously been assigned to managed systems or groups, you have the option to preserve those assignments during the import process.

---

## Scheduler

You can use Scheduler to run a single noninteractive task or set of noninteractive tasks at a later time. (Only noninteractive tasks, which are defined as those tasks that do not require any user input or interaction, can be scheduled.) 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 changes to an existing job as a a new job.

## Starting Scheduler

You can start Scheduler in either of two ways:

- Scheduling a task directly
- Dragging a task to a managed system or group (only certain tasks support this option)

To schedule a task using the second technique, see “Dragging a task onto a managed system or group” on page 32.

### 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.

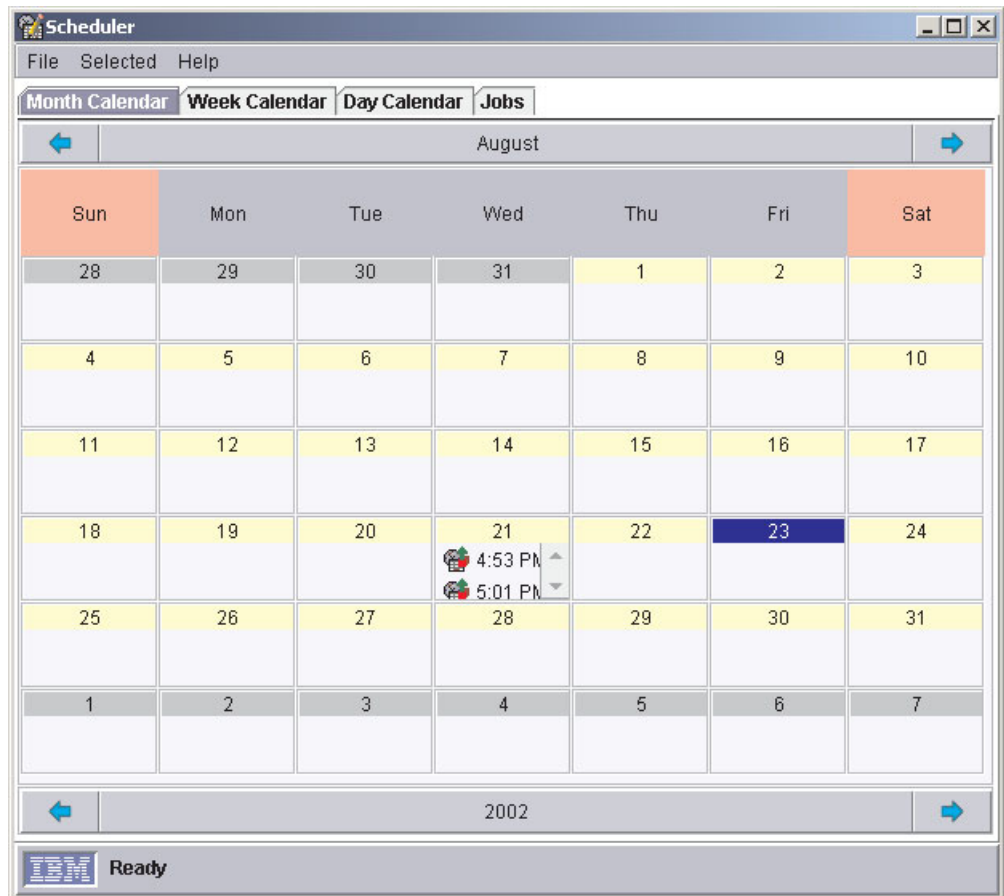


Figure 15. Scheduler window

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

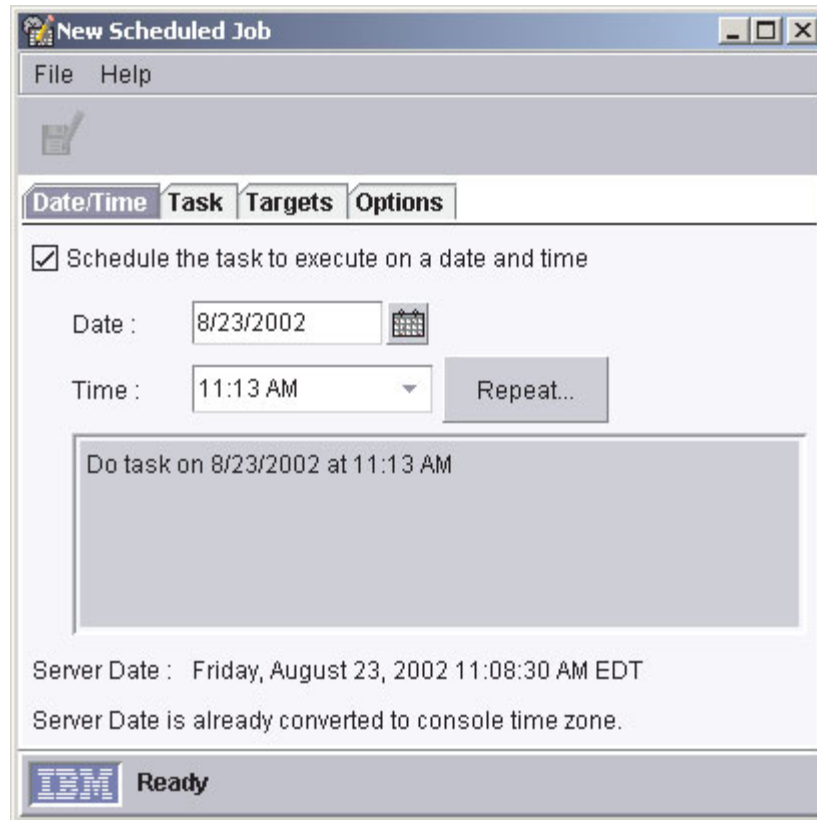


Figure 16. New Scheduled Job window

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:** The server date and time is indicated in the New Scheduled Job window; Scheduler uses this date and time to determine when the scheduled job runs.

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.

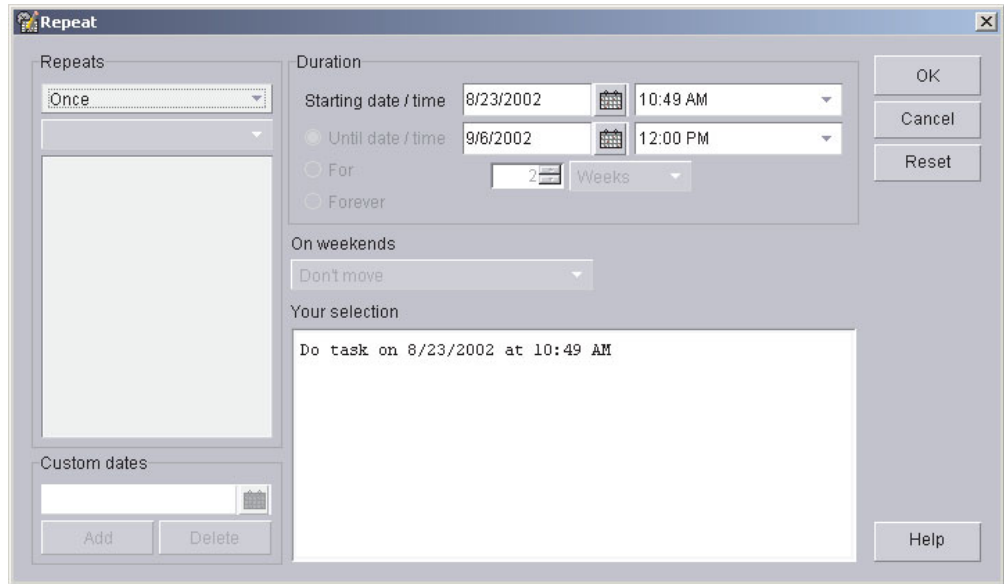


Figure 17. Repeat window

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**

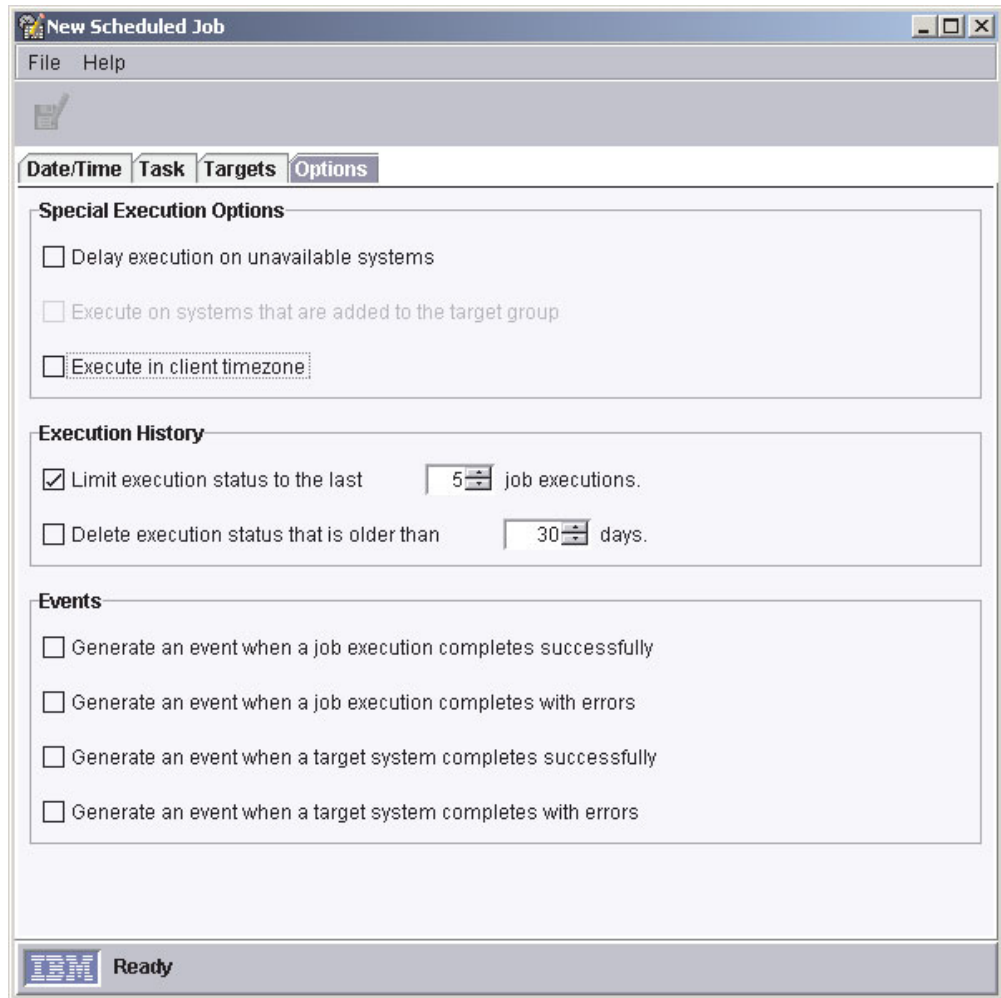


Figure 18. Options page in New Scheduled Job window

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 Capacity Manager, 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.



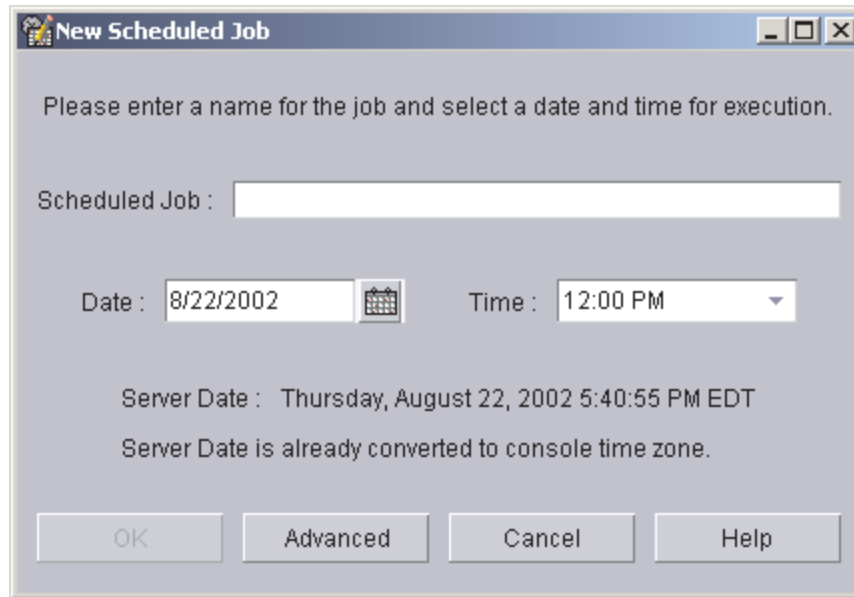


Figure 19. New Scheduled Job window, when you opt to schedule a task that is activated by dragging it onto a managed system

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 29 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 15 on page 28).

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 20).

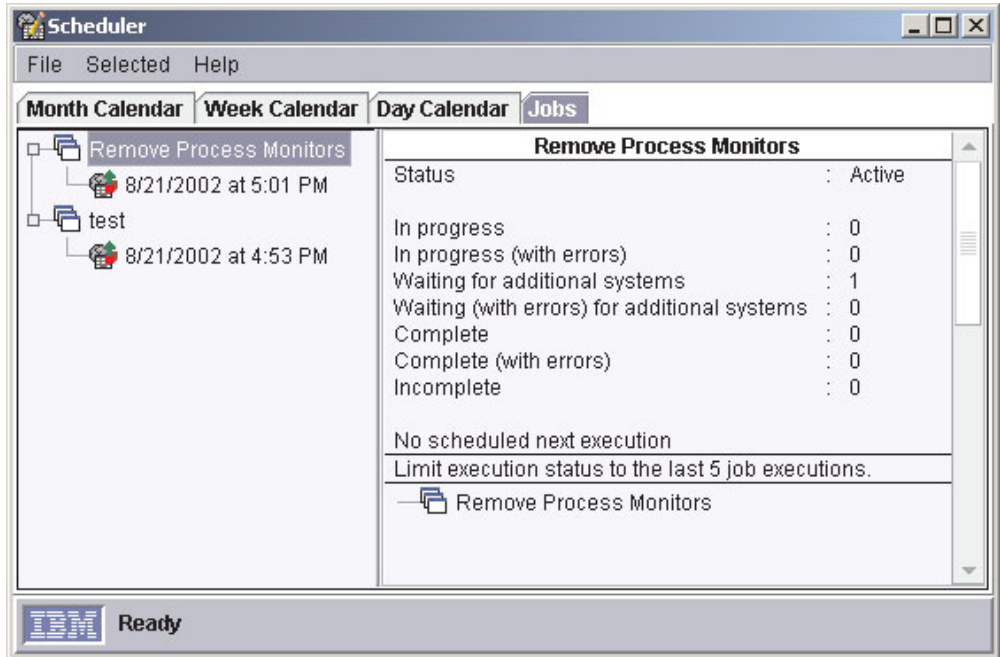


Figure 20. Selecting a job type in the left pane on the Jobs page in the Scheduler window

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 (see Figure 21 on page 35).

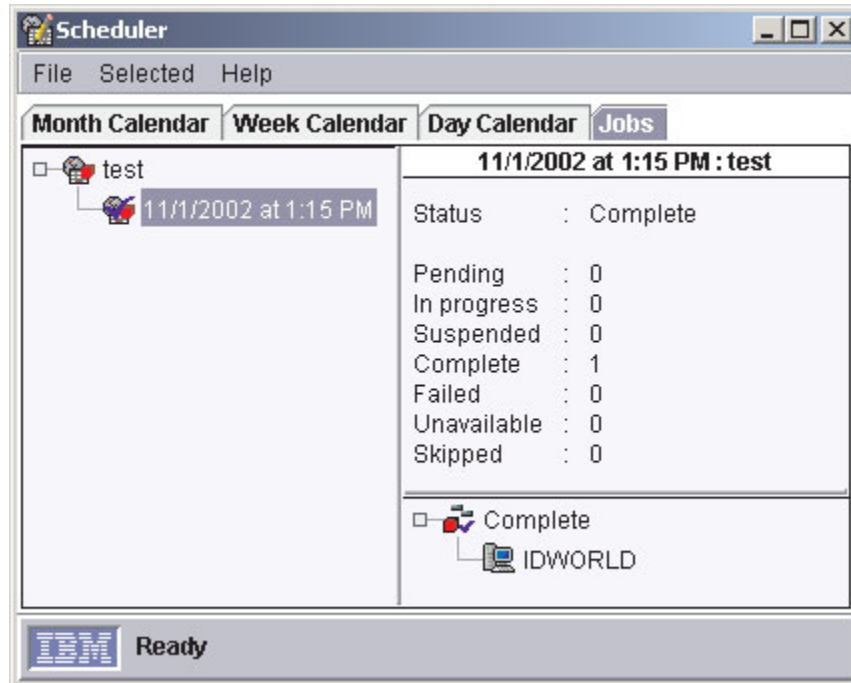


Figure 21. Selecting a specific job execution in the left pane on the Jobs page in the Scheduler window

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

---

## Message Browser

You can use the Message Browser to view alerts sent to IBM Director Console. The Message Browser is displayed automatically whenever an alert is sent to the management console. You can opt to be notified 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 20 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 117 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, change the defaults for new IBM Director user IDs, and delete user IDs using the User Administration task. For more information about user administration tasks, see the *IBM Director 4.1 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.

## Encryption administration

You can enable or disable encryption, change the encryption algorithm, create new server keys, or issue a new encryption key and send the new encryption key to all managed systems using the encryption administration function in IBM Director Console. Click **Options** → **Encryption Administration**. The Encryption Administration window opens.



Figure 22. Encryption Administration window



---

## Chapter 3. Working with managed systems using IBM Director Console tasks

This chapter provides information about IBM Director Console tasks. IBM Director provides a robust suite of systems-management functionality through the IBM Director Console tasks. You can use these tasks on systems or groups of systems. Each task is represented with an icon in the IBM Director Console Tasks pane. This chapter lists all the available tasks, both standard and Server Plus Pack, alphabetically for easy reference.

The tasks that you can use in your systems-management environment can vary, depending on the features and options you have installed as well as the managed system hardware in your environment. See the section for each task for information about any limitations.

---

### IBM Director Console tasks and BladeCenter products

Some tasks you can use with BladeCenter units (see Table 1 for a list of tasks and whether you can use a task on a BladeCenter unit or component). BladeCenter units consist of a chassis, one or more switches (up to 4 total), 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 appear in the RMON devices group, which is a subgroup of the SNMP devices group.

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
Active PCI Manager				X
Asset ID™				X
BladeCenter configuration	X			

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

Task	Chassis	Switch	Blade server	
			Without IBM Director Agent installed	With IBM Director Agent installed
BladeCenter management	X			
BladeCenter Deployment wizard	X			
BladeCenter Switch Management LaunchPad		X		
Blue indicator light	X		X	X
Capacity Manager				X
CIM Browser				X
Configure SNMP agent				X
DMI Browser				X
Event action plans	X	X	X	X
File Transfer				X
Hardware Status	X		X	X
Inventory	X	X	X	X
Microsoft Cluster Browser				X
Network Management				X
Power Management			X	X
Process Management				X
Rack Manager	X	X		X
Remote Control				X
Remote Session		X		X
Resource Monitors		X		X
ServeRAID Manager				X
SNMP devices (Browser)		X		X
Software Distribution				X
Software Rejuvenation				X
System Accounts				X
System Availability				X

## Active PCI Manager

Using the Active PCI Manager task, a part of the Server Plus Pack, you can manage peripheral component interconnect (PCI) and peripheral component interconnect-extended (PCI-X) adapters in managed systems. Active PCI Manager provides two interfaces for performing tasks:

- Fault Tolerant Management Interface (FTMI)
- Slot Manager (previously released under the name Active PCI Manager)



## Fault Tolerant Management Interface (FTMI)

Fault Tolerant Management Interface (FTMI) is an administrative tool for managing network adapters on managed systems. The networked adapters must be members of fault-tolerant groups that have been created by the configuration software from the adapter vendors. You can use FTMI to view fault-tolerant adapters and fault-tolerant groups and perform offline, online, failover, and eject operations for the displayed adapters. A Common Information Model (CIM) provider program from the adapter vendor receives requests from FTMI and then handles the supported CIM functions of the adapter to perform the requested operations. FTMI is currently implemented based on CIM version 2.3.

### Defining fault-tolerant groups and fault-tolerant adapters

A fault-tolerant group is a logical group that contains two or more network adapters that are controlled by the same device driver. Adapters must be able to share work (load-balanced) or take work (spare) from another adapter in the designated group, as needed.

Fault-tolerant groups are usually configured when the associated device drivers are configured through the operating system. Each adapter in a group is given a name and a unique device ID. The vendor of each adapter provides the software for configuring fault-tolerant groups.

There are two types of fault-tolerant groups:

- Extra capacity group

In this group, multiple online adapters collectively act as a single adapter to the system. The online adapters share work and assume any work from adapters in the group that go offline or fail. Some adapter vendors refer to this feature as adaptive load balancing, bidirectional load balancing, or adapter teaming. The collective, single adapter is also sometimes referred to as a virtual adapter or virtual network interface card (NIC).

- Spare group

In this group, only one adapter in the group is online at any given time. The remaining adapters in the group are powered on but do not perform any work. These offline adapters are used for failover operations when the primary (active) adapter fails. Some adapter vendors refer to this feature as adapter fault tolerance, failover teaming, or transmit load balancing.

### Starting the FTMI subtask

To start the Fault Tolerant Management Interface subtask, in the IBM Director Console Tasks pane, expand the **Active PCI Manager** task; then, drag the **Fault Tolerant Management Interface** subtask onto a managed system that supports Active PCI Manager. The Fault Tolerant Management Interface window opens.

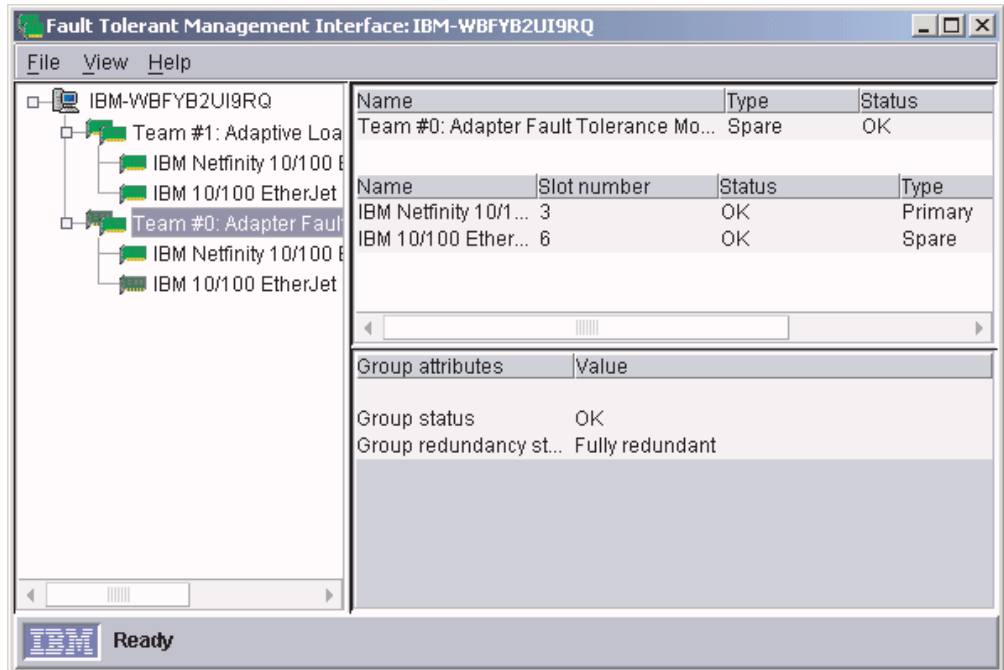


Figure 23. Fault Tolerant Management Interface window

In the Fault Tolerant Management Interface window, the left pane displays a tree structure of the fault-tolerant groups and fault-tolerant adapters defined for the managed system. The icon for each fault-tolerant group or adapter indicates whether the adapter is online or offline or what type of group is defined (extra capacity or spare) and whether any error conditions are present.

The right pane displays information about the managed system, fault-tolerant group, or fault-tolerant adapter selected in the left pane. Depending on the item selected, multiple tables of information are displayed.

FTMI updates the icons and table information whenever offline, online, or failover operations occur for an adapter. Additionally, you can refresh the window manually by clicking **View → Refresh**. This function can take several seconds.

**Displaying information about fault-tolerant adapters:** Icons for each fault-tolerant adapter are displayed under the fault-tolerant groups in the tree view of the FTMI window. Click an adapter icon to display its properties in the right portion of the window.

The upper-right pane displays the adapter name, slot number, status, type, and device ID.

The lower-right pane displays additional adapter attributes. The attributes are grouped into three sections, each providing information about the status of the adapter, the physical adapter, and the physical slot.

**Displaying information about fault-tolerant groups:** The icon for each fault-tolerant group is displayed under the managed system in the left pane. Click a group icon to display information about that group. FTMI displays three tables of information about the group: two in the upper-right pane and one in the lower-right pane.

The table in the lower-right pane displays additional attributes about the fault-tolerant group. It displays the status of the group and its redundancy. For extra capacity groups, the table also displays the minimum number of adapters that the group must contain.

### Performing FTMI operations

You can perform FTMI operations on fault-tolerant adapters, but not on fault-tolerant groups. The device driver for a fault-tolerant adapter can initiate offline and failover operations for its associated adapter automatically. You can initiate online, offline, failover, and eject operations for an adapter manually, depending on which of these are valid for the selected adapter.

**Offline operations:** Offline operations are supported for online adapters in extra capacity groups. Offline operations occur under two scenarios:

- The associated device driver determines, by its own criteria, that an online adapter in an extra capacity group has failed. If a fault-tolerant adapter in an extra capacity group fails to respond to commands from its device driver, the device driver can suspend or redirect requests that the adapter is unable to perform, and the adapter will go offline.
- You decide that an online adapter in an extra capacity group should be taken offline.

In both cases, FTMI notifies the adapter software to begin the offline operation. The adapter software directs work to the other online adapters in the extra capacity group so that the selected adapter is no longer active. The adapter software then takes the adapter offline.

*Starting a manual offline operation:* To start a manual offline operation, in the left pane of the Fault Tolerant Management Interface window, right-click the online adapter that you want to take offline and click **Offline**.

*Notification of an offline operation:* After an offline operation, FTMI automatically updates the window. Depending on the number of groups and adapters, this refresh can take several seconds.

Additionally, you can use FTMI CIM queries and the Event Filter Builder to create IBM Director alerts that are used in event action plans to notify the system administrator whenever an adapter goes offline. For details, see “FTMI CIM queries” on page 44.

After an adapter has gone offline, the administrator can then replace the adapter by ejecting it and installing a new one in its place. In this scenario, the administrator must use the software of the adapter vendor to add the new adapter into the affected extra capacity group.

**Online operations:** Online operations are supported for offline adapters in extra capacity groups. An adapter that has failed or that has been brought offline by the vendor software, such as the standby or backup adapter, cannot be brought online.

To start a manual online operation, in the left pane of the Fault Tolerant Management Interface window, right-click the offline adapter in the group that you want to bring online and click **Online**.

FTMI notifies the adapter software to begin the online operation. The adapter software brings the adapter online and accepts work for the adapter. This work is assigned from the other online adapters in the group.

After an online operation, FTMI automatically updates the window. Depending on the number of groups and adapters, this refresh can take several seconds.

Additionally, you can use FTMI CIM queries and the Event Filter Builder to create IBM Director alerts that are used in an event action plan to notify the system administrator whenever an adapter comes online. For details, see “FTMI CIM queries”.

**Failover operations:** Failover operations are supported for online adapters in spare groups. Failover operations occur under two scenarios:

- The associated device driver determines, by its own criteria, that an online adapter in a spare group has failed.
- A system administrator decides to manually failover an online adapter to a spare adapter so it can be replaced.

In both cases, FTMI notifies the adapter software to begin the failover operation. The adapter software causes the primary adapter to go offline and makes the newly selected (offline) adapter in the spare group the new active (online) adapter.

*Starting a manual failover operation:* To start a manual failover operation, in the left pane of the Fault Tolerant Management Interface window, right-click the online adapter in the spare group that you want to use for the failover operation, click **Failover to**, and select an adapter.

*Notification of a failover operation:* After a failover operation, FTMI automatically updates the window. Depending on the number of groups and adapters, this refresh can take several seconds.

Additionally, you can use FTMI CIM queries and the Event Filter Builder to create IBM Director alerts that are used in an event action plan to notify the system administrator whenever a failover operation occurs. For details, see “FTMI CIM queries”.

After the designated system administrator receives an indication that an adapter has failed over, the administrator can replace the adapter by ejecting it and installing a new one in its place. In this scenario, an administrator must use the software of the adapter vendor to add the new adapter to the affected spare group.

**Eject operations:** Eject operations (also known as hot-eject operations) are supported for all adapters in extra capacity groups and for offline adapters in spare groups that are in hot-plug slots.

**Note:** For online adapters in extra capacity groups, use an offline operation instead of an eject operation when you want to stop activity on the adapter and you plan to bring it online at a later time without performing a hot-add operation. For details, see “Offline operations” on page 43.

An eject operation in FTMI directs the adapter software to make an operating-system request to eject the adapter and power off the slot that contains the adapter. After an adapter has been ejected through FTMI, you must physically raise and lower the latch on the slot to hot-add the adapter.

### **FTMI CIM queries**

FTMI comes with a set of CIM queries that you can use to create event filters in the Event Filter Builder. The FTMI CIM queries are located in the Event Filter Builder window under the **CIM** option and the **Fault Tolerant Management Interface**

**Queries** suboption. For more information about using the event filter builder and event action plans, see “Event action plans” on page 20 and Chapter 4, “Event management”, on page 151.

FTMI CIM queries that are used in an event filter are invoked every 60 seconds to determine if an event should be reported. For this reason, the FTMI CIM queries impact performance and you should give careful consideration to the events that you want to monitor automatically.

The following table lists the FTMI CIM queries for fault-tolerant adapters and fault-tolerant groups.

*Table 2. FTMI CIM queries*

FTMI CIM query	Returns a message when	Query test used
Network Adapter Offline	The adapter changes to offline.	Availability=Offline
Network Adapter Online	The adapter changes to online.	Availability=Running/Full power
Network Adapter Failed	The adapter has failed.	Status=Error
Redundancy Group Change	The RedundancyStatus group property has changed for a spare group.	The status has changed in the last 60 seconds.

## Slot Manager

Using Slot Manager, you can access the following tools:

- A Slot Manager window that you can use to view information about how the PCI and PCI-X adapters are connected in the system chassis and any input/output (I/O) expansion drawers of a managed system.
- An Analyze function that analyzes the PCI performance of the PCI bus, slots, and adapters in a managed system. For details, see “Analyzing PCI performance” on page 50.
- An Add Card wizard that determines the most suitable slot in which to insert a new adapter. For details, see “Adding adapters” on page 52.

To start Slot Manager, in the IBM Director Console Tasks pane, expand the **Active PCI Manager** task; then, drag the **Slot Manager** task onto a managed system that supports Active PCI Manager. The Slot Manager window opens.

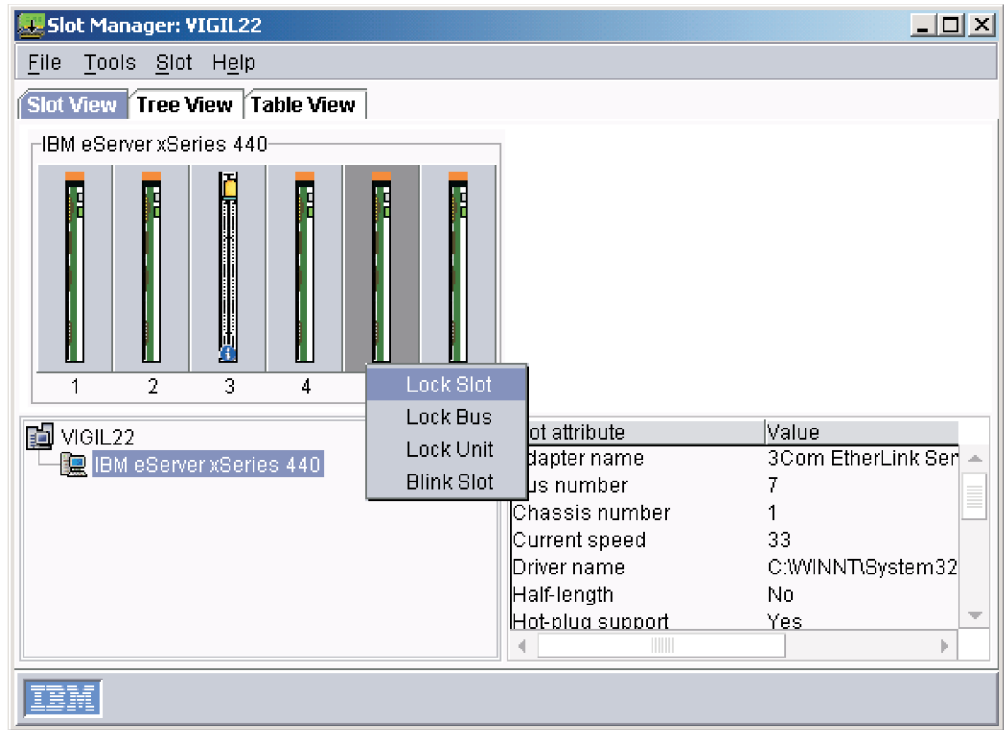


Figure 24. Slot Manager window using Slot view

The Slot Manager window displays information about how the PCI and PCI-X adapters are connected in the system chassis and in any input/output (I/O) expansion drawers of a managed system.

The interface presents the system information through icons in the Slot view and Tree view and through a text table in the Table view. To change the view, click the tab of the view you want to see.

**Note:** The Slot Manager window does not display information about built-in PCI adapters nor the service-processor slot.

Each of the views in Slot Manager displays values for slot and adapter attributes. The attribute for the current slot speed indicates the speed in MHz at which a slot is operating and whether the slot is operating in PCI or PCI-X mode. The attribute for the maximum slot speed indicates the speed in MHz at which a slot is capable of operating and whether the slot is capable of operating in PCI or PCI-X mode. If the slot speed number is not followed by an X, the slot is operating at that speed in PCI mode. If the slot speed number is followed by an X, the slot is operating at that speed in PCI-X mode.

### Slot view

The Slot View page displays a graphical representation of the slots and adapters found in the managed system (see Figure 24). The lower-left portion of the window shows icons representing the managed system, each system chassis, and each I/O expansion drawer. Click a system chassis icon or an I/O expansion icon to display its current slot configuration in the top portion of the page. The slot-attribute pane in the lower-right portion of the page is also updated to display information about the selected system chassis or I/O expansion drawer. If the slot has an adapter, the slot-attribute pane also displays information about the adapter in that slot.

The top portion of the page shows the slots in a system chassis or an optional I/O expansion drawer graphically in a left-to-right order that corresponds to the numbers on the back of the system chassis or expansion drawer. An icon represents each slot, and Slot Manager displays different slot icons depending on the state of the slot (locked, unlocked, empty, full, error status, and so on). Below each slot icon, Slot Manager displays the slot label for that slot.

**Note:** Slot Manager displays the slots in lowest-to-highest order, from left to right. However, the actual system chassis could have the lowest slot value on the right. In this case, the display in Slot Manager is the reverse of the actual system chassis.

### Tree view

The Tree View page displays a graphical tree hierarchy of the slots and adapters found in the managed system. The left pane of the page displays icons representing the managed system, each system chassis, and each I/O expansion drawer, all slots, and all adapters in a tree that can be expanded and collapsed. The slots in the tree are presented in a lowest-to-highest order that corresponds to the numbers on the back of the system chassis or I/O expansion drawer.

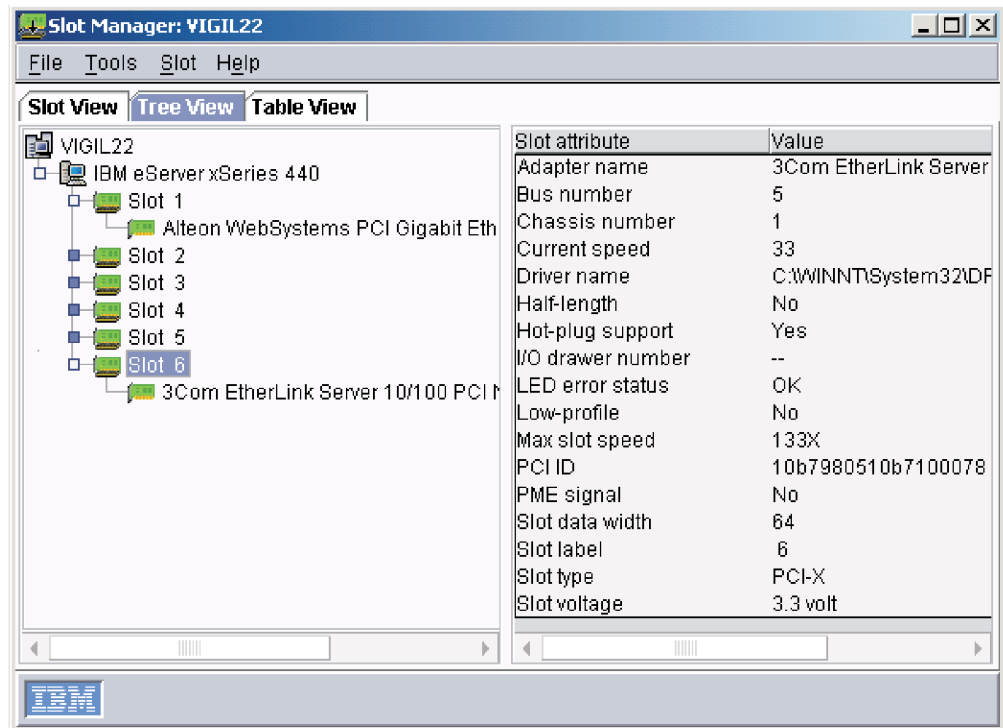


Figure 25. Slot Manager window using Tree View

The right pane shows the attributes for the item (system chassis, I/O expansion drawer, slot, or adapter, but not managed system) currently selected in the tree. To view attributes for a different item, click the applicable item in the tree.

### Table view

The Table View page displays a table of slots found in the managed system, which includes the supported system chassis and any optional I/O expansion drawers. This table contains columns that identify the various slot and adapter attributes.

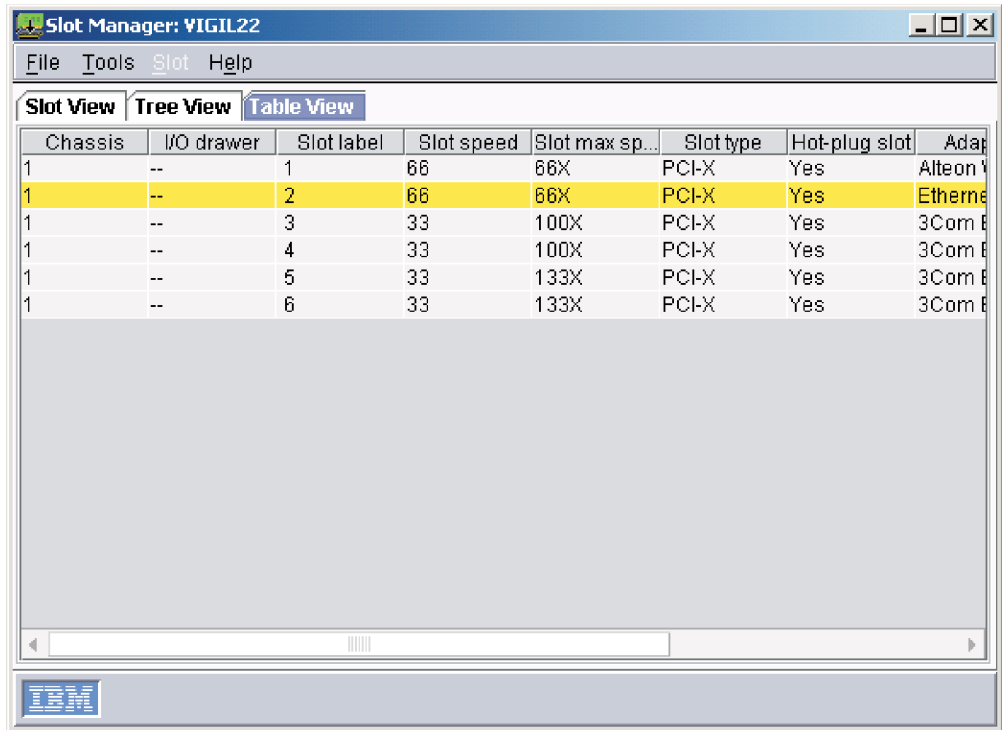


Figure 26. Slot Manager window using Table View

The table is ordered on the **Slot label** column. Click a different column name to sort the table in ascending order on that column. When you click the column name again, the Table view sorts the table in descending order on that column.

If an adapter is running at less than optimal speed, the Table view displays the row identifying the corresponding slot with a yellow background color. Run the Analyze function to determine whether a better slot location exists for the adapter. However, in some situations, the capabilities of the adapter might be greater than what is possible on the system chassis or I/O expansion drawer.

### Understanding slot error status

When the Attention light-emitting diode (LED) is lit for a slot, you can use the Slot Manager to determine the cause of the error. Slot Manager reports the error status of a given slot in multiple ways:

- In the Slot view and Tree view, additional icons are displayed for a slot to indicate that it has an error status.
- In the Slot view and Tree view, the right pane contains the LED error status attribute that lists the error status for the selected slot.
- In the Table view, the **Attn LED Status** column displays the error status for the selected slot.

The hardware can turn on the Attention LED for several hardware reasons, but Slot Manager cannot turn it off.



The error status of a slot can be any of the following:

- OK (no error)
- Hot eject successful
- Bus speed mismatch
- Power fault on card in slot



- Surprise removal occurred
- Slot disabled at current speed
- Too many adapters on bus
- Bus connection error

When a slot has an error status, two additional icons are displayed for the slot.

These two icons indicate that the slot needs attention  and that additional information  is available.

The following illustration shows examples of the slot icons in the Slot view and Tree view that indicate an error status.

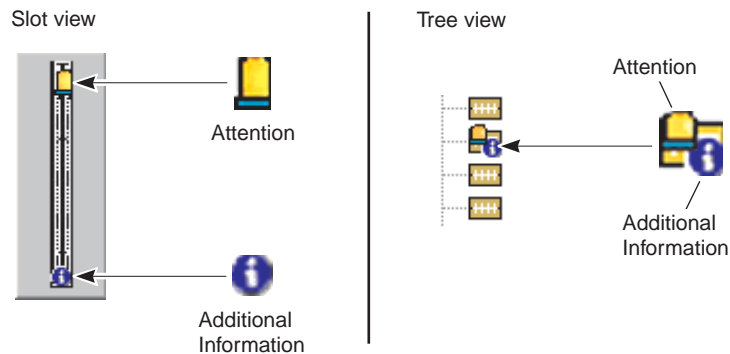


Figure 27. Examples of slot error status

**Note:** After an adapter is ejected, Slot Manager indicates that the slot has an error status. The error status remains until you physically close the adapter-retention latch on the affected slot. After you close the latch, Slot Manager automatically refreshes the window.

When a slot error status is Bus speed mismatch, the hardware turns off the slot. This prevents Slot Manager from detecting enough PCI information about the adapter to offer any solutions.

### Working with slots and buses

You can use the Lock functions to lock a specific adapter slot or bus or all slots in a specific system chassis or I/O expansion drawer so that when you run a PCI analysis, that slot, slots, or bus are not included in the solution. To lock a slot, in the Tree or Slot view, right-click the slot you want to lock; then, click **Lock slot**. To lock a bus, in the Tree or Slot view, right-click the bus you want to lock; then, click **Lock bus**. To lock all slots in a system chassis or I/O expansion drawer, in the Tree or Slot view, right-click the system chassis or I/O expansion drawer you want to lock; then, click **Lock unit**. After a lock is enabled, a lock icon is displayed on the slot icon or icons.

You can use the Blink function to flash the Attention LED associated with any slot and to locate the position of a slot in a chassis. The Blink function works for slots that support the Attention LED feature. To blink the Attention LED associated with a slot in the managed system, in the Slot or Tree view, right-click the slot; then, click **Blink slot**. After the Blink function is enabled, the Slot Manager window displays attention icons as appropriate. The physical Attention LED continues to flash until you disable the Blink function, you physically close the adapter-retention latch on the slot, or you restart the managed system.

Use the Refresh function to manually request an update of the system information shown in the Slot Manager window. By default, the view is refreshed automatically whenever an event occurs or when a slot flashes or turns off, for example, when a hot-add or hot-eject operation occurs. With the Refresh function, you can force a refresh request rather than waiting for an event to occur. To run the Refresh function, click **Tools** → **Refresh**.

### Analyzing PCI performance

The primary function of Slot Manager is to analyze the PCI performance of a managed system. The Analyze function provides this PCI performance analysis by examining several aspects of the system PCI bus and slot layout. Using the layout, along with the abilities of the adapters already installed in the managed system, the Analyze function runs a PCI optimization algorithm to determine the performance of the layout. The goal of the Analyze function is to have each adapter in the system running in its best mode of operation and each PCI or PCI-X bus in the system running at its highest bus speed.

If the Analyze function determines that the adapters are arranged in such a way that the managed system has performance issues, it displays information about these performance issues. If possible, it also provides a solution that describes recommended actions to optimize or improve the location of adapters. For example, it can describe where to move the adapters, what slots you can use, and what adapters to place into those slots.

After you have started Slot Manager, you can run a PCI performance analysis on the managed system by clicking **Tools** → **Analyze** from any view (Slot, Tree, or Table). The Optimization Steps window displays the results of the performance analysis.

In analyzing the PCI performance of the managed system, the Analyze function examines all slots in the system chassis and any optional I/O expansion drawers. This examination includes locked slots as well as turned-off slots. However, if a slot is locked, the Analyze function solution will not suggest relocating an adapter from or to the locked slot. Slot Manager locks all slots that contain startup devices, such as disk adapters. This avoids solutions that change the order of the boot devices, which can cause problems with starting the system or with disk-drive letter assignments. Additionally, Slot Manager locks any slots that have an error status of Bus connection error.

You can manually lock individual slots, all slots on a bus, or all slots in the system chassis or an I/O expansion drawer. See “Working with slots and buses” on page 49 for more information.

**Note:** Slot Manager cannot detect a PCI slot that is unusable because an optional serial port bracket is covering it on the system chassis. In this scenario, ensure that the affected slot is locked in Slot Manager so that it is not considered by the Analyze function.

**Potential performance issues:** Several factors can affect the managed system PCI performance, such as incompatible operating speeds between buses and adapters or exceeding the recommended number of adapters on a bus. The Analyze function categorizes these issues as major, moderate, or minor performance issues depending on the effect of the issue on system PCI performance.

If the PCI optimization routine finds no performance issues, the configuration is considered optimal. In this case, the Analyze function returns a message stating that no changes to the system are needed.

The performance issues that the PCI optimization routine can detect are described below.

*Major performance issues:* The Analyze function determines that there are major performance issues when one or more of the following scenarios occur on the managed system being analyzed:

- The adapters installed on any bus segment are not capable of operating at the same speed.
- A bus is exceeding the number of adapters it can support at a given bus speed. For example, a bus might have four slots but only two slots that can run at 66 MHz. If all four slots contain 66 MHz adapters, the bus is forced to run at a slower speed (in a PCI-backward-compatible mode) for all four adapters to work. The Analyze function will detect this and report that the bus cannot be optimized with the current number of adapters installed.
- A bus is operating at a speed or mode slower than the maximum capability of any adapter on that bus.

*Moderate performance issues:* The Analyze function determines that there are moderate performance issues when one or more of the following scenarios occur on the managed system being analyzed:

- A 32-bit wide bus contains a 64-bit PCI-X adapter.
- All adapters installed on any bus segment are not capable of the same operating mode (for example, PCI-X versus conventional mode).

*Minor performance issues:* The Analyze function determines that there are minor performance issues when there is at least one bus with multiple cards while another bus is empty. If it detects any unused buses, the Analyze function suggests configurations that place the adapters on all available buses. The resulting suggestion ensures that no bus has multiple adapters while another bus is empty.

**Optimization solution:** The Optimization Steps window displays the results of the performance analysis from the Analyze function. If the PCI optimization algorithm finds major, moderate, or minor performance issues, the Optimization Steps window displays these issues and, if possible, provides instructions for how best to rearrange the adapters.

The Optimization Steps window provides a graphical representation of the suggested layout and detailed steps for how to achieve this layout from the current configuration. In these steps, the adapter names are underlined, and when you click an adapter name, the corresponding slot icon is updated in the Slot view or Tree view to indicate the required action.

### Important

You must turn off the managed system before following any solution that recommends you take these actions:

- Move an adapter to a slot that does not support hot-plug operations.
- Move an adapter to a bus that is running at a higher speed than the adapter can run.

The system must be turned off when moving the adapter so that the bus speed is reset appropriately for that adapter when the system is turned back on. Otherwise, the managed system can return unexpected errors such as a Bus Speed Mismatch error for the suggested slot.

You can print the PCI analysis report. After you have run a PCI performance analysis, in the Optimization Steps window, click **File** → **Print**. Or, you can click **File** → **Copy** and paste the solution into a text-processing application. Slot Manager does not retain a history of solutions, so you must either print or copy the solution if you want to retain it.

### Adding adapters

Slot Manager has an Add Card wizard that works with the Analyze function to determine the most suitable slot in which to insert a new adapter.

The Add Card wizard comes with specifications for certain adapters. In the first window of the wizard, you can select from a list of supported adapters. If you are using an adapter that is not in the list, use the second window of the wizard to provide the specifications of the adapter. After you have selected or defined the adapter you plan to use, the wizard runs the Analyze function. When the analysis is complete, the Add Card wizard displays a suggested slot number to which the adapter can be added. If the Add Card wizard cannot find a suitable slot, it displays a message to that effect.

The Add Card wizard looks only for open slots in which to hot-add the adapter. It will not suggest that other adapters be moved first. The Add Card wizard will not suggest an available slot if using that slot for the new adapter would make the system performance suboptimal. If the Add Card wizard does not suggest a slot for the new adapter, and you still decide to add the new adapter to an available slot in the system, you should run the Analyze function to determine any performance issues that might have been introduced and address them as applicable. For details, see “Analyzing PCI performance” on page 50.

#### Notes:

1. Slot Manager cannot validate the information gathered by the Add Card wizard against the physical adapter until the adapter is installed in the system. If you enter the wrong adapter information in the wizard, the adapter might not work properly in the suggested slot, or the system might not be optimized if the adapter is used in the suggested slot.
2. Slot Manager cannot detect a PCI slot that is unusable because an optional serial port bracket is covering it on the system chassis. In this scenario, ensure that the affected slot is locked in Slot Manager so that it is not considered by the Analyze function.

### Filtering for Slot Manager events

You can create an event filter in the Event Filter Builder that specifically filters for Slot Manager events. Event filters are used in event action plans, which can be set up to notify you when a specific event occurs. In the Event Filter Builder window, on

the Event Type page, expand the **Active PCI** tree, then expand the **Slot events** tree to display four events specific to Slot Manager:

**Power fault**

Adapter has a power fault.

**Surprise removal of an adapter**

A user lifts the adapter-retention latch on a slot without first ejecting the adapter through the operating system.

**Add complete**

The operating system detects that a previously empty slot now has a powered-on adapter. This event occurs after a successful hot-add operation.

**Eject**

A user requests that the operating system eject an adapter. The eject operation unloads the driver from the adapter and powers off its slot in preparation for removing the adapter while the system is powered on.

**Note:** Other Slot Manager events might be listed under the **Slot events** tree in the Event Filter Builder window. These are events that are only listed in IBM Director after they occur. You can create event filters using these events also.

---

## Asset ID

You can use the Asset ID task to view lease, warranty, user, and system information, including serial numbers. You can also use Asset ID to create personalized data fields to add custom information.

Asset ID retrieves the hard disk drive serial numbers, system serial number, and system board serial number for all the Enhanced Asset Information Area EEPROM-enabled systems. Or, if a managed system does not have the Enhanced Asset Information Area EEPROM, Asset ID writes to and retrieves information from the Desktop Management Interface (DMI) database to maintain much of the information needed for asset tracking.

To start the Asset ID task, in the IBM Director Console Tasks pane, drag the **Asset ID** task onto a managed system. The Asset ID window opens.

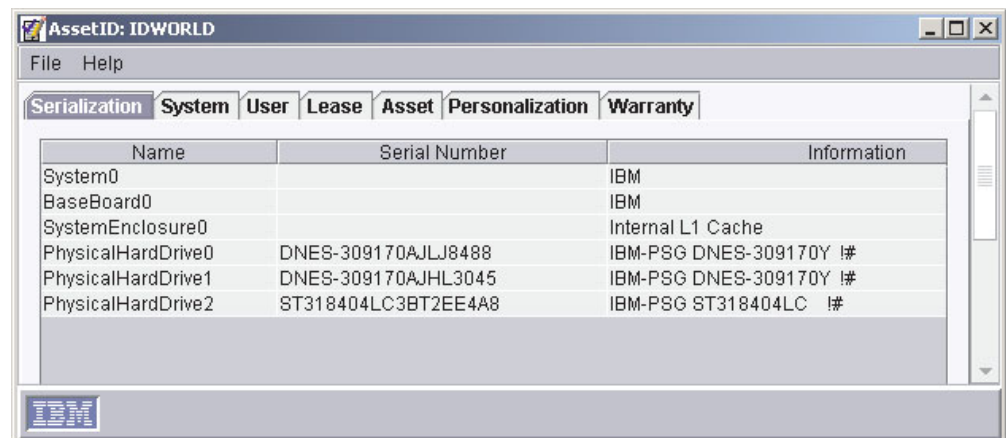


Figure 28. Asset ID window

There are seven pages:

**Serialization**

Displays information about the serial numbers.

**System**

Displays information about the managed system or device.

**User** Displays information about the logged-in user.

**Lease** Displays the lease agreement information.

**Asset** Displays the inventory information about the managed system.

**Personalization**

Displays a free-form window where you can type information about your users or systems. There is a 64-character maximum for each of these fields.

**Warranty**

Displays information about the warranty on the managed system or device.

Click the applicable tab to view the information.

---

## BladeCenter Assistant

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

Within the BladeCenter Assistant, there are four subtasks:

- BladeCenter Configuration
- BladeCenter Management
- Deployment wizard
- Switch Management LaunchPad

You can use the first two subtasks for BladeCenter unit configuration and management. You can use the Deployment wizard subtask to configure a BladeCenter chassis and create a reusable profile that can be used to configure new BladeCenter chassis automatically. The Deployment wizard subtask is discussed in more detail in the *IBM Director 4.1 Installation and Configuration Guide*. The Switch Management LaunchPad subtask is used to launch a third-party application to manage your switches.

## Starting the BladeCenter Configuration or BladeCenter Management subtask

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

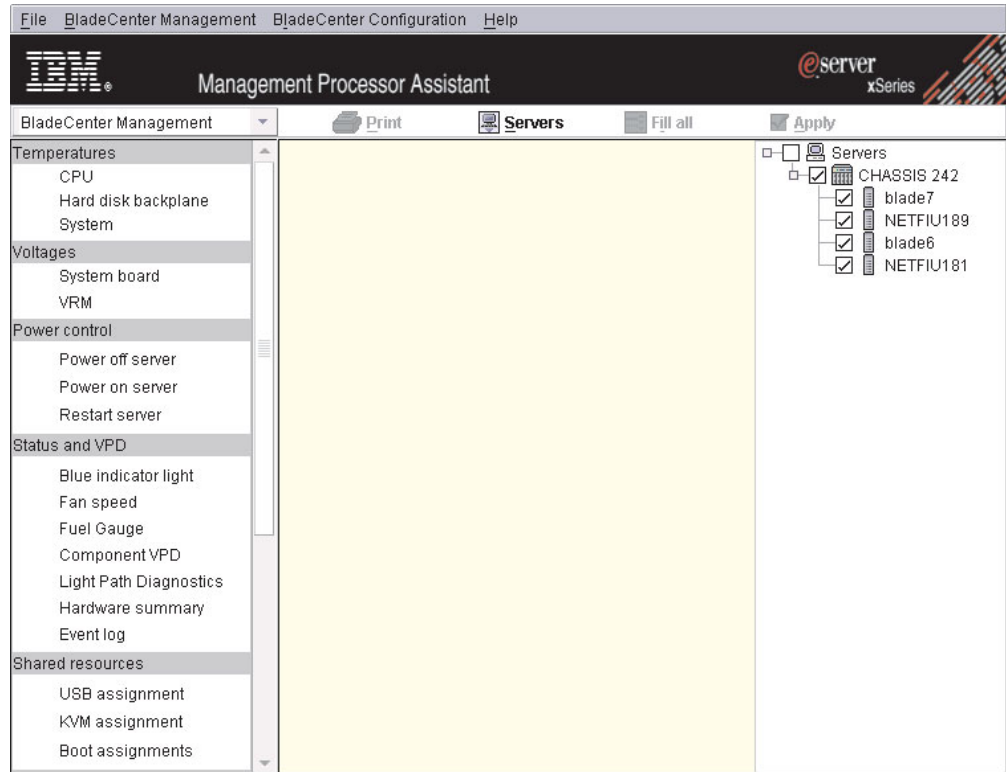


Figure 29. Management Processor Assistant window when activating the BladeCenter Management subtask

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 blade servers that you targeted when starting the task and the associated BladeCenter chassis and all attached blade servers.

Using the “Fill all” function, you can mass configure many servers at the same time by copying the values from the row for one system to other systems selected. When the source row provides parameters that are not applicable for a target system, the row for that system is skipped. To copy the values in one row to all selected entries in a table, select the other entries using the Ctrl key; then, click **Fill all**.

To save any changes, click **Apply**. Depending on the subtask, this function updates the information stored on IBM Director Server, modifies the configuration information on a service processor, or runs a management action.

You can also sort on the contents of a column by clicking the appropriate column heading.

## BladeCenter Configuration subtask

You can use the BladeCenter Configuration subtask to view and configure BladeCenter chassis and blade server information.

## 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.

## 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 profile, 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**.

## Creating and changing login profiles

You can use the login profiles to access a service processor that requires a user ID and password. You can create up to 12 login profiles.

Complete the following steps to create or change login profiles:

1. Click **Configuration** → **Login profiles**.
2. To add a new user profile, click **Add an entry**.  
To change a user profile, click the user profile you want to change and make changes.  
To delete a user profile, click the user profile you want to delete, and manually delete the information displayed in the **User ID** field.
3. Click **Apply**.



## BladeCenter Management subtask

You can use the BladeCenter Management subtask to view BladeCenter chassis, blade server, and switch information, power on and off servers, restart a managed system, view and change KVM policy and assignment, view and change USB policy and assignment, and much more.

### 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 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 blade servers on and off

You can power a blade server on or off remotely.

Complete the following steps to power off a blade 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 blade server:

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

Complete the following steps to restart a blade server:

1. Click **BladeCenter Management** → **Power control** → **Restart server**.
2. Select the **Restart immediately** check box.
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 start (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**.

### **Viewing and changing 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**.

### **Viewing and changing switch settings**

You can view and change switch 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 switch vital product data (VPD), 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**.

## Deployment wizard

You can use the BladeCenter Deployment wizard to configure a new BladeCenter chassis when it is added to the IBM Director environment. See the *IBM Director 4.1 Installation and Configuration Guide* for more information about how to use the Deployment wizard.

## Switch Management LaunchPad subtask

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

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

---

## Capacity Manager

The Capacity Manager task, part of the Server Plus Pack, is a resource-management planning tool that you can use to monitor managed-system performance. It identifies bottlenecks and potential bottlenecks, recommends ways to improve performance through performance analysis reports, and forecasts performance trends. Similar to the Resource Monitors task, which you can also use to monitor resource utilization, Capacity Manager can be used to capture resource-monitor trends and for longer term resource-utilization monitoring. (See “Resource Monitors” on page 109 for more information.) You can use Capacity Manager on any managed system that has the Capacity Manager Agent installed on it.

In IBM Director Console, Capacity Manager has three components:

### **Monitor Activator**

Displays the status of resource and performance analysis monitors on managed systems; you can specify which monitors are active.

### **Report Generator**

Includes Report Definitions, which you can customize for generating reports.

### **Report Viewer**

Provides four views of your generated report data and graphs of monitor performance.

## Viewing and activating monitors

Using the Monitor Activator subtask in Capacity Manager, you can view which resource monitors, including performance analysis monitors, are currently active on a managed system or group. And, you can activate and deactivate monitors on a managed system. The performance analysis monitors are activated by default when you install Capacity Manager.

There are four types of performance analysis monitors:

- CPU utilization
- Memory usage
- Disk usage
- Network utilization

Capacity Manager automatically discovers new resource monitors and removes monitors for devices that no longer exist. Performance analysis monitors for Windows network adapter cards and physical disks are discovered and checked once every 24 hours or whenever the Capacity Manager Agent is restarted.

To view the monitors that are present on a managed system or group, in the IBM Director Console Tasks pane, expand the **Capacity Manager** task. Drag the **Monitor Activator** subtask onto a managed system or group that has the Capacity Manager Agent installed on it. The Monitor Activator window opens.

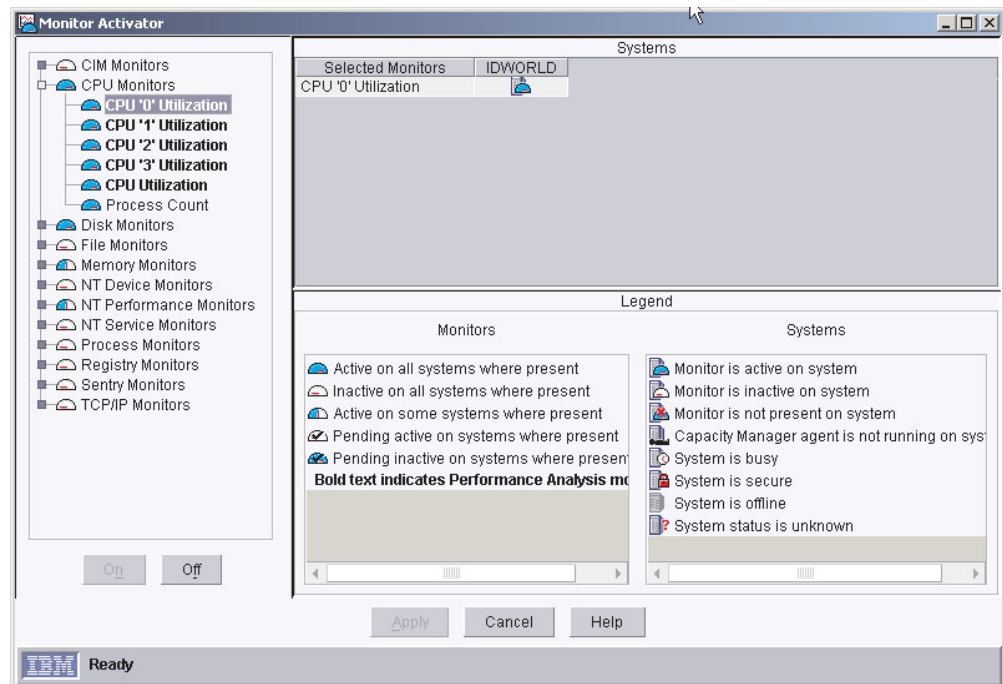


Figure 30. Monitor Activator window

In the left pane, all monitors are displayed in a tree structure; each monitor has an icon to indicate its status. The names of performance analysis monitors are displayed in bold. For example, in Figure 30, **CPU "0" Utilization** is a performance analysis monitor, and **Process Count** is a resource monitor.

In the Systems pane, an icon is displayed beside each managed system or group to indicate its status. In the Legend pane, the monitor and managed-system icons and their descriptions are displayed.

To activate a monitor, in the left pane, click the monitor; then, click **On**. To deactivate a monitor, in the left pane, click the monitor; then, click **Off**. When you are finished activating and deactivating monitors, click **Apply**. The Monitor Activator window closes. As a safety feature, you cannot select a group of monitors by clicking the group name. You must select each monitor individually. If you have deactivated a monitor, it will not be reactivated until you manually reactivate it.

## Identifying bottlenecks

When you schedule Capacity Manager to periodically check for bottlenecks, or when you choose to generate a report manually, the performance analysis function looks for bottlenecks in managed-system hardware performance. When one or more performance analysis monitors meet or exceed their preset threshold settings,

and you have selected the **Generate Bottleneck events** check box when you defined the report, a bottleneck event is generated. You can adjust the threshold settings on performance analysis monitors, but the default settings cannot be changed without impairing the performance analysis function.

Corresponding to the types of performance analysis monitors are the four main types of bottlenecks:

- CPU
- Memory
- Disk
- LAN adapter

When the performance analysis function detects a bottleneck, it diagnoses the problem and determines a potential solution. The performance analysis section of the report details the problem and recommendations.

Multiple bottlenecks can also occur. For example, a disk bottleneck and a memory bottleneck can occur concurrently. In this case, the performance analysis algorithm recognizes that insufficient memory can lead to disk thrashing, so the recommendation is to add more memory and leave the disk drives unchanged. As systems and devices often interact in this way, each combination of bottlenecks (that is, CPU, memory, disk, and LAN adapter) constitutes a separate bottleneck with its own recommendation.

Often when one bottleneck occurs, other bottlenecks are not evident because the first bottleneck slows the system. A latent bottleneck is one that is not evident while the system has slowed down. Performance analysis reports a managed system or device as having a latent bottleneck if a performance monitor for that system or device exceeds the warning threshold at least 50% of the time that the performance monitor for another system or device is constrained.

You can use one of the following methods to determine whether a managed system or group has bottlenecks:

- Using the Report Generator function, schedule a report to be generated when a bottleneck is detected. Complete the following steps:
  1. Schedule performance analysis to check for bottlenecks and generate an event when a threshold is exceeded or met.

If a bottleneck is found, a report is generated and stored in the IBM\Director\reports directory (unless you specify another directory in the report definition). In the performance analysis section, the bottleneck is listed and recommendations for correcting the bottleneck are given. An event is generated and is recorded in the event log.

If no bottleneck is found, nothing happens.
  2. Create an event filter, which you can use as part of an event action plan to notify you when an event is generated and, therefore, that a bottleneck has occurred.
- Using the Report Generator function, generate a report immediately.

A report is generated and displayed. If a bottleneck is found, in the performance analysis section of the report, the bottleneck is displayed by showing the monitor name in bold and in red, and recommendations for correcting the bottleneck are given. An event is generated and is recorded in the event log.

If no bottleneck is found, the Report Viewer window opens to display other data collected, and the performance analysis icon indicates that no bottlenecks were found.

## Receiving automatic notification of a bottleneck

Capacity Manager uses the performance analysis function to determine where and when bottlenecks occur. Complete the following steps to be notified automatically when a bottleneck occurs:

1. Schedule performance analysis to check for bottlenecks and generate an event when a threshold is exceeded or met, thus indicating a bottleneck. If a bottleneck is detected, an event is generated and a report is generated.
2. Create an event filter, which can be used as part of an event action plan to notify you of the event.

**Note:** Performance analysis is available only for managed systems running the Windows or Linux operating systems.

### Scheduling to check for bottlenecks

You can schedule the performance analysis function to check for bottlenecks on a regular basis and generate an event that is added to the event log whenever a bottleneck is detected. If a bottleneck is detected, a report is generated.

Although you do not have to check for bottlenecks on an hourly basis, as in the following procedure, you must be sure that the **Generate bottleneck events** check box is selected for the report definition you are using. Otherwise, an event action plan cannot notify you that a bottleneck has occurred, because event action plans depend on events to trigger an event action.

Complete the following steps to check for bottlenecks on an hourly basis:

1. In the IBM Director Console Tasks pane, expand the **Capacity Manager** task.
2. Expand the **Report Generator** subtask. Drag **Hourly Bottleneck Events** onto the managed system or systems or group you want to monitor for bottlenecks.
3. Click **Schedule**. The New Scheduled Job window opens.
4. Type a job name, and select a date and time for the job to run initially. Click **Advanced** to schedule the job to repeat at regular intervals. The New Scheduled Job window opens.
5. On the **Date/Time** page, select the **Repeat** check box. The Repeat window opens.
6. In the Repeats group box, select **Hourly** from the list.
7. Click **OK**.
8. Click **File** → **Save As**. The Save Job window opens.
9. Type a descriptive name for the scheduled job. Click **OK**. A confirmation message is displayed indicating you have successfully saved the job.
10. Click **OK** to close the message window.

If you use this procedure, the specified managed systems are checked every hour for bottlenecks. If a bottleneck is detected, two things happen:

- A report is generated and saved in the IBM\Director\reports directory (unless you specify another directory in the report definition).
- Each managed system with a bottleneck generates an event, and the event is displayed in the IBM Director event log.

## Creating an event filter

You must create an event action plan if you want to be notified when a bottleneck occurs. This section covers creating an event filter only. You must create an event action plan, customize an event action, and apply the event action plan to the managed systems or groups you selected to monitor using the Hourly Bottleneck Events report option in the preceding section. For more information about creating and implementing event action plans, see “Event action plans” on page 20.

Complete the following steps to create an event filter specifically for bottlenecks:

1. In IBM Director Console, click **Tasks** → **Event Action Plan Builder**. The Event Action Plan Builder window opens.
2. Click **File** → **New** → **Simple Event Filter**. The Simple Event Filter Builder window opens.
3. In the Event Type page, in the left pane, clear the **Any** check box. In the right pane, expand **Capacity Manager**; then, expand **Bottleneck**, and click **Recommendation**.

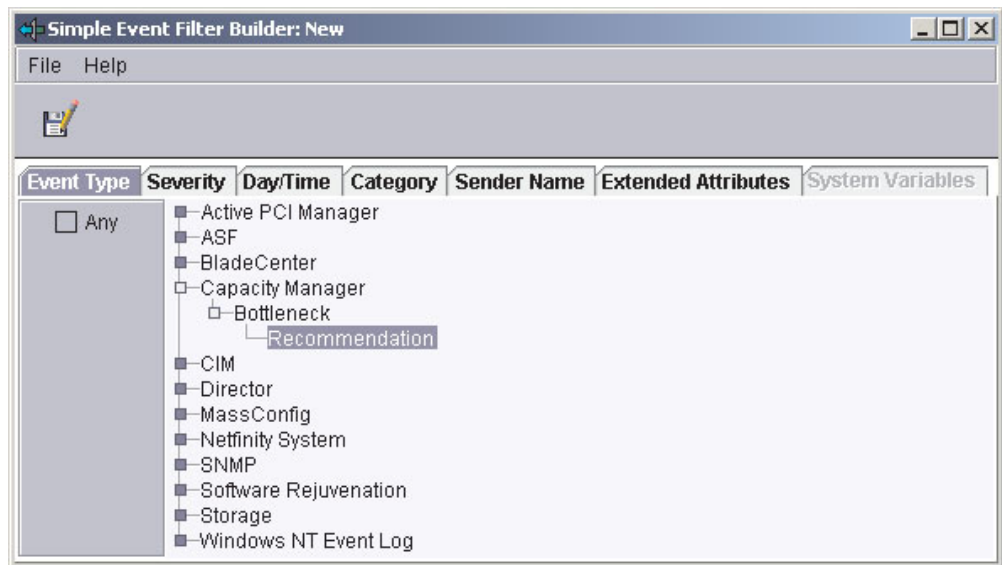


Figure 31. Simple Event Filter Builder window

4. Click the **Extended Attributes** tab. Clear the **Any** check box.
5. In the **Keywords** list, click **Hours since bottleneck first started**. In the **Operator** list, click **Equal to**. In the **Values** field, type 2.
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 **Simple Event Filter**.

## Generating a report

You can generate a report for immediate viewing, or you can save the report to a file for later viewing.

To generate a report, you must specify the details you want included in the report. You can create a report definition or use a predefined report definition. Five predefined report definitions are included in Capacity Manager:

- Daily report to viewer



- Hourly bottleneck events to file
- Hourly report to viewer
- Monthly report to file
- Weekly report to file

To use a predefined report definition to create a report, drag the report definition you want to use onto one or more managed systems or group. A status window opens to indicate the progress.

If the report definition specifies that the report is generated to the report viewer, the Report Viewer window opens. If the report definition specifies that the report is generated to a file, the report, when generated, is saved automatically to the IBM\Director\reports directory (unless you specify another directory in the report definition), whether you click **Execute Now** or **Schedule**.

### Creating a report definition

To create a new report definition, expand the **Report Generator** subtask; then, double-click **New Report Definition**. The Report Definitions window opens.

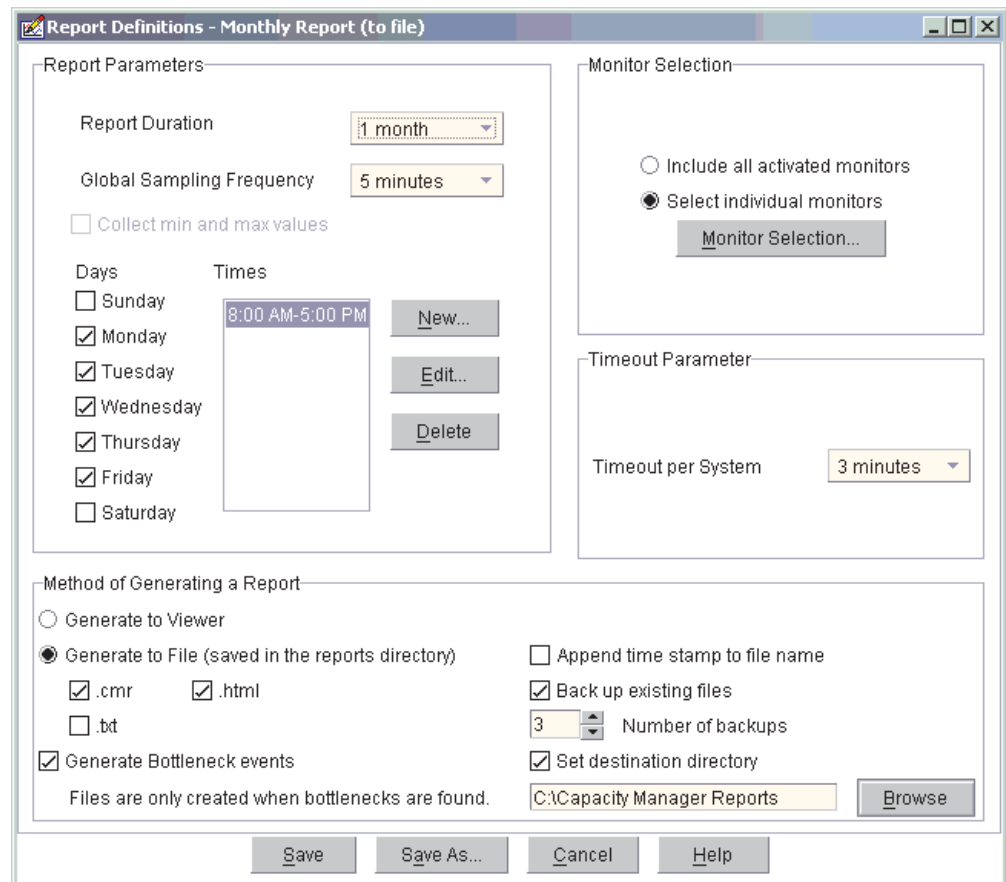


Figure 32. Report Definitions window

In the Report Definitions window, selecting the **Collect min and max values** check box specifies that the minimum and maximum data points for each sample are collected. An advantage to collecting the minimum and maximum data points is that you can use a slower sampling frequency, which collects data less frequently, reducing the size of the report and still receiving informative managed-system

performance data. Also, if memory usage is an issue, you should consider using a slower sampling frequency. Note that the average is always collected.

**Timeout per system** specifies the number of minutes Capacity Manager will wait for a system to respond before considering the system unable to provide the data.

After you have customized a report definition, you can generate a report that includes only those parameters you have specified.

Complete the following steps to generate a report:

1. In the IBM Director Console Tasks pane, expand the **Capacity Manager** task.
2. Expand the **Report Generator** subtask; then, drag a report definition onto one or more managed systems or group.
3. If you selected a report that is generated to a file, click **Execute Now**, or click **Schedule** to schedule the report for generation at a later time. (For more information about scheduling tasks, see “Scheduler” on page 27.)

If you click **Execute Now**, a status window opens to indicate the progress. The report is saved automatically to the IBM\Director\reports directory.

If the report definition specifies that the report is generated to the report viewer, the Report Viewer window opens.

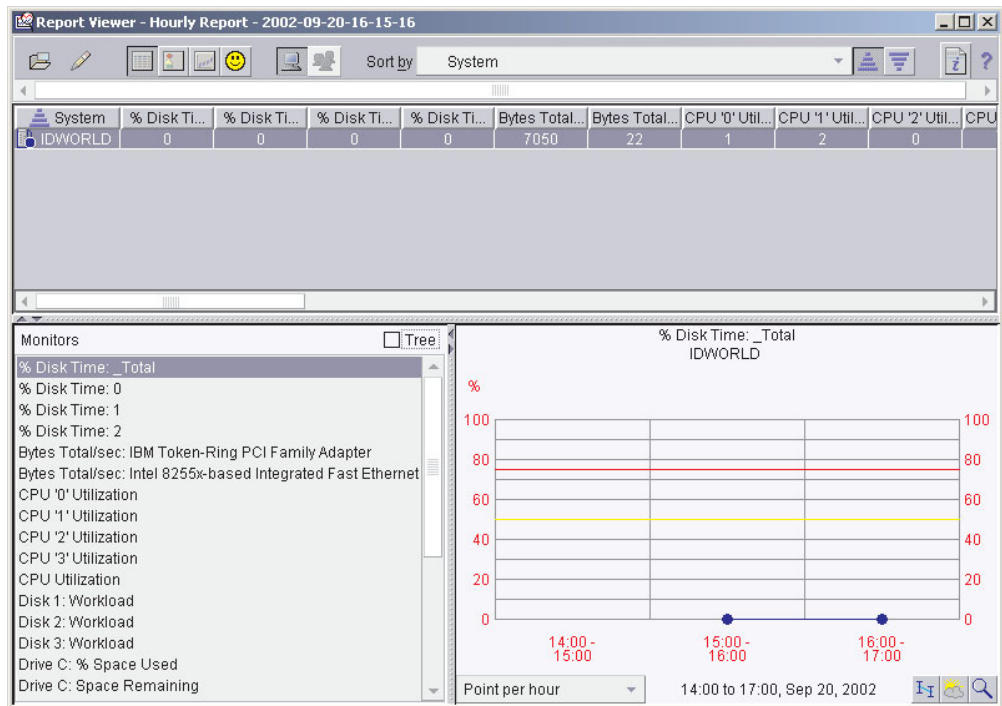


Figure 33. Report Viewer window

**Report Viewer interface:** The pane in the upper half of the viewer displays the managed system or systems and associated information. You can view this managed-system information in six ways:

**Table view**

Displays tabular listings of managed systems, monitors, and parameters. Table cells for monitors are highlighted in red if the monitor value is above the critical threshold that you defined, or yellow if the monitor value is

above the warning value. This view is the default view and is displayed automatically when the Report Viewer window opens.



**Icons view**

Displays all managed-systems information in one pane.



**HyperGraph view**

Displays the Table view cell values graphically for a selected monitor or managed-system parameter for all managed systems in the report. An icon on the graph represents each managed system.

**Performance Analysis**

Displays the performance analysis report in the upper pane. The icon that is displayed is dependent on the status of the performance analysis section of the report. (See Table 3.)



**System view**

Displays the data for an individual managed system. This is the default mode.



**Group mode**

Displays the data for a managed group as a whole (if the report was generated for a group; otherwise, this option is not available).

You can change the view by clicking the applicable button in the toolbar.

The Performance Analysis icon that is displayed in the toolbar is dependent on the status of the performance analysis report. The Performance Analysis function icons and their descriptions are listed in the following table.

*Table 3. Performance analysis icon descriptions*

Icon	Description
	The performance analysis report is ready and will be displayed in a moment.
	Performance analysis is complete. The report viewer freezes while the results are loaded for viewing.
	The performance analysis report is ready and has no bottleneck recommendations, although the Details section might discuss some current or latent bottlenecks.
	The performance analysis report is ready, and you have bottlenecks on a managed system.
	The performance analysis report could not be prepared. Click  (Edit) → <b>Enable Performance Analysis</b> and regenerate the report.
	The performance analysis report could not be prepared. You are missing one or more critical monitors, or you have less than two hours of data collected.

The Monitors pane, in the lower-left portion of the Report Viewer window, lists managed-system monitors alphabetically. If a monitor is enclosed in brackets, the managed system or device associated with that monitor has been removed. You can select the **Tree** check box to display the monitors in a tree structure.

The lower-right pane of the Report Viewer displays a graph of the monitor selected in the Monitors pane. If you select System mode in the toolbar, you see a line graph of the performance of the managed system. If you select Group mode, you see a

graph of the performance of all the managed systems in the group, with the data for each managed system graphed separately. Within this pane, you can use the following tools:

#### **Resolution**

Adjusts the density of the points in the graph. You can change the resolution by selecting from the list at the bottom left of the pane. This tool uses an average of the raw data points to present the requested number of points for a given period of time.

#### **Trend**

Displays a trend graph of the data.

#### **Forecast**

Displays predicted data based on the least-squares linear regression calculations of future managed-system performance. (See “Viewing a performance forecast graph” on page 70 for more information.)

#### **Zoom**

Expands a selected portion of the graph time line.

## **Viewing report details**

The performance analysis report consists of two sections:

#### **Recommendations**

Shows only the subset of details on which you need to act.

#### **Details**



Shows everything that was found, and contains links so you can see a graph of the performance of the monitor in question.

The managed systems with the most severe bottlenecks appear first on the report list. A bottleneck that is reported in the Details section is displayed in the Recommendations section if it meets one of the following criteria:

- It occurred on the last day of the report.
- It occurred more than 25% of the time, and it occurred more than any other bottleneck on that managed system.
- It has a high probability of occurring in the future. However, performance analysis must have enough data to make a reliable forecast.

## **Saving and printing a report**

You can save a report in HTML for later viewing and printing in a Web browser, or you can print report information directly in IBM Director.

To print the graph pane, in the Report Viewer window, click  (File) → **Print** → **Graph Print**. To print the performance analysis report, click  (File) → **Print** → **Performance analysis report**.

A report saved in HTML contains the following sections:

#### **Table of Contents**

Contains links to the other sections.

#### **Report Table**

Presents the same monitor and managed-system data that is also available in the Report Viewer in the Table view.

### Report Information

Includes the file name, analysis start and end dates, days of the week and hours of coverage, name of the report definition, and a list of any managed systems that were requested but not included in the report.


### Performance Analysis recommendations

Recommends remedies for the most serious bottlenecks.


### Performance Analysis details

Includes information about the frequency and duration of both active and latent bottlenecks and their remedies.

Complete the following steps to save a report summary on the management console as an HTML file:

1. Click  (File) → **Export report to local HTML**. The “Export report to local HTML” window opens.
2. Type a new file name and click **Save**.

Complete the following steps to save a report summary on the management server as an HTML file:


1. Click  (File) → **Export report to remote HTML**. The “Export report to remote HTML” window opens.
2. Type a new file name and click **Save**.

After you save the report as an HTML file, you can print the report from a Web browser. A printed version of the report includes the monitor and managed-system parameter information from the Table view.

## Viewing previously generated reports


Complete the following steps to view a previously generated report:

1. In the IBM Director Console Tasks pane, expand the **Capacity Manager** task.
2. Double-click **Report Viewer**. The “Open remote report” window opens.
3. If you want to view a report that has been saved to the management server, select a file and click **Open**. The Loading Report window displays the progress. Then, the Report Viewer window opens and displays the report.

If you want to open a report that has been saved to the management console, click **Cancel**; then, click  (File) → **Open local report**. The “Open local report” window opens. Select a file and click **Open**. The Loading Report window displays the progress. Then, the Report Viewer window opens and the report is displayed.


## Predicting future performance

Using the Forecast function, you can review a prediction of future performance of selected managed systems. Capacity Manager uses forecasting in the following components:

- In the performance analysis section of a report. If there are no realized bottlenecks, Capacity Manager uses forecasting to predict, with a level of confidence, if and when it foresees a monitor performance bottleneck.
- In a managed-system monitor performance graph. On a graph of a selected monitor for one or more managed systems, you can click  (Forecast) to see a forecast of the performance on the selected managed systems. The graph depicts both the observed data and the forecast.

To calculate future performance, Capacity Manager applies a wavelet transform to the monitor data prior to performing a least-squares linear regression. With this transformed data, it computes a forecast line with a 95% prediction interval. The forecast duration is equal to the duration of the observed data. For the forecast to be valid, Capacity Manager must have a minimum of 24 days of previously collected data where the managed-system monitors have been running at least 50% of the time.

## Viewing a performance forecast graph

To view the forecast graph for a selected managed system, in the Report Viewer window, click  (Forecast) in the lower-right corner of the lower-right pane. Capacity Manager displays the forecast graph for the monitor selected.

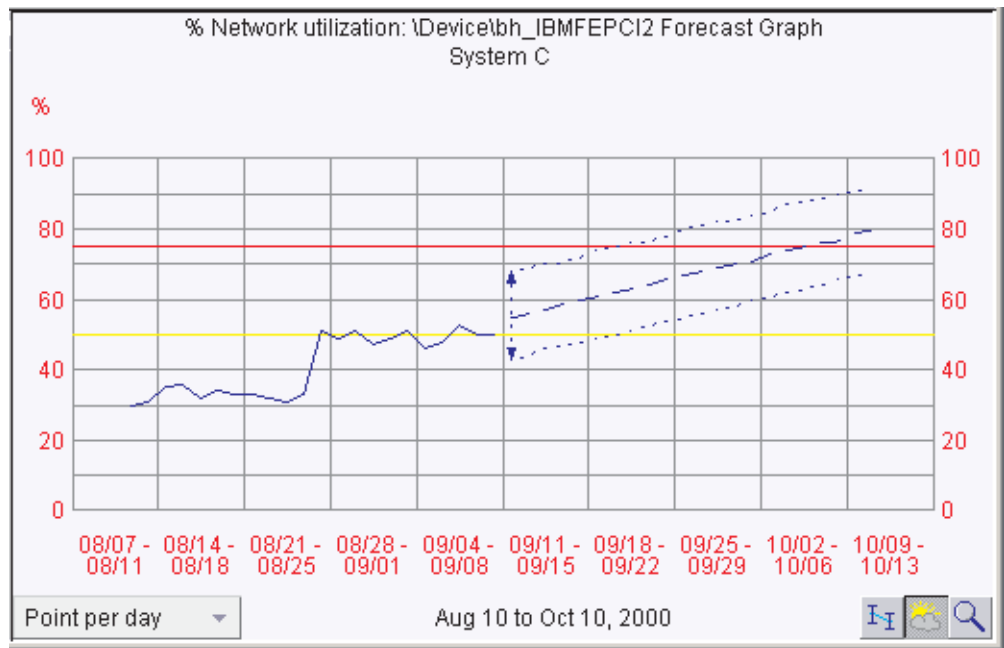


Figure 34. Lower-right pane in the Report Viewer window displaying a performance forecast graph

### Notes:

1. You cannot use the Zoom tool and the Forecast tool at the same time.
2. The forecast data is more meaningful for managed systems that are individually graphed rather than shown in a trend graph. To change from a trend graph to a graph of individual managed systems, either set your trend graph threshold to a higher number or select fewer managed systems to graph at one time.

### Forecast display details

The forecast line is a dashed line with an arrow at the end. This line describes possible future data values that are consistent with the prediction that an actual future data value will fall within equal probability above or below the forecast line. The forecast duration is equal to your data-collection period. For example, if you have a month of collected data, the forecast will be for a month into the future.

The prediction interval is represented by the dotted lines above and below the forecast line. The prediction interval represents the range of data values that are located above and below the forecast line and are consistent with the prediction


that an actual future data value will fall within the interval with a probability of 95%. The width of the interval depends on the variability of the observed monitor data: the greater the variability, the wider the prediction interval. The prediction interval is displayed when you request a forecast of a single managed system. Graphs of multiple managed-system forecasts do not show prediction intervals.

If you do not know how to interpret a wide prediction interval for a forecast, select a finer resolution of your data from the **Resolution** list. Your data points might have a broad variance that is hidden by averaging that occurs when data is displayed at a coarser resolution.

**Notes:**

1. The vertical bar at the beginning of the forecast data depicts the range.
2. The gap between the actual collected data and the beginning of the predicted data serves as a separator between these two data sets.

## Changing settings

Accessed through the Report Viewer window by clicking  (Edit menu) → **Settings**, the Settings window consists of three tabbed pages:

- **Graph**
- **Window**
- **Monitors**

Use these pages to configure the appearance of the graph in the Graph pane, the appearance of the viewer, and threshold settings for each monitor, respectively.

---

## CIM Browser

The Common Information Model (CIM) Browser task provides in-depth information that you can use for problem determination or developing a system-management application using the CIM layer.

To provide data through the CIM Browser task, a managed system must have a Common Information Model Object Manager (CIMOM) installed that the IBM Director CIM Agent detects and uses.

You can use the CIM Browser task to perform the following tasks:

- View the CIM structure for a selected CIM-enabled managed system
- View property values for selected classes
- Set values for individual properties
- Execute the methods of selected class instances
- Create browser subtasks, or shortcuts, for specific CIM tasks

## Starting the CIM Browser task

To start the CIM Browser and view information for a single managed system, in the IBM Director Console Tasks pane, drag the **CIM Browser** task onto the managed system for which you want to view information. The CIM Browser window opens.

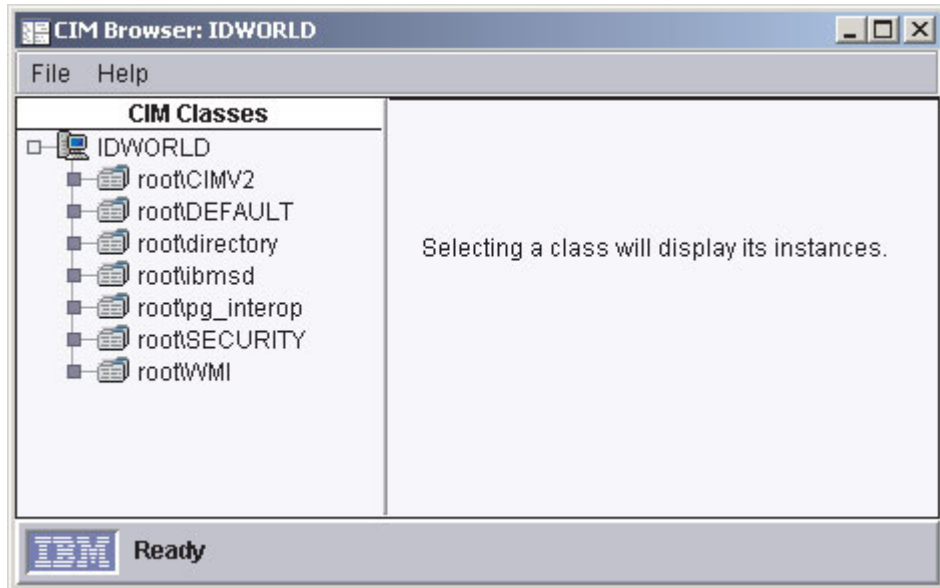


Figure 35. CIM Browser window

To open the browser for two or more managed systems, select the managed systems for which you want to view information. From the Tasks pane, drag the **CIM Browser** task to any system in the set of selected managed systems.

If one or more managed systems is not configured for CIM data, a message is displayed indicating that the target system or systems do not support the task. If a managed system is inaccessible, for example, if it is offline, the CIM Browser window opens, but you cannot expand the CIM tree of the managed system.

## Viewing information in the CIM Browser

To turn the displaying of managed system classes on or off, right-click a managed system and click **Display System Classes**. Managed system classes are indicated by a double underscore that precedes the class name. Also, you can expand the managed system tree to display the CIM name spaces of the managed system, then expand a name space to display its classes. The name space that contains the IBM-specific classes is `root\cimv2`.

To view an instance of a class, click the class name. If an instance of the class is found, the right pane splits. In the lower-right pane, the associated properties and methods are displayed under the **Properties** and **Methods** tabs, respectively. All classes can have associated properties or methods.

**Note:** Displaying instances of some CIM classes causes excessive resource usage on the managed system. The resource usage continues until all instances have been opened, even if the request is cancelled. Therefore, it is recommended that you avoid attempting to view instances of `root\cimv2:CIM_DirectoryContainsFile` and `root\cimv2:Win32_Subdirectory` on managed systems running Windows.

## Setting a property value for a CIM class instance

Do not change the value of a property unless you are thoroughly familiar with the structure and manipulation of CIM data. Improperly setting a property value can cause unpredictable results on the target system.



Complete the following steps to change the value of a property:

1. In the CIM Browser window, navigate to the class instance for which you want to change a property value. In the lower-right pane, the Properties page displays the class instance properties.
2. Right-click the property row you want to change and click **Set value**. The Set Value window opens and the current value is displayed.
3. Type the new value and click **OK**. If IBM Director cannot change the value on the target system, a message indicates the failure.

## Executing a method for a CIM class instance

Do not execute a method unless you are thoroughly familiar with the structure and manipulation of CIM data. Executing a method improperly can cause the connection to the target system to be lost.

Complete the following steps to execute a method for a CIM class instance:

1. In the CIM Browser window, navigate to the class instance that has the method you want to execute. In the lower-right pane, click the **Methods** tab. The associated methods are displayed.
2. Right-click a method and click **Execute**. The Execute Method window opens.
3. If the method has any input arguments, one or more input fields are displayed. Type the arguments in these fields.
4. Click **Execute** to run the method. If IBM Director cannot run the method on the target system, a message indicates the failure.

## Creating shortcuts to classes and methods

By creating browser subtasks, or shortcuts, you can bypass navigating through the class tree to reach a specific class or method. You can create two types of shortcuts:

- A user-selected class in which, when applied to a managed system, only the instances, properties, and methods associated with a specified class on the selected managed system are displayed.
- A user-selected method that, when applied to a managed system, is executed.

### Creating a CIM class shortcut

Complete the following steps to create a shortcut for a specific CIM class:

1. In the CIM Browser window, navigate to the class for which you want to create a shortcut.
2. Right-click the class name and click **Create browser task for class**. A window opens with the name of the class entered as the default name.
3. Type a new name, or keep the default name. Click **OK**. The new subtask is displayed under **CIM Browser** in the IBM Director Console Tasks pane.

You can use the shortcut by dragging it onto a CIM-enabled managed system that has the instance, properties, and methods associated with those in the shortcut.

### Creating a CIM class method shortcut

Complete the following steps to create a shortcut for a specific CIM class method:

1. In the CIM Browser window, navigate to the class that has the method for which you want to create a shortcut. In the lower-right pane, click the **Methods** tab to display the associated methods.
2. Right-click a method and click **Execute**. The Execute Method window opens.

3. If the method has any input arguments, one or more **Input** fields are displayed. Type the arguments in these fields.
4. Click **Save**. A window opens with the name of the method entered as the default name.
5. Type a new name or keep the default name. Click **OK**. The new shortcut is displayed under **CIM Browser** in the IBM Director Console Tasks pane.

To run the method, drag the shortcut onto a CIM-enabled managed system that supports the method you want to run.

---

## Configure Alert Standard Format

You can use the Configure Alert Standard Format (ASF) task to set up monitoring of power states on managed systems and notification of impending system failure.

Complete the following steps to configure a managed system for ASF:

1. In the IBM Director Console Tasks pane, drag the **Configure ASF** task onto the managed system for which you want to configure ASF. The Alert Standard Format window opens.
2. On the General page, click the **Enable ASF Hardware** and **Enable All Platform Event Traps** check boxes.
3. Click the **Configuration** tab.
4. Type all the required settings.

**Note:** The Alert Standard Format Agent does not perform checks to determine if the IP address for the management server is reachable from the managed system. If the management server does not receive any ASF alerts, check to see if the correct IP address for the management server has been configured on the managed system.

5. Click **Apply**.

---

## DMI Browser

The Desktop Management Interface (DMI) Browser task provides in-depth information about DMI components. Used primarily for systems management, DMI does not support management of network devices, such as bridges, routers, and printers, as SNMP does.

To provide DMI data, managed systems must be running Windows 2000 or Windows XP. Also, the managed systems must have a DMI Service Provider (version 2.0 or later) installed. To obtain a DMI Service Provider, contact Smart Technology Enablers, Inc. (STEI) at [www.enablers.com](http://www.enablers.com).

You can use the DMI Browser to perform the following tasks:

- View the DMI components and groups for a selected DMI-enabled managed system
- View attribute values for selected group classes
- Set values for individual attributes
- Create a browser subtask, or shortcut, for specific group classes

Because IBM Director Console does not automatically display DMI-enabled managed systems as a separate group of managed systems, you might want to create a new dynamic group that contains only DMI-enabled managed systems.

## Starting the DMI Browser task

To start the DMI Browser and view information for a single managed system, in the IBM Director Console Tasks pane, drag the **DMI Browser** task onto the managed system for which you want to view information. The DMI Browser window opens.

To open the browser for two or more managed systems, select the managed systems for which you want to view information. Then, from the Tasks pane, drag the **DMI Browser** task to any system in the set of selected managed systems.

If one or more managed systems is not configured for DMI data, a message is displayed indicating that the target system or systems does not support the task. If the managed system is inaccessible, for example, if it is offline, the DMI Browser window opens but you cannot expand the DMI tree for the managed system.

## Viewing component information in the DMI Browser

Double-click a managed system to display the DMI components of the managed system, and then click a component to display descriptive information in the right pane.

To view the group classes of a component, double-click the component name. You can view the attributes of a group class by clicking the group class name. The right pane splits, a description of the group class is displayed in the Groups pane, and the associated attributes and methods are displayed in the lower-right pane.

## Setting an attribute value for a DMI group

Do not change an attribute value unless you are thoroughly familiar with the structure and manipulation of DMI data. Improperly setting a system value can cause unpredictable results on the target system.

Complete the following steps to change an attribute value:

1. In the DMI Browser window, navigate to the attribute for which you want to change the value.
2. Right-click the attribute row and click **Set value**. The Set Value window opens and the current value is displayed.
3. Type the new value and click **OK**. If IBM Director is unable to change the value on the target system, a message indicates the failure.

## Creating a group class shortcut

You can create a browser subtask, or shortcut, as a quick way to locate a specific DMI group class. After it is created, you can use the browser shortcut on a managed system to view information associated only with the specific group class.

Complete the following steps to create a group class shortcut:

1. In IBM Director Console, drag the **DMI Browser** task onto a managed system to open the DMI Browser window.
2. Double-click the managed system to display the associated components.
3. Double-click a component to display the contained group classes.
4. Right-click the group class name and click **Create task for group class**. A window opens, displaying the name of the group class as the default name.
5. Type a new name, or keep the default name. Click **OK**. The new task is displayed under **DMI Browser** in the IBM Director Console Tasks pane.

You can use the shortcut by dragging it onto a DMI-enabled managed system that has the same group class registered with the DMI service layer to view the associated data.

If you create a shortcut for a group class and apply it to a managed system with two or more DMI components containing the same group class, separately tabbed pages are displayed for each component containing the group class. For example, if you create a shortcut for the Component ID group class and apply the shortcut to a managed system with two or more DMI component IDs, separately tabbed pages are displayed for each component ID that is defined.

If you apply a user-defined shortcut for a group class to a managed system that does not have registered components containing the group class, the following error message is displayed: The targeted system does not support this class.

---

## Event action plans

See “Event action plans” on page 20.

---

## Event Log

You can use the Event Log task to 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.

Events (100) - Last 24 Hours							Event Details
Date	Time	Event Type	Event Text	System Na...	Severity	Category	
10/14/2002	1:34:48 PM	SNMP.iso...		IBM2022720	Unknown	Alert	
10/14/2002	1:31:16 PM	SNMP.iso...		IBM2022720	Unknown	Alert	
10/14/2002	1:31:16 PM	SNMP.iso...		IBM2022720	Unknown	Alert	
10/14/2002	1:12:13 PM	CIM.Directo...	200210141...	SLS5600	Harmless	Alert	
10/14/2002	1:10:47 PM	CIM.Directo...	200210141...	SLS5600	Harmless	Alert	
10/14/2002	1:09:22 PM	Director.To...	System 'SR...	SRI3	Harmless	Resolution	
10/14/2002	1:09:21 PM	CIM.Directo...	200210141...	SLS5600	Harmless	Alert	
10/14/2002	1:07:51 PM	CIM.Directo...	200210141...	SLS5600	Harmless	Alert	

Figure 36. 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.

## Viewing and changing display options

Not all events may be displayed, depending on the display options set. For instance, the default number of events displayed is 100, and the default time range is events that have occurred in the past 24 hours. To view the currently set time range or change the time range displayed, click **Options** → **Set Time Range**. To view the number of events displayed or change the number of events displayed, click **Options** → **Set Log View Count**.

## Exporting events from the event log

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

Complete the following steps to export an event from the event log:

1. In the Event Log window, click the event or events you want to export to a file.
2. Click **File** → **Export**, and click the file format to which you want to export the event or events. The applicably named window opens.
3. Type a file name in the **File Name** field.
4. Click **OK**.

---

## File Transfer

The File Transfer task is a secure alternative to FTP. You can use the File Transfer task to transfer files from one location to another location and to synchronize files, directories, or drives. You can transfer individual files and directories between:

- Management console and the management server
- Management console and a managed system
- Management server and a managed system

File transfer between two managed systems is not supported directly. However, you can transfer a file from one managed system to a management console or management server and then transfer that file to a different managed system.

## Starting the File Transfer task

In the IBM Director Console Tasks pane, drag the **File Transfer** task onto the managed system (the target system) to which you want to transfer files. IBM Director takes a few seconds to query the files on the source system and on the target system; then, the File Transfer window opens. Depending on the version of IBM Director Agent, the window is displayed differently.

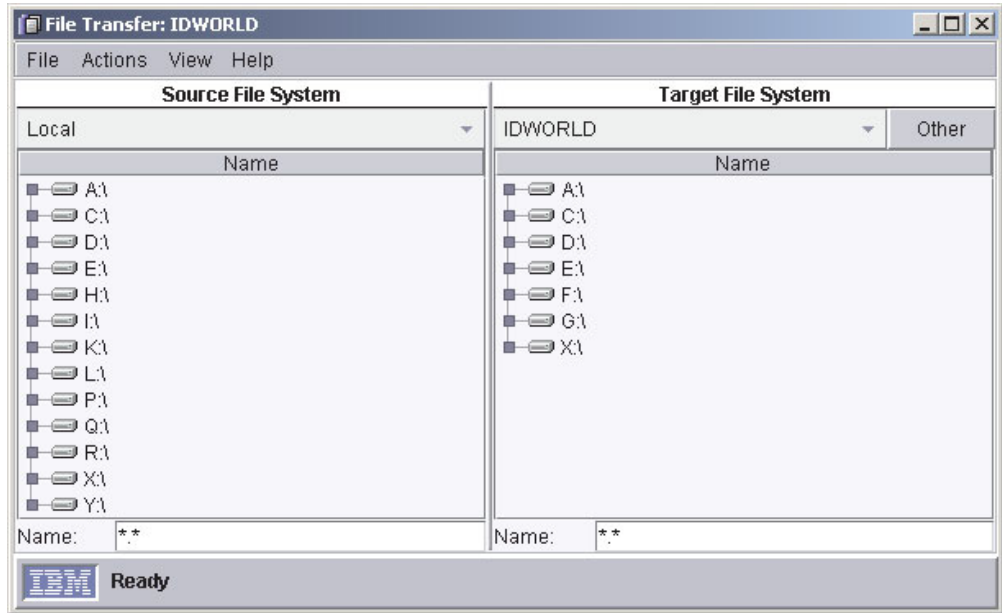


Figure 37. File Transfer window

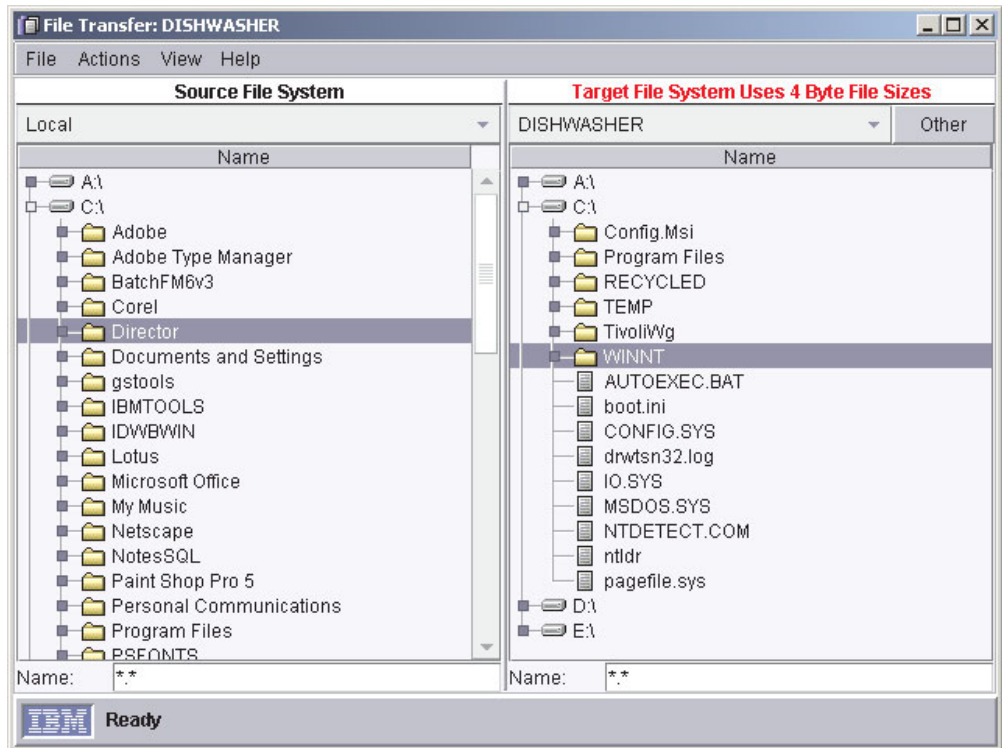


Figure 38. File Transfer window when target managed system has IBM Director Agent 3.1 installed

### Transferring files

Expand a drive in the Source File Systems pane or Target File Systems pane. The contents of that drive are displayed, showing subdirectories and files. To transfer

files or subdirectories, from the Source File System pane, drag the files or subdirectories you want to transfer onto the drive you want the files to reside on in the Target File System pane.

Using the wild-card function, you can transfer multiple files that have the same file extension but different file names or the same file names but different file extensions. When the File Transfer window opens, the **Name** field contains \*.\* by default.

### Changing the target system

You can change the target system from within the File Transfer window by selecting a different managed system from the list at the top of the Target File System pane.

Complete the following steps to change the target system from within the File Transfer window:

1. Beside the list, click **Other**. The Choose Target window opens, listing all available managed systems that support file transfer.
2. Select the managed system you want to transfer files to or from and click **OK**. The managed system is added to the target system list and is selected as the target system.

You can add up to six managed systems to the list at a time. If you add more than six, the managed system added earliest to the list is removed from the list.

## Transferring files between managed systems

You can transfer files indirectly from one managed system to another managed system by first transferring the files to the management server or console, then from the management server or console to the selected target managed system.

After you transfer the files from the source managed system to the management server or console, the file or subdirectory refreshes to contain the transferred file. Then you can transfer the file to the target managed system.

## Synchronizing files, directories, or drives

When you synchronize files, directories, or drives, you replace the contents of the target file, directory, or drive with the contents of the source file, directory, or drive. You can synchronize a source file, directory, or drive with as many target managed system files, directories, or drives as you choose, but you must synchronize the file, directory, or drive on each managed system individually. You cannot synchronize multiple target managed systems from a source managed system at the same time.

Complete the following steps to synchronize files, directories, or drives:

1. If you want the source to be identical to the target, in the Source File System pane, right-click the source; then, click **Synchronize from Target**. If you want the target to be identical to the source, in the Target File System pane, right-click the target; then, click **Synchronize from Source**.
2. You might receive a message indicating that the selected names are different. Click **Yes** to continue.

The selected files, directories, or drives are now synchronized.

## 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 39 for an example.

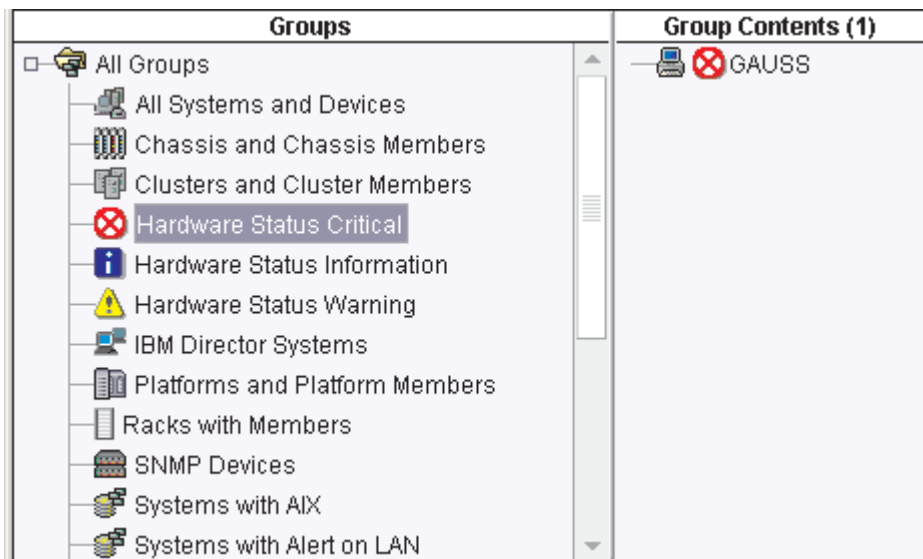


Figure 39. IBM Director Console displaying hardware status groups

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 40. 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.

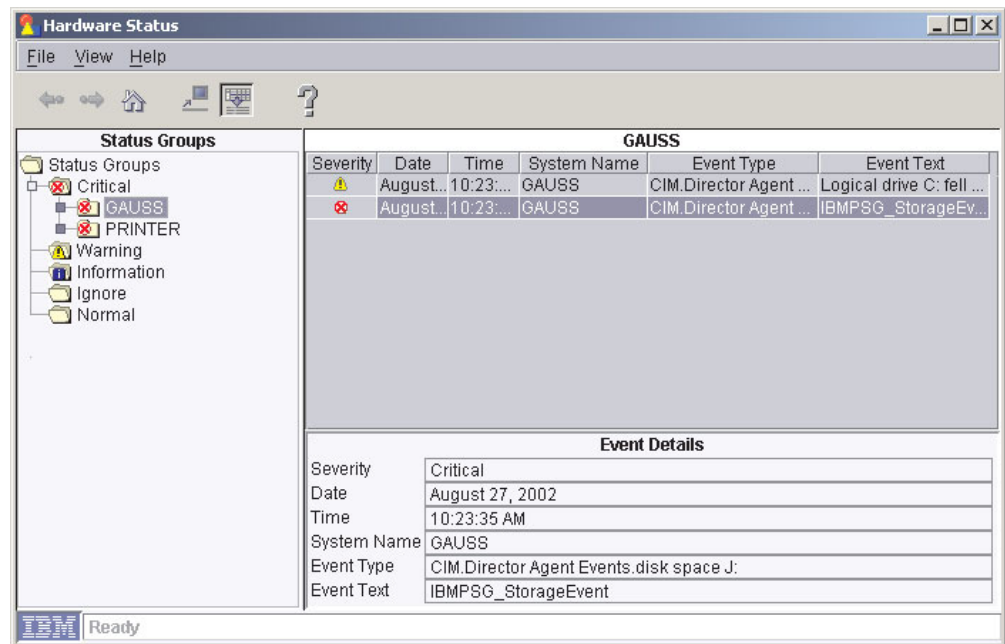


Figure 41. Hardware Status window showing all hardware status events

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 of IBM Director Console (for an example of a critical icon displayed next to a managed system, see Figure 39 on page 80). A Hardware Status window such as that in Figure 42 on page 82 opens.

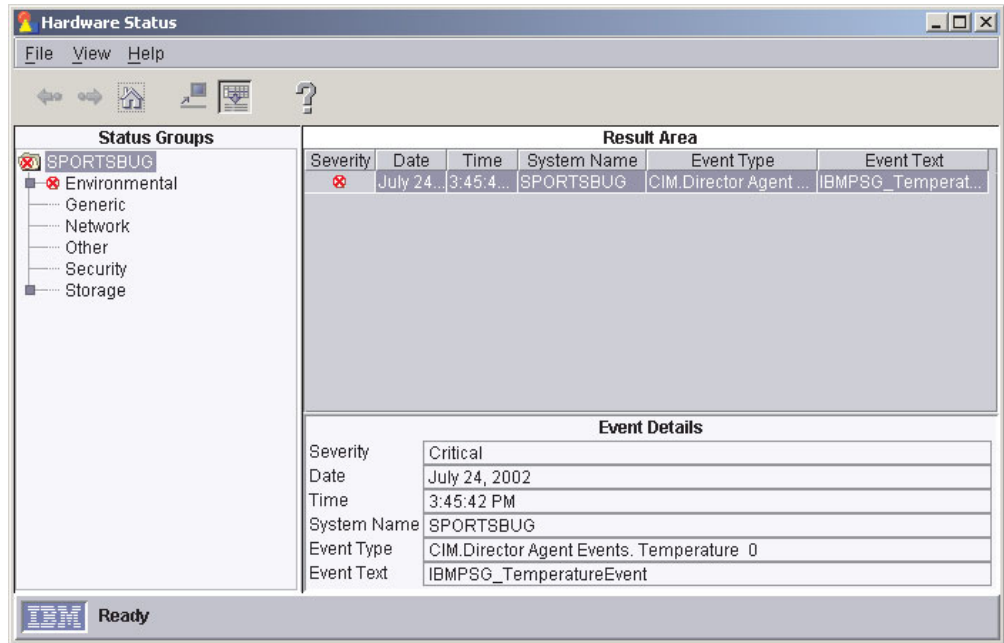


Figure 42. Hardware Status window showing events for a single managed system

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 the Inventory task 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 27 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. See “Viewing and editing the inventory software dictionary” on page 85 for more information.

## 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.

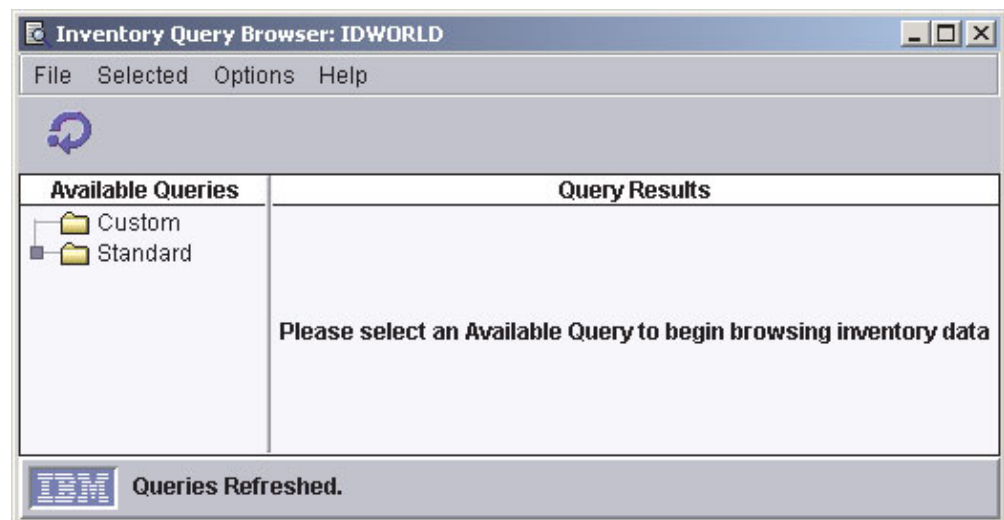


Figure 43. Inventory Query Browser window

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 27 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.

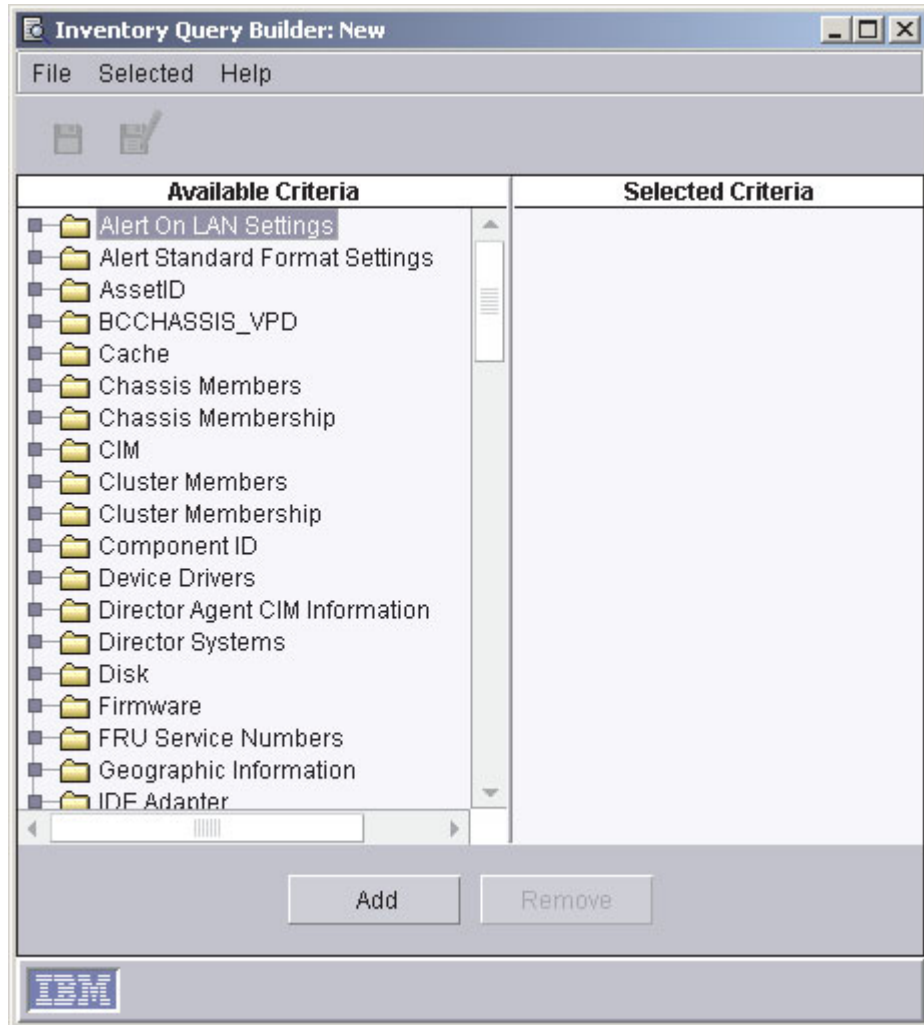


Figure 44. Inventory Query Builder window

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.

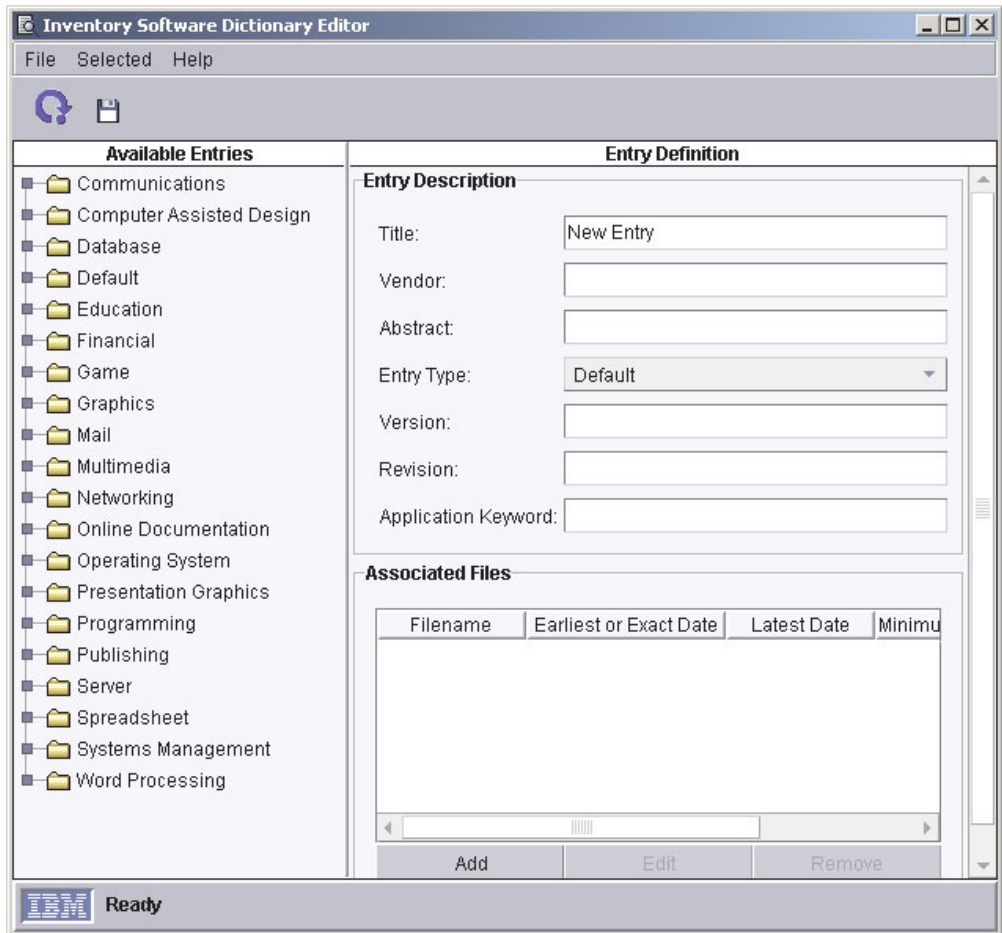


Figure 45. Inventory Software Dictionary Editor window

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 86 through step 6 on page 86.
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 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 45 on page 86.)
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. All entries must be present on the managed system or device for the managed system or device to be displayed.

---

## Management Processor Assistant

The Management Processor Assistant (MPA) task works with IBM servers that contain one or more of the following service processors or adapters:

- Advanced System Management processor (ASM processor)
- Advanced System Management PCI adapter (ASM PCI Adapter)
- Integrated system management processor (ISMP)
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

Using MPA, system administrators can configure, monitor, and manage the service processors in xSeries and Netfinity servers.

With MPA, you can view environmental data such as temperature, voltage, and fan speeds, view server and component data, and view the event log stored on the service processor. You can also configure system-management alerts such as operating-system alerts and timeouts, turn servers on and off and set delays, configure an alert-forwarding strategy, and configure network settings.

## Starting the Management Processor Assistant task

In the IBM Director Console Tasks pane, expand the **Management Processor Assistant** task. There are three subtasks:

- Communications Configuration
- Management Processor Configuration
- Server Management

Depending on which subtask you want to work with, drag the applicable subtask onto a managed system that supports Management Processor Assistant. The Management Processor Assistant window opens.



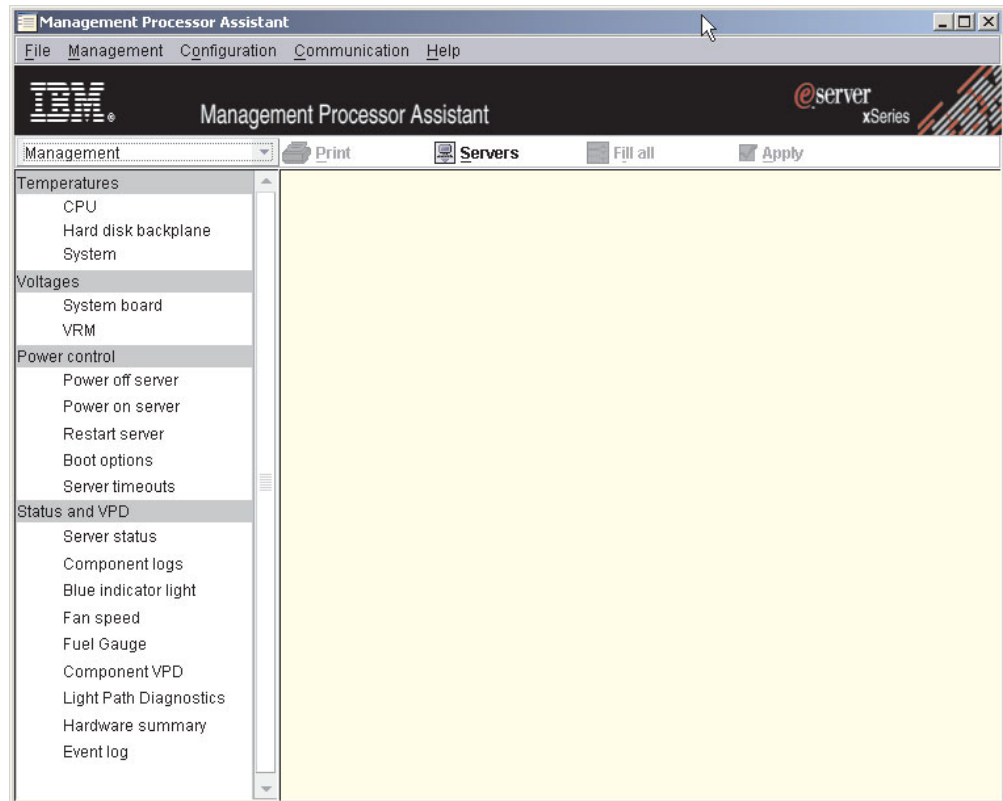


Figure 46. Management Processor Assistant window when activating the Server Management subtask

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

To select which servers you want to work with out of those targeted when starting the task, click **Servers** at the top of the right pane. The right pane is subdivided, the far-right subpane displaying, in a tree structure, all servers that you targeted when starting the task and any systems that contain a meaningful association with those servers that you targeted. For example, if you target an RXE-100 Remote Expansion Enclosure, the MPA task is activated against it and the physical platform that represents the xSeries server to which the enclosure is connected.

If MPA is unable to establish communications with the service processor for that system, a message is displayed that tells you to right-click the server in the far-right pane and click **Communication**. The Communication configuration pane opens, where you can enter parameters. If you do not do this, you will not be able to connect to that server, and the system will be displayed as grayed out in the far-right subpane.

Using the “Fill all” function, you can mass configure many servers at the same time by copying the values from the row for one system to other systems selected. When the source row provides parameters that are not applicable for a target system, the row for that system is skipped. To copy the values in one row to all selected entries in a table, select the other entries using the Ctrl key; then, click **Fill all**.

To save any changes, click **Apply**. Depending on the subtask, this function updates the information stored on IBM Director Server, modifies the configuration information on a service processor, or runs a management action.

You can also sort on the contents of a column by clicking the appropriate column heading.

## Communications Configuration subtask

You can use the Communications Configuration subtask to configure how IBM Director Server communicates with service processors. You can configure IP settings, RS-485 settings, and prioritize network communications.

You can update the parameters for multiple systems at the same time. For example, you use the Communications Configuration subtask on several systems. You can change the user ID and password and click **Fill all** to set the new user ID and password combination for all the systems you initially targeted.

Any changes you make using the Communications Configuration subtask are not applied until IBM Director Server communicates with the service processor. Thus, when you provide new values, they are not validated to ensure that IBM Director Server can connect to the service processor, even if you click **Apply**. If the values are not valid, IBM Director Server fails in its attempt to connect to the service processor.

### Example of how to establish out-of-band communication with a service processor

Complete the following steps to connect to IBM Director Server using out-of-band communication for an ASM processor with a Remote Supervisor Adapter:

1. Because IBM Director does not automatically discover ASM processors or on-board Remote Supervisor Adapters, you must create a management processor managed object or Remote Supervisor Adapter managed object in IBM Director Console. For information on how to do this, see the *IBM Director 4.1 Installation and Configuration Guide*, specifically the “Manually creating a management processor object” section in Chapter 9.
2. In the IBM Director Console Tasks pane, expand the **Management Processor Assistant** task. Drag the **Communications Configuration** subtask and drop it onto both an ASM processor managed object and a Remote Supervisor Adapter managed object. The Management Processor Assistant window opens. A message is displayed indicating a failure to connect.
3. Click **OK**. The Server tree is displayed in the right pane.
4. Disconnect from the Remote Supervisor Adapter by right-clicking the Remote Supervisor Adapter in the Server tree and clicking **Disconnect**.
5. Wait 60 seconds for disconnection to occur.
6. In the Server tree, right-click the ASM processor and click **Communications**. The “Communication configuration” window opens.
7. In the RS-485 settings group box, click **Gateway name** and click the Remote Supervisor Adapter in the list.
8. Select the **Enable** check box.
9. In the Global settings group box, verify that **RS-485** is selected as the first connection priority.
10. If you have assigned a different user ID and password (other than the default) to the Remote Supervisor Adapter, you must specify the user ID and password in the Global settings group box.

11. Select the **Store password** check box to enable the ASM processor to autoconnect using the Remote Supervisor Adapter upon next use.
12. Click **Apply** to connect. The Connection established using new connection parameters message is displayed.
13. Click **OK**. You can use the MPA task immediately.

The connection settings are used for both interactive and noninteractive MPA subtasks. If you provide parameters that are not valid, a noninteractive task might fail. If you cannot connect to the service processor, check the parameters you provided in the Communications Configuration subtask. For more information about service processors and communicating with IBM Director Server, see *IBM Director 4.1 Installation and Configuration Guide*, specifically the “Managing service processors” section in Chapter 3.

## Management Processor Configuration subtask

You can use the Management Processor Configuration subtask to view and configure service processor information, configure an alert-forwarding profile, restart a service processor, and much more.

### 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 **Configuration** → **VPD**. The data is displayed in the middle pane.

### 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 **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 profile, 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 **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 server to have your network settings take effect.

Complete the following steps to restart a service processor:

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

3. Click **Apply**.

### **Configuring modem settings**

You can configure both modem hardware and software settings.

Complete the following steps to configure modem hardware settings:

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

Complete the following steps to configure modem software settings:

1. Click **Configuration** → **Modem settings** → **Software**.
2. Make any configuration changes.
3. Click **Apply**.

### **Creating and changing dial-in login profiles**

You can use the dial-in login profiles that require a user ID and password to access the service processor. You can create up to 12 login profiles.

Complete the following steps to create or change dial-in login profiles:

1. Click **Configuration** → **Login profiles**.
2. To add a new user profile, click **Add an entry**.  
To change a user profile, click the user profile you want to change and make changes.  
To delete a user profile, click the user profile you want to delete, and manually delete the information displayed in the **User ID** field.
3. Click **Apply**.

## **Server Management subtask**

You can use the Server Management subtask to view server information, power on and off servers, restart a managed system, view and change start (boot) options, and much more.

### **Viewing environmental data**

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

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

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

To view fan speed, click **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, FRU number, part number, serial number, and manufacturer ID.

To view component data, click **Management** → **Status and VPD** → **Component 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 service processor. It includes information about the event, for example, the event severity. To view the event log stored on the service processor, click **Management** → **Status and VPD** → **Event log**.

**Note:** If you have started the MPA task on more than one server, clicking **Retrieve** lists all events for all servers listed. To see the events for a particular server only, select the applicable server in the Servers pane; then, click **Retrieve**.

## Viewing hardware summary

The hardware summary includes such information as the service processor, service processor type, model, and serial number, and UUID.

To view the hardware summary, click **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 **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 server. Complete the following steps to view the LEDs:

1. Click **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 server that has a problem. Complete the following steps to change the LED status on a server:

1. Click **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.

**Note:** If Unknown is displayed in the State column, the server does not support querying the current value.

3. Click **Apply**.

## Powering servers on and off

You can power a server on or off remotely. Note that to power off a server properly, you must install the service processor device driver and, depending on the operating system of the server, the Management Processor Assistant Agent. See your service processor guide for information about installing device drivers or agents.

Complete the following steps to power off a server:

1. Click **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 **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 a managed system**

Complete the following steps to restart a managed system:

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

### **Viewing and changing start (boot) options**

You can view and change whether a PXE restart (reboot) occurs when the server is next restarted.

Complete the following steps to view and change start options:

1. Click **Management** → **Power control** → **Boot options**.
2. In the **PXE reboot on next system restart** check box, select or deselect the check box for the applicable server.
3. Click **Apply**.

---

## **Microsoft Cluster Browser**

You can use the Microsoft Cluster Browser task to view the structure, nodes, and resources associated with a Microsoft Cluster Server (MSCS) cluster. You can determine the status of a cluster resource and view the associated properties of the cluster resources. The Microsoft Cluster Browser does not display the status of a cluster as a whole, but displays the individual cluster resource statuses.

### **Starting the Microsoft Cluster Browser task**

In the IBM Director Console Tasks pane, drag the **Microsoft Cluster Browser** task onto the cluster about which you want information. The Microsoft Cluster Browser window opens.

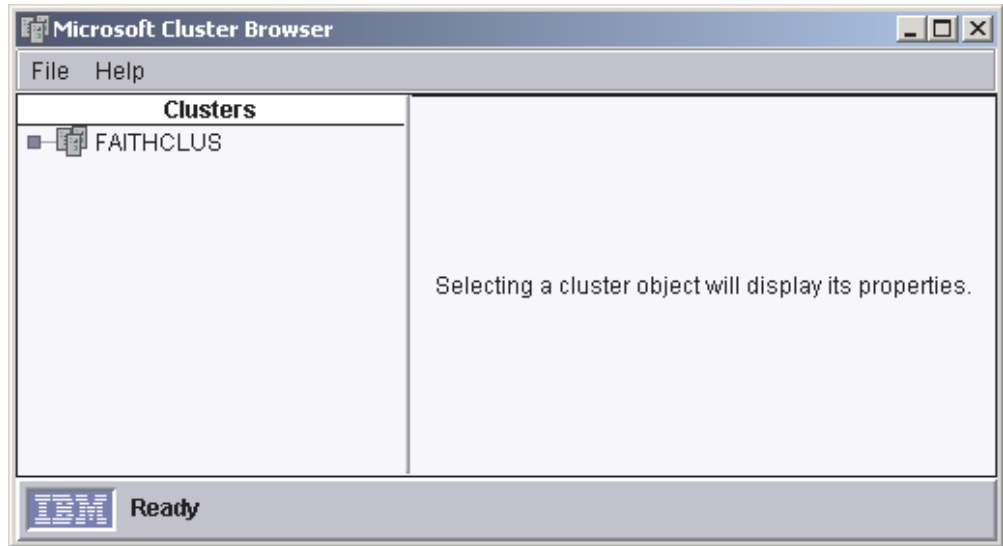


Figure 47. Microsoft Cluster Browser window

To view cluster status and description, in the Clusters pane, double-click the cluster.

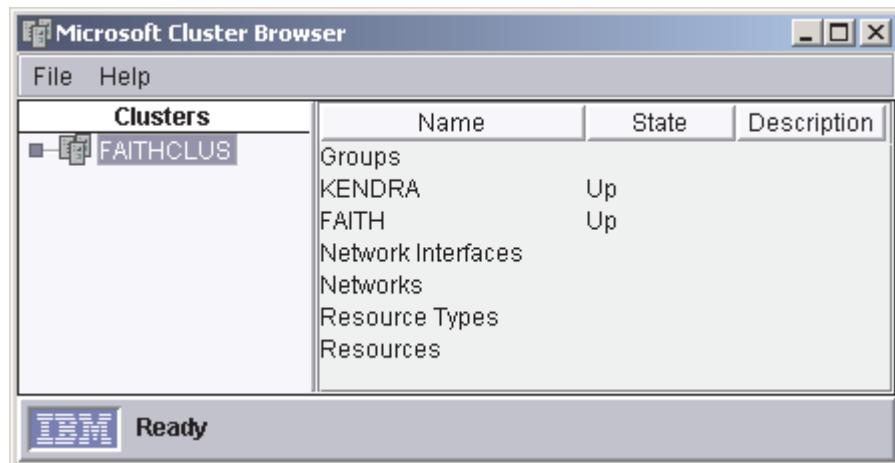


Figure 48. Microsoft Cluster Browser window showing the status of a cluster

To view information about the resources assigned to the cluster, in the Clusters pane, expand the properties tree and double-click the applicable resource.

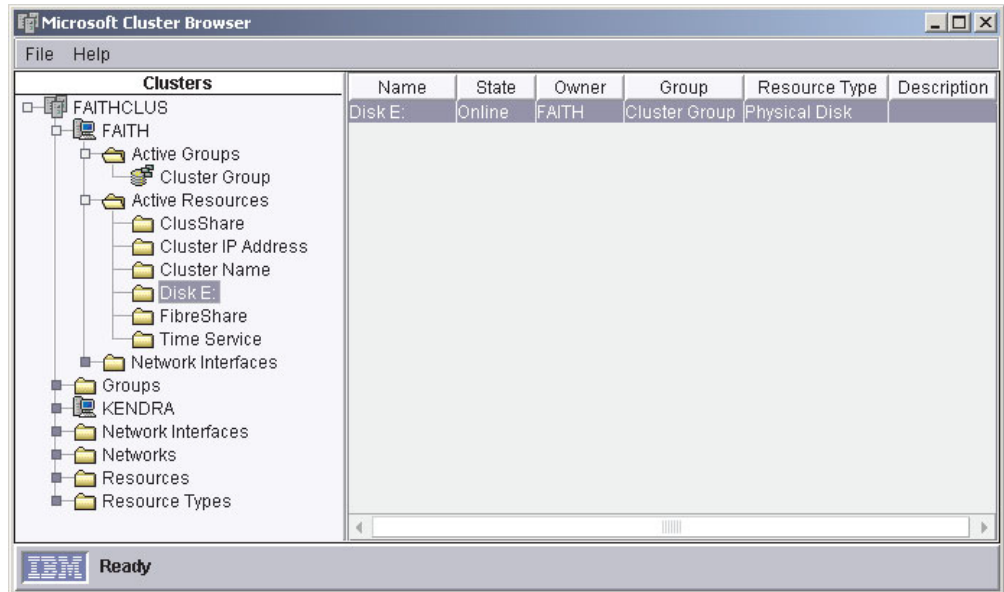


Figure 49. Microsoft Cluster Browser window showing cluster resource details

## Process Management

You can use the Process Management task 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

**Note:** For managed systems running Caldera Open UNIX, the only Process Management task or subtask that you can use is Process Tasks.

## 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. 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. (This is available for managed systems running Windows operating systems only.)



## Device Services

Shows all hardware device drivers installed on that managed system or group. (This is available for managed systems running Windows operating systems only.)

Name	Process ID	User	Thread Count	Priority	Monitored	Memory
Idle	0		1	Idle	No	16K
System	2		26	Normal	No	216K
smss	20		6	High	No	36K
csrss	24		7	High	No	284K
\\?\C:\WINNT\system32\winlogon.exe	34		2	High	No	68K
C:\WINNT\system32\services.exe	40		15	Normal	No	3052K
C:\WINNT\System32\snmp.exe	42	SYSTEM	6	Normal	No	1140K
C:\WINNT\system32\lsass.exe	43		11	Normal	No	836K
C:\WINNT\System32\nddeagnt.exe	46	Administrator	1	Normal	No	56K
C:\WINNT\system32\RpcSs.exe	61		6	Normal	No	800K
C:\WINNT\system32\spoolss.exe	66		6	Normal	No	132K
C:\TivoliWg\bin\tgipcv.exe	82	SYSTEM	2	Normal	No	52K
C:\TivoliWg\bin\tgipc.exe	86	SYSTEM	7	High	No	2844K
C:\TivoliWg\bin\tgwtopo.exe	95	SYSTEM	4	High	No	1072K
c:\winnt\system32\pstores.exe	97		4	Normal	No	124K
D:\SmsV2.21\elClient\Bin\SmsClientWatchd...	100	Administrator	1	Normal	No	80K
C:\TivoliWg\bin\tgwescli.exe	114	SYSTEM	6	High	No	1080K
C:\TivoliWg\bin\tgwmonit.exe	117	SYSTEM	3	High	No	1204K
D:\log\Bin\libpmap.exe	119	Administrator	1	Normal	No	220K
D:\SmsV2.21\elClient\Bin\SmsClient_.exe	126	Administrator	2	Normal	No	25112K
C:\WINNT\System32\CMD.exe	134	Administrator	1	Normal	No	60K
D:\log\Bin\libpmap.exe	139	Administrator	2	Normal	No	1012K
C:\TivoliWg\bin\tgwfran.exe	140	SYSTEM	2	High	No	1856K
C:\WINNT\Explorer.exe	143	Administrator	5	Normal	No	660K
C:\WINNT\System32\CMD.exe	146	Administrator	1	Normal	No	60K

Figure 50. 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. 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. The Process Management window opens.
2. Click the **Services** tab and right-click the service that you 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. The Process Management window opens.
2. Click the **Device Services** tab. Right-click the device that you 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.

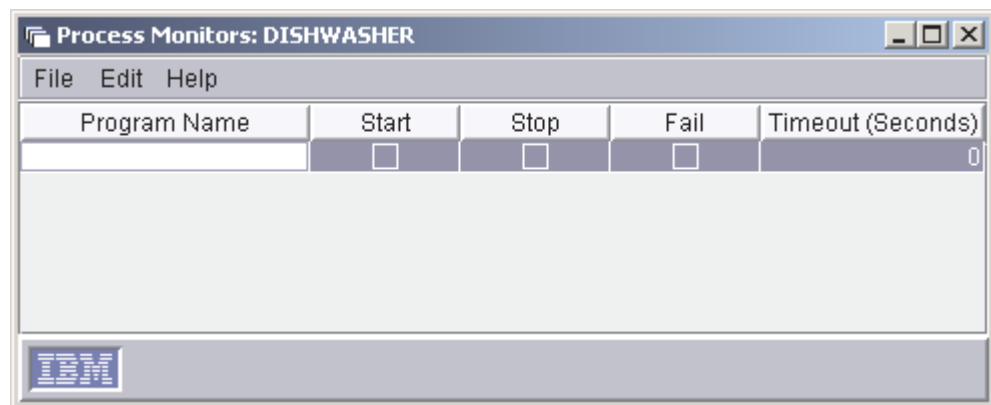


Figure 51. Process Monitors window

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 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 27 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.

### Removing process monitors individually

Complete the following steps to remove process monitors individually:

1. Drag the managed system 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.

### Removing all monitors from a system or group of systems

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

1. Drag the **Remove Process Monitors** subtask onto the managed system 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 27 for more information about how to schedule tasks.

## Viewing process monitors

To view a list of the process monitors running on a managed system, drag the **Process Monitors** task onto the managed system. 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 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 27 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 applicably. 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.

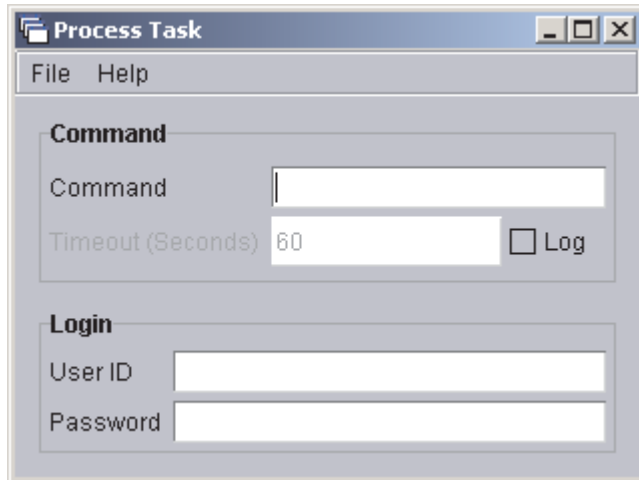


Figure 52. Process Task window

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 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 27 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 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. The Process Management window opens.
2. Click **Actions** → **Execute Command**.
3. The Execute Command window opens.



Figure 53. 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 function 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. At a command line, type  
`regedit`
2. Navigate to the registry entry  
`HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Director\CurrentVersion.`
3. Double-click **RestrictAnonCmdExec**.
4. In the **Value data** field, change **0** to **1**.
5. Click **OK**. The changes take effect immediately.

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

1. Change to the directory where 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.

---

## Rack Manager

You can use the Rack Manager task, part of the Server Plus Pack, to group your equipment in rack suites. Using Rack Manager, you can create virtual racks by associating equipment such as managed systems and devices, networking devices, power devices, and monitors with a rack to visually represent an existing rack in your environment. If the inventory collection function of IBM Director does not recognize a managed system or device in Rack Manager, you can associate it with a predefined component of a similar size.

One reason you might want to use Rack Manager is to view hardware-status alerts that occur on managed systems or devices in a rack. If a rack component has a hardware-status alert, the rack component is outlined in red, blue, or yellow, depending on the alert level.

### Starting the Rack Manager task

To start the Rack Manager task, in the IBM Director Console Tasks pane, drag the **Rack Manager** task onto a managed system or group. The Rack Manager window opens.

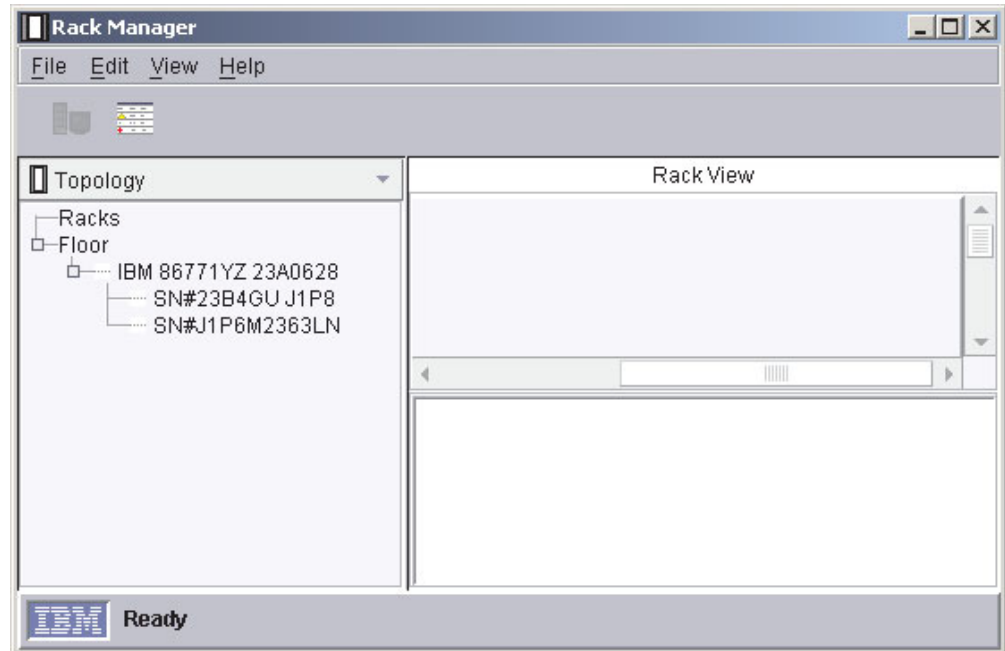


Figure 54. Rack Manager window

The left pane displays the Topology view by default. You can change the left pane view by clicking the list above the left pane. Four views are available:

#### Topology

Displays the Racks tree, which contains any racks that have been created, and the Floor tree, which contains all managed systems and devices that have not been added to a rack. A BladeCenter unit is displayed as a Chassis tree. Expanding a Chassis tree displays all blade servers in that chassis.

#### Components

Displays the predefined components available for association and for inclusion in a rack.

#### Cluster

Displays clusters and cluster members, if any clusters components exist. Otherwise, this option is disabled.

#### Multi-Node Systems

Displays complexes, partitions, virtual nodes, and I/O expansion units, if any exist. Otherwise, this option is disabled.

Information in all of these views is displayed in a tree structure.

The information in the right pane can be displayed in two ways:

#### Rack View

The right pane is subdivided into two subpanes. The information in the upper-right subpane displays rack information graphically. For example, if a rack component has a hardware-status alert, the rack component is outlined in red (for critical alert), yellow (for warning alert), or blue (for informational alert). The lower-right subpane displays the properties of the component selected in the upper pane or the left pane. If the inventory collection

function of IBM Director does not recognize the managed system or device selected in the left pane, Unknown is displayed for some of the properties displayed in the lower-right pane.

#### **Table View**

The right pane displays rack information, such as position in rack, hardware status, and state, in a table structure.

To view the rack information graphically, click **View** → **Rack view**. To view the rack information in table structure, click **View** → **Table view**.

## **Starting a component association**

Some managed systems and devices are not rack mountable until they are associated with a predefined component. This occurs when the inventory collection function of IBM Director does not recognize the managed system or device.

Complete the following steps to associate an unknown managed system or device with a predefined component:

1. In the Topology view, from the **Floor** tree, right-click the managed system or device and click **Associate**. The Associate window opens.
2. Expand the applicable tree and click the predefined component type, such as xSeries 440 Model 1AX, that most closely resembles the managed system or device in size.
3. Click **OK**. The properties of the component that was associated with that managed system or device are displayed in the lower-right subpane.

You can change the association of a component by first canceling the component association, then re-associating it with a different predefined component.

## **Canceling a component association**

You might want to cancel a component association in any of the following situations:

- You have made an incorrect component association.
- Inventory collection on the component has been performed successfully.
- The association is no longer valid.

To cancel the association of a managed system or device with a predefined component, in the Topology view left pane, right-click the component you want to disassociate and click **Disassociate system**. The component information in the lower-right subpane reverts to the information that was received initially through the inventory collection function of IBM Director.

## **Creating and configuring a rack**

You must first create a rack, then add components to the rack.

Complete the following steps to create a rack and add components to the rack:

1. In the Topology view, click **File** → **New Rack**. The Rack Properties window opens.
2. Type a name and location for the rack. Select the type of rack from the list.
3. Click **OK**. The new rack is displayed in the right pane. Be sure that the right pane is displaying the Rack view.
4. To add a component to the rack, in the left pane, expand the **Floor** tree.



5. From the **Floor** tree, drag a managed system or device onto a rack displayed in the right pane.

If the inventory collection function of IBM Director does not recognize the managed system or device, a message is displayed, asking if you want to associate the managed system or device with a predefined component. Click **OK**. The Associate window opens.

- a. Expand the applicable tree and click the predefined component type, such as xSeries 440 Model 1AX, that most closely resembles the target managed system or device in size.
- b. Click **OK**. The properties of the component that was associated with that managed system or device are displayed in the lower-right subpane.
- c. From the left pane, drag the managed system or device onto a rack.

The managed system or device is displayed in the right pane as a component of the rack.

6. (Optional) In the Components view, expand the applicable category of components.
7. Drag the predefined component onto a rack in the right pane. The component is displayed in the rack.

## Adding components to an existing rack

Complete the following steps to add components to an existing rack:

1. In the Rack Manager window, in the left pane of the Topology view, expand the **Floor** tree.
2. Drag a managed system or device onto a rack.

If the inventory collection function of IBM Director does not recognize the managed system or device, a message is displayed, asking if you want to associate the managed system or device with a predefined component. Click **OK**. The Associate window opens.

- a. Expand the applicable tree and click the predefined component type, such as xSeries 440 Model 1AX, that most closely resembles the managed system or device in size.
  - b. Click **OK**. The properties of the component that was associated with that managed system or device are displayed in the lower-right pane.
  - c. From the left pane, drag the managed system or device onto a rack. The managed system or device is displayed in the right pane as a component in the rack.
3. (Optional) In the left pane, select the **Components** view from the list.
  4. Expand the applicable category of components.
  5. Drag the predefined component onto a rack in the right pane. The component is displayed in the rack.

## Removing a rack component

To remove a rack component, in the right pane of the Topology view, right-click the rack component you want to delete and click **Delete**. This action deletes the managed system or device from the rack, and displays the managed system or device in the left pane in the Floor tree.

---

## Remote Control

You can use the Remote Control task to manage a remote system by displaying the screen image of the managed system on a management console. You can use Remote Control on managed systems running Windows 2000 or Windows XP only. You cannot use Remote Control on SNMP devices.

Remote Control has three control states:

**Active** Remote-control mode. A management console controls the managed system, and the user of the managed system loses all use of the keyboard and mouse. Only one management console can be in control of a specific managed system in the active state; all other attached management consoles can only monitor the managed-system display.

**Monitor**

View-only mode. Management consoles attached to the managed system only display the screen image of the managed system.

**Suspend**

View-only mode without image refresh. Management consoles attached to the managed system only display the screen image of the managed system. The screen image that is displayed on the management consoles does not change when the screen image changes on the managed system.

## Starting a remote-control session

To start a remote-control session, in the IBM Director Console Tasks pane, drag the **Remote Control** task onto a managed system. The Remote Control window opens.

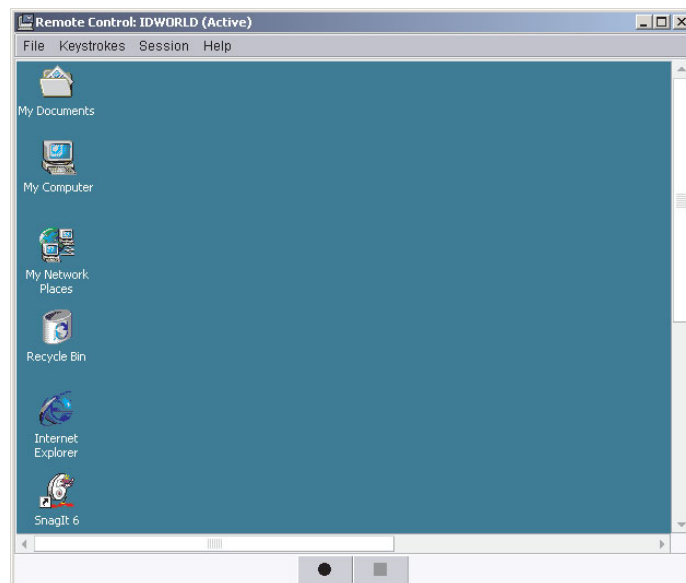


Figure 55. Remote Control window

The user of the managed system can regain control at any time by pressing Alt+T on the managed system.

## Changing remote-control states

To change the remote-control state, in the Remote Control window, click **Session**; then, click the state to which you want to change. The state is displayed at the top of the Remote Control window.

## Changing the refresh rate

You can change the rate at which the screen image refreshes in the Active and Monitor remote-control states. The following refresh rates are available:

### **Fastest**

Screen refresh with no delay

**Fast** Screen refresh every 2 seconds

### **Medium**

Screen refresh every 10 seconds

**Slow** Screen refresh every 30 seconds

To change the refresh rate, in the Remote Control window, click **Session** → **Refresh rate**; then, click the refresh rate you want.

## Recording a remote-control session

You can record a remote-control session as a file and replay it later on IBM Director Console. Complete the following steps to record a remote-control session:

1. In the Remote Control window, click **File** → **Start Session Logging**. The Save Session As window opens.
2. Type a name for the session log file. Click **OK**. Recording begins immediately.
3. When you want to stop recording, click **File** → **Stop Session Logging**. The session log file is saved in the IBM Director Console Task pane under the Remote Control task.

## Playing a recorded remote-control session

To play a recorded remote-control session, double-click the recorded remote-control session that was saved in the IBM Director Console Task pane under the Remote Control task. The remote-control session player opens. Use the controls at the bottom of the window to play, stop, and pause.

## Restricting remote-control usage

You can restrict remote-control usage by using one of two methods:

- Remote-access authorization
- User administration

### **Remote-access authorization**

Using this method, the user of the remote system can accept or reject a remote-control session when another user attempts to start the Remote Control task. If the user does not respond to the request within 15 seconds, the attempt is rejected. This option can be configured during installation of IBM Director Agent by enabling the **Require user authorization for screen access** option in the Network Driver Configuration window. This setting must be enabled on each managed system for which you want to require local authorization. See the *IBM Director 4.1 Installation and Configuration Guide* for more information.

## User administration

Using this method, you can specify the tasks a user can access, and prevent user access of the Remote Control task.

Complete the following steps to prevent a user from accessing the Remote Control task:

1. In IBM Director Console, click **Options** → **User Administration**. The User Administration window opens.
2. Click the user whose access you want to limit.
3. Click **User** → **Edit**. The User Editor window opens.
4. Click the **Task Access** tab. Select the **Limit user access only to the tasks listed** check box.
5. Click each of the tasks to which you want the user to have access and click **Add**. Make sure you do not add the **Remote Control** task to the Tasks User Can Access pane.
6. Click **OK**.

## Sending key combinations

When using the Remote Control task, nearly all key combinations are automatically passed through to the remote managed system. However, operating-system requirements restrict the use of certain key combinations, for example, Ctrl+Alt+Del. The following key combinations cannot be used during a remote-control session because they interfere with the operating system the management console is running on:

- Alt+Esc
- Alt+Tab
- Ctrl+Esc
- Ctrl+Alt+Del

However, in the Remote Control window, you can click **Keystrokes** and then click the applicable option to enter those key combinations for the remote managed system.

---

## Remote Session

Similar to Remote Control, you can use the Remote Session task to run command-line programs on a remote managed system. Remote Session uses less network traffic and system resources than the Remote Control task, and therefore is useful in low-bandwidth situations.

To start the Remote Session task, in the IBM Director Console Tasks pane, drag the **Remote Session** task onto a managed system. A command prompt-like window opens. When targeting a managed system running Linux, Remote Session uses the Telnet protocol. Therefore, a Telnet server must be installed on the managed system.

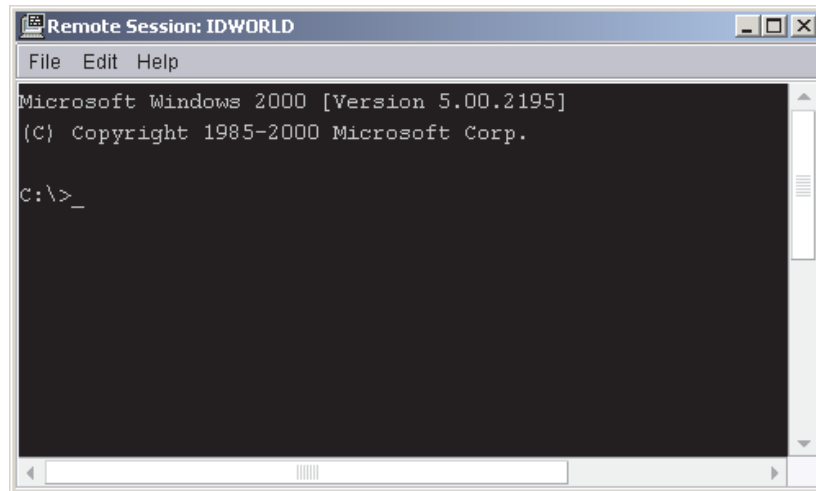


Figure 56. Remote Session window for a managed system running Windows

---

## Resource Monitors

You can use the Resource Monitors task 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 20 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 211.)

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.

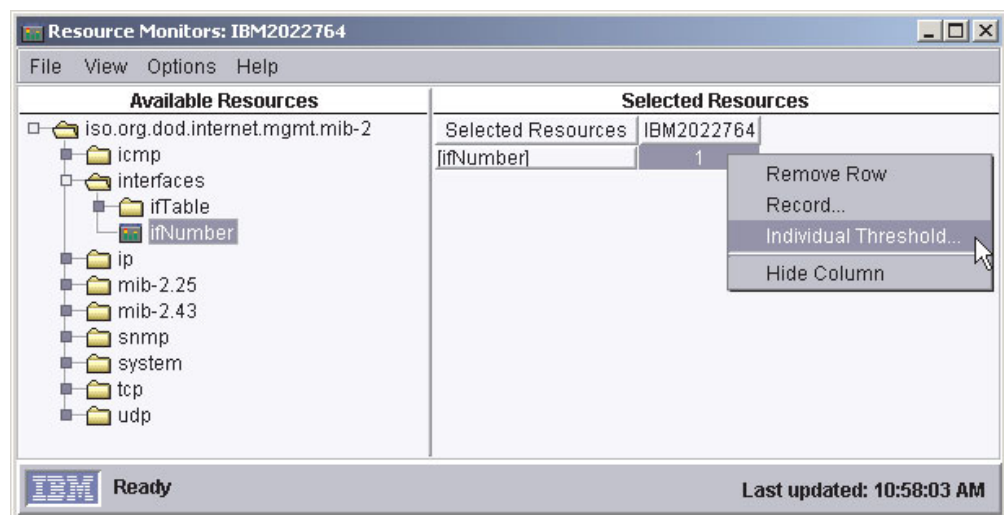


Figure 57. Resource Monitors window for a managed device

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 58 on page 111) or a text string (Figure 59 on page 112), you see the applicable window.

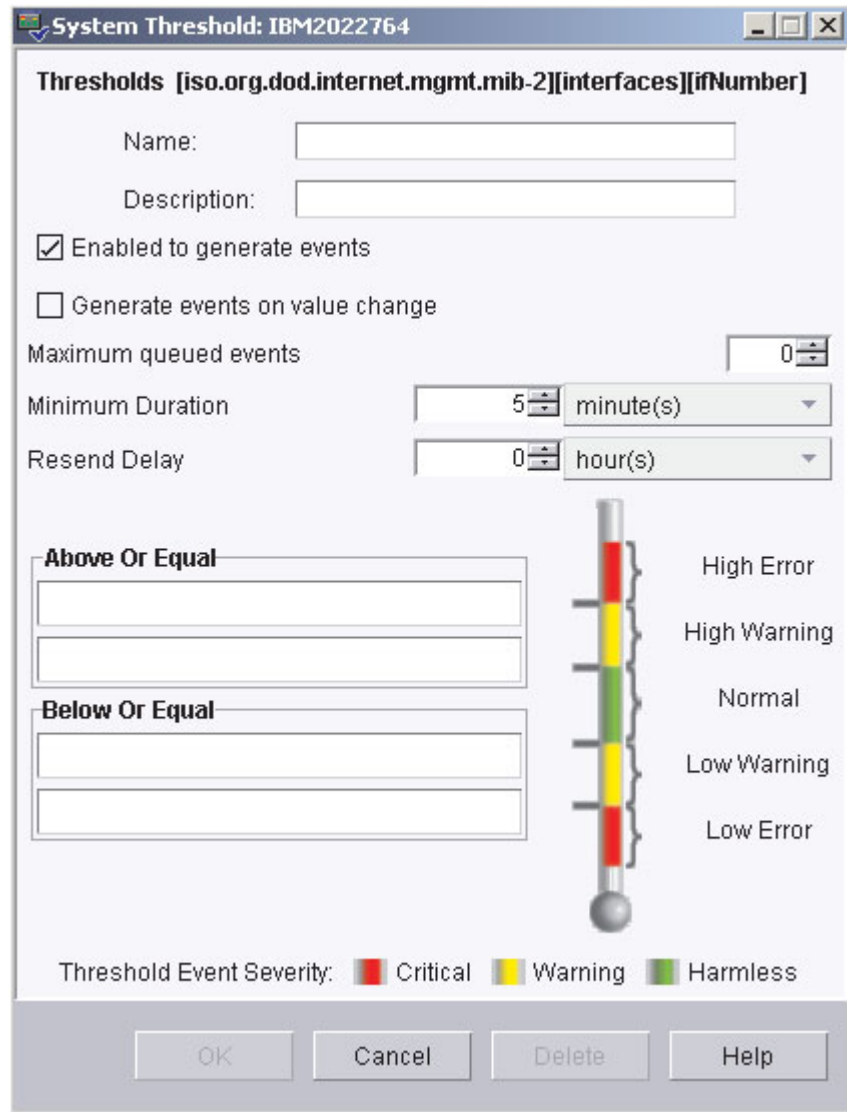


Figure 58. System Threshold window for setting numeric thresholds

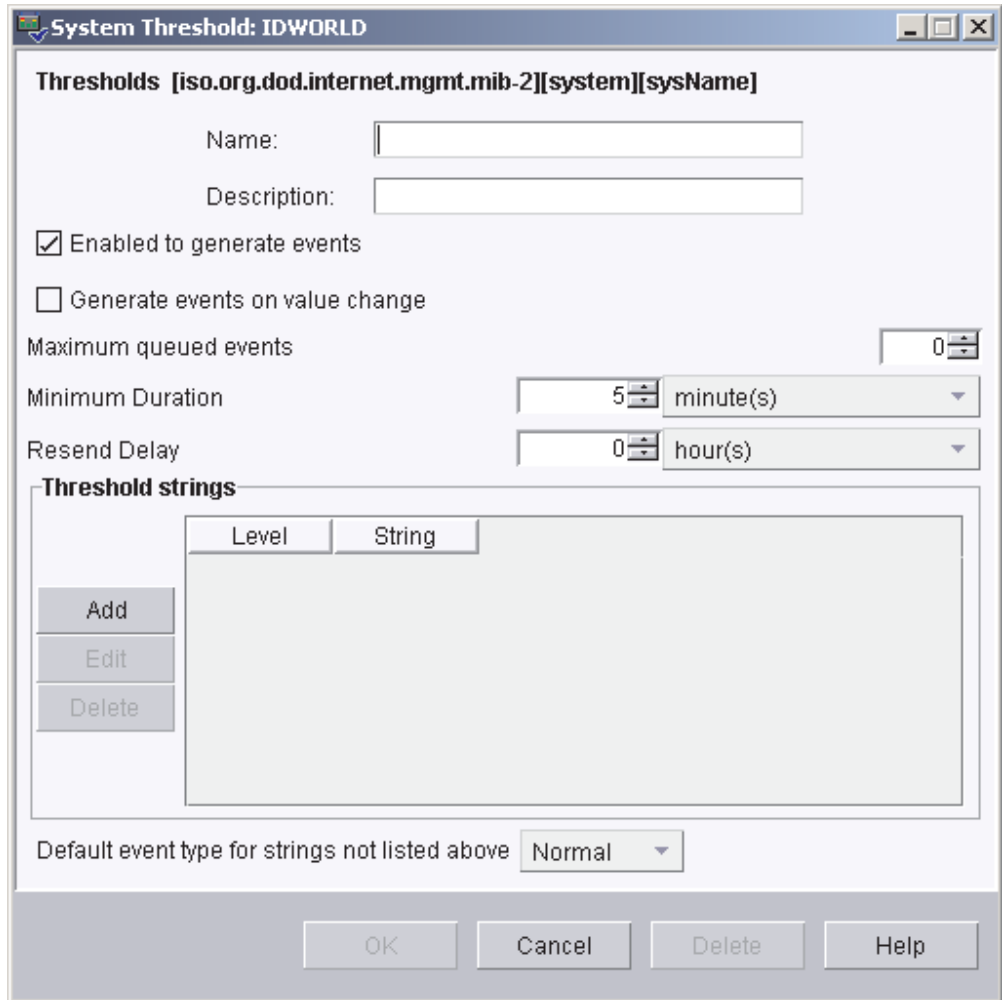


Figure 59. System Threshold window for setting text threshold strings

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 notified 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 20 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 applicable attribute in the Selected Resources pane. 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 beside the applicable attribute in the Selected Resources column 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 4. 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**.

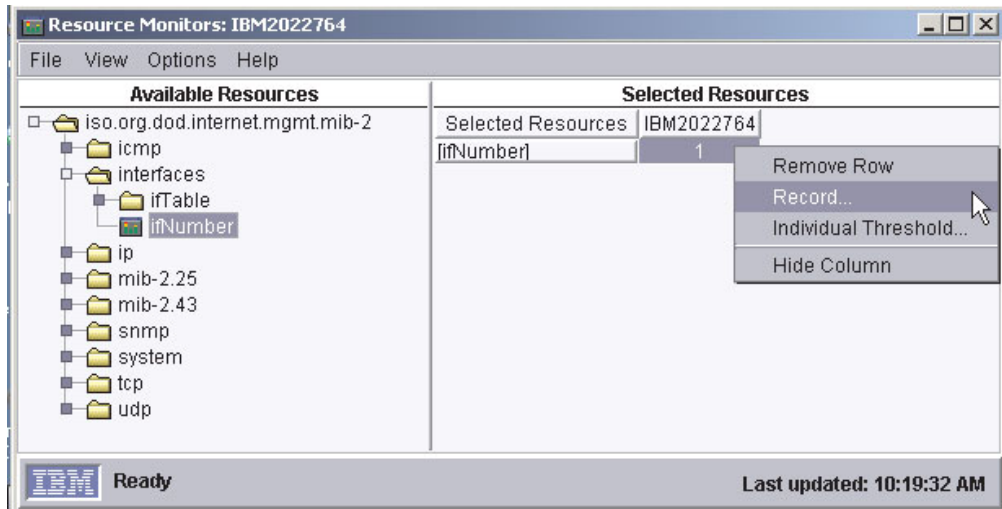


Figure 60. Resource Monitors window

The Resource Monitor Recording window opens.



Figure 61. The Resource Monitor Recording window

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

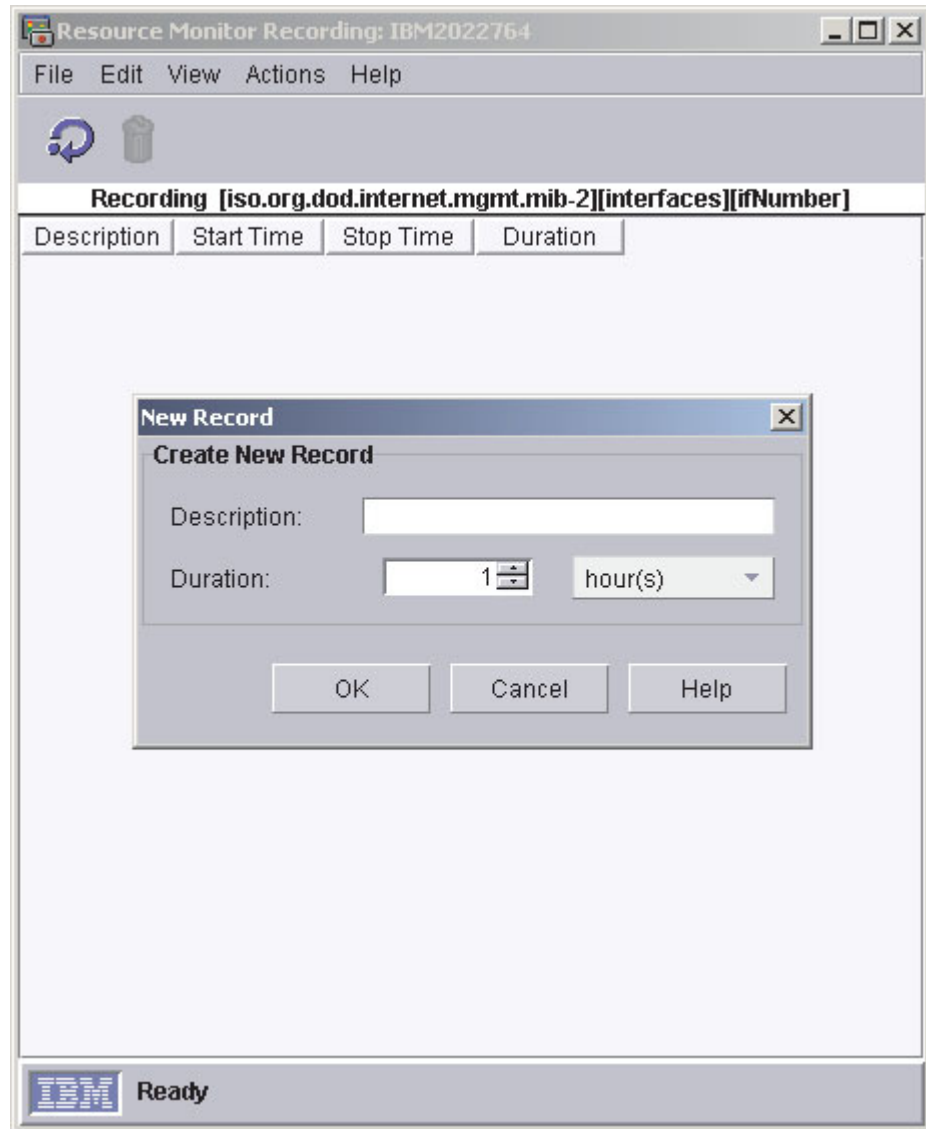


Figure 62. New Record window

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 text, CSV, 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, select the file type, 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.

## Exporting and importing threshold tasks

You can export a threshold task for use on another management console. Complete the following steps to export a threshold task:

1. In the IBM Director Console Tasks pane, expand the Resource Monitors task, and right-click the threshold task and click **Export to File**. The Export to File window opens.
2. Type a file name in the **File Name** field.
3. Click **Save**.

Complete the following steps to import a threshold task:

1. In the IBM Director Console Tasks pane, right-click the Resource Monitors task and click **Import Plan from File**. The Import Threshold Plan from File window opens.
2. Type a file name in the **File Name** field or navigate to the file and click the file name.
3. Click **Import**.

## 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 function.

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

See “Scheduler” on page 27.

---

## ServeRAID Manager

You can use the ServeRAID Manager task to monitor ServeRAID adapters or an integrated SCSI controller with RAID capabilities that are installed locally or remotely on servers. In IBM Director, you can use ServeRAID Manager to view information related to arrays, logical drives, hot-spare drives, and physical drives, and view configuration settings. You can also view alerts (which in the ServeRAID Manager task are called notifications) and locate defunct disk drives.

### Starting the ServeRAID Manager task

To start ServeRAID Manager, in the IBM Director Console Tasks pane, drag the **ServeRAID Manager** task onto a managed system that supports ServeRAID. The ServeRAID Manager window opens.

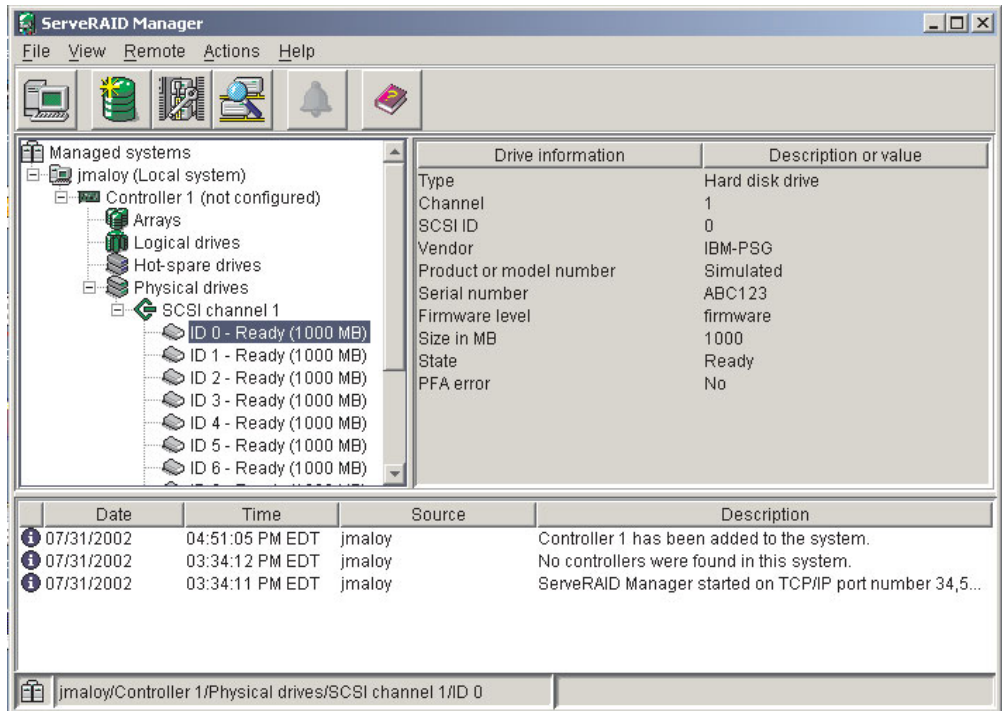


Figure 63. ServeRAID Manager window

The left pane is the tree pane, and right pane is the main pane. The bottom pane is the event viewer.

You can use ServeRAID Manager to view information about RAID controllers and the RAID subsystem (such as arrays, logical drives, hot-spare drives, and physical drives).

## Viewing system or device information

To view system or device information, expand the ServeRAID Manager tree; then, click the relevant tree object. Detailed information about the selected system or device is displayed in the right pane.

## Viewing ServeRAID alerts

You can view ServeRAID alerts in the event viewer. Three icons in the event viewer provide information about Error, Warning, and Information alerts.

## Locating defunct disk drives

You can locate defunct disk drives, which are called physical drives in ServeRAID Manager. In the tree pane, click the physical drives tree object to expand the tree. A red icon identifies any defunct disk drives. Also, in the main pane, the **State** field indicates if a disk drive is defunct.

---

## 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 ipNetToMediaNetAddress table, 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 default to the value of sysName. If this value is blank, then the host name of the device is used. If the host name 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, you can view the SNMP traps using the event log on the SNMP managed device that originated the trap. 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** tab 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.

## Using the SNMP Browser

You can use the SNMP Browser task 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 should 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 MIB files normally needed for SNMP browsing for commonly defined devices. They are located in the Director\proddata\snmp directory.

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

Use 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.

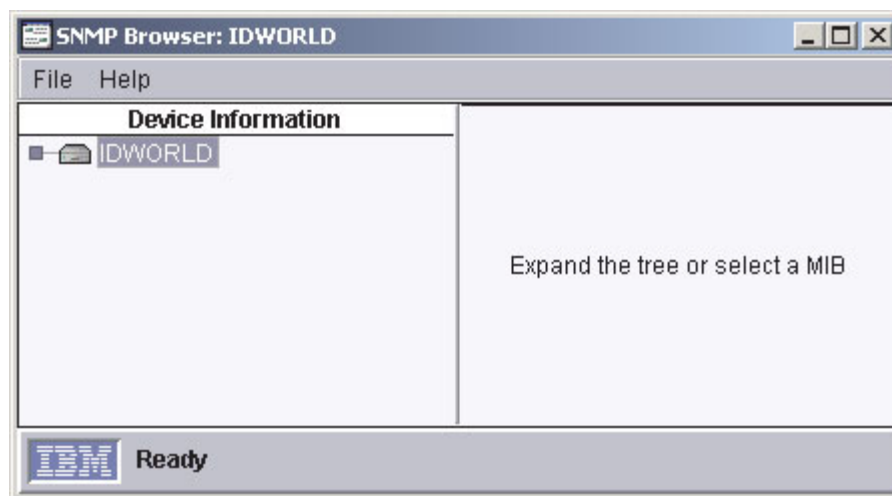


Figure 64. SNMP Browser window

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



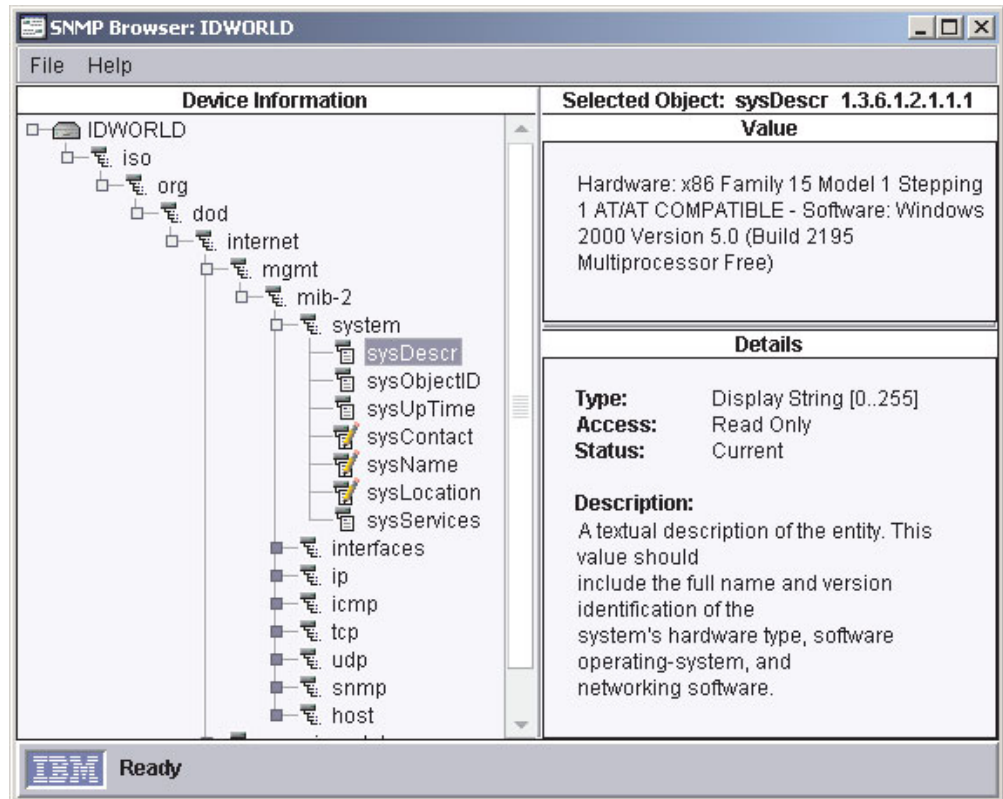



Figure 65. SNMP Browser window with a device tree expanded

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 applications and data, build a software package, and distribute the package to IBM Director managed systems. There are two editions of software distribution: standard and premium. To use the Premium Edition, you must have purchased and installed IBM Director Software Distribution Premium Edition on the management server.

With IBM Director Software Distribution Standard Edition, you can import only software distributed by IBM and build a software package using only the Director Update Assistant wizard. With the Premium Edition, you can:

- Import software not distributed by IBM and build a software package using one of the following wizards:
  - InstallShield Package wizard (for Windows)
  - Microsoft Windows Installer Package wizard (for Windows)
  - RPM Package wizard (for Linux)
- Import software distributed by IBM and build a software package using Director Update Assistant wizard
- Import non-IBM or IBM software and build a software package using the Custom Package Editor, which is a custom alternative to using a wizard
- Export a software package for use on another management server
- Import a software package created in IBM Director using the Director File Package wizard

## Understanding software distribution

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

1. Obtain the software. The most common method of obtaining IBM software is through UpdateXpress.
2. Import the software into IBM Director Server and build a software package.
3. Distribute the software package to managed systems using one of these methods:
  - Streaming from the management server to selected managed systems
  - Redirected distribution
  - (InstallShield and Microsoft Windows Installer only) Redirected installation from the file-distribution server

You must understand the methods IBM Director uses to distribute software. A streamed distribution streams the package from the management server to the managed system. The one advantage to this method is that 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. Otherwise, the entire package must be resent.

A redirected distribution streams the software package to one or more shared directories (shares) that you specify in the Server Preferences window, on the File Distribution Servers page. One reason you might want to use redirected distribution is to prevent network congestion. Another reason is that with redirection, the managed system only receives the minimum installation code needed to access the share and install the software from the management server. One limitation is that if the installation is interrupted, for example, if the connection is lost, the installation must be started again.

With redirected distribution, a file-distribution server functions as a storage location for a software package. The share caches a software package. After a package has been cached on a share, the cached package is used for future distributions, which can reduce the amount of time required to distribute a package. A software package is only cached on a share when the package is distributed.

During a redirected distribution, IBM Director Server first determines if the package is already cached on one of the shares. If the package is not cached, IBM Director Server searches its list of shares to determine which share has enough free space to save the package. If a share is not found that has enough free disk space to cache the package, the least recently used package might be deleted if doing so would create enough free space for the new package. If a package is edited and saved, the cache entry is deleted from any share where the package was stored.

The list of shares that can potentially be used in a redirected distribution is determined by IBM Director Server and the file-distribution server preferences set for the managed systems involved, and the ability of the management server and the managed systems to access the share.

To use this method, IBM Director must be set up to use a file-distribution server. You can use either an FTP-based share or a UNC-based share. See the *IBM Director 4.1 Installation and Configuration Guide* for more information about setting up a share.

For software that uses Microsoft Windows Installer or InstallShield as the installation utility, when using the redirected distribution method, the software package is installed directly from the file-distribution server automatically. However, you can specify that the package stream from the file-distribution server by selecting the applicable check box in the Set Managed System Distribution Preferences window.

## Importing software and building software packages

You can use a wizard or the Custom Package Editor to import files and build a software package.

### Using Director Update Assistant

The Director Update Assistant is a wizard that imports software distributed by IBM into IBM Director and creates the software package or packages. If you obtained the software using UpdateXpress, you must use this wizard.

Complete the following steps to import the software and create a software package or packages:

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

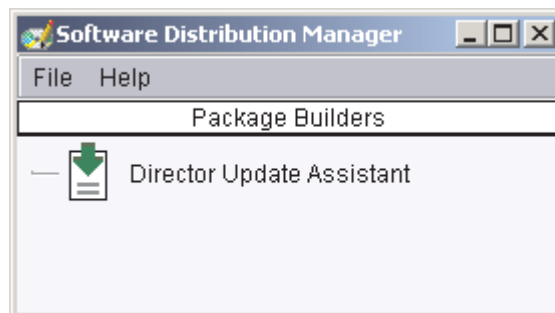


Figure 66. Software Distribution Manager window (Standard Edition)

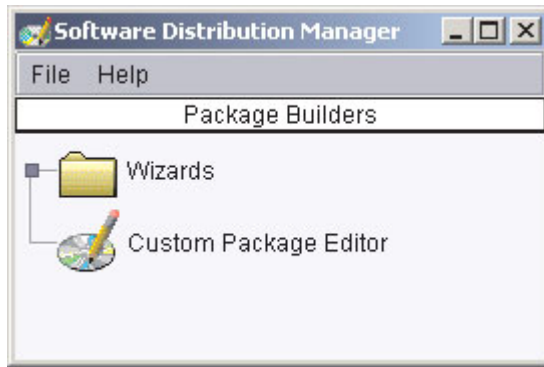


Figure 67. Software Distribution Manager window (Premium Edition)

2. (Standard) Double-click **Director Update Assistant**.  
 (Premium) Expand the **Wizards** tree. Double-click **Director Update Assistant**.  
 The Director Update Assistant wizard starts.

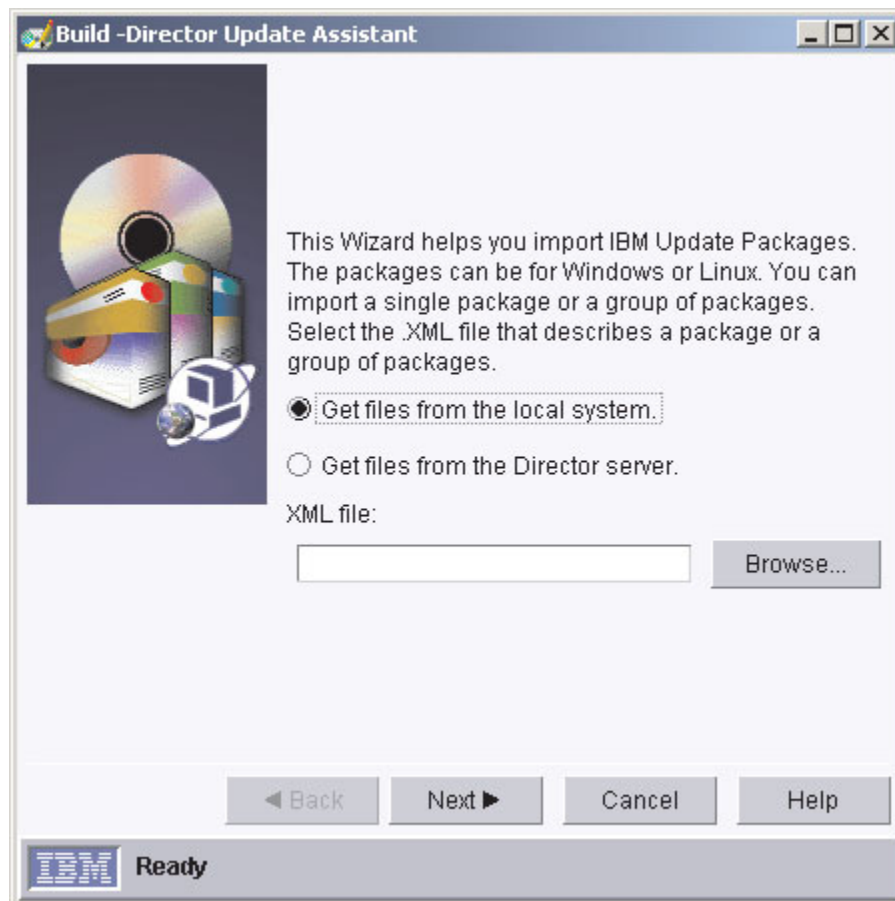


Figure 68. Director Update Assistant wizard

3. Specify whether the files reside on the local management console or on the management server by clicking the applicable button.
4. Then, type the location of the XML file that describes the software package or packages you want to import, or click **Browse** to locate the XML file.

5. Click **Next**. If one software package is specified in the XML file, the package is displayed in the Packages pane. If more than one software package is specified, a tree structure is displayed in the Packages pane. For example, for *UpdateXpress*, a folder is displayed for each managed-system type specified in the XML file. Expanding each folder displays a list of the software packages that apply to the specific managed system. If you click a package in the Packages pane, a description of the software package is displayed in the Details pane.  
By default, no software packages are selected for import into IBM Director, which is indicated by the red X displayed beside each package in the Packages pane.
6. Double-click the package or packages in the Packages pane to select the package for import. Or, if you want to select all the packages, or just those that are deemed critical by IBM, you can right-click the folder and click **Select All Items** or **Select Critical Items**, respectively. The red X displayed beside the package in the Packages pane changes to a green checkmark to indicate that the package will be imported.  
  
(Managed systems running Windows only) In the Options pane, you can specify an alternate response file to run by typing the path name in the **Alternate response file** field.  
  
(Managed systems running Linux only) In the Options pane, you can specify an alternate installation script to run by typing the path name in the **Alternate install script** field.
7. Click **Finish**.

If you import only one software package, the package name is displayed in the IBM Director Console Tasks pane under the **All Software Distribution Packages** category. If you import more than one software package, a software-distribution category is created for each managed-system type. Individual software packages are displayed under each category. The packages are also displayed in the IBM Director Console Tasks pane under **All Software Distribution Packages**.

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 133.

### **Using the InstallShield Package wizard (Premium Edition only)**

Use this wizard to import the software and build a software package for an application that uses InstallShield as its installation utility. You can create packages for software that uses InstallShield Professional 5, 6, or 7 for Windows. IBM Director uses InstallShield Silent, which provides a silent, or unattended, installation. InstallShield Silent requires a response file, which is created either by recording an installation or manually with an editor. Note that you can distribute a software package created with this wizard to managed systems running Windows only.

Most applications do not indicate anywhere in the documentation that they use InstallShield. To determine if an application uses InstallShield, start the installation EXE file (usually *setup.exe*). When the first window opens (which is the standard InstallShield Setup window), minimize that window; then, right-click the taskbar, and click **About**. The following window opens:



Figure 69. About InstallShield window

If you see the words “InstallShield” in this window, you should use the InstallShield Package wizard in the Software Distribution task to build a software package.

Next, you must determine if a response file is included with the software you want to distribute. If a response file is included, you must test the response file to ensure it can be used to install the software. If no response file is included, you must create a response file and test it. The response file must be included as part of the software package. The managed system uses it during installation to permit and perform an unattended installation.

To determine if a response file is included with the software for which you want to build a package, search for an ISS file (typically `setup.iss`). If no response file is included, record one using the installation command for the software, typically `setup.exe` or `install.exe`. For example:

```
setup -r -f1x:\response_filename.iss
```

where:

- `setup` is the installation command
- `x:\response_filename` is the filepath where you want to save the response file. If you do not specify the `-f1` parameter, InstallShield saves the response file in `c:\windows\setup.iss`.

When the installation command executes, you are prompted for required information. The responses you provide must reflect how you want the application to be installed on the managed system. For more information about response files, go to [www.InstallShield.com](http://www.InstallShield.com).

When you build the response file, you also install the software locally. Before you can test the response file, you must uninstall the software. After you uninstall the software, test the recording of the response file or the response file that is included with the software. Type the following command:

```
setup -s -f1x:\response_filename.iss
```

where:

- `setup` is the installation command for the product
- `x:\response_filename` is the filepath of the response file you recorded or the response file included with the software. If you do not specify the `-f1` parameter, InstallShield assumes the response file is located at `c:\windows\setup.iss`.

When the command completes, check the system log file. If the software installed successfully, the result code is 0. If the software does not install properly, you cannot distribute it using IBM Director.

**Note:** Many software products are not designed for unattended installation, although InstallShield provides the capability. Contact the product vendor if the software does not support unattended installation.

Complete the following steps to import the software and create a software package or packages:

1. In the IBM Director Console Tasks pane, double-click the **Software Distribution** task. The Software Distribution Manager window opens.
2. Expand the **Wizards** tree. Double-click **InstallShield Package**. The InstallShield Package wizard starts.

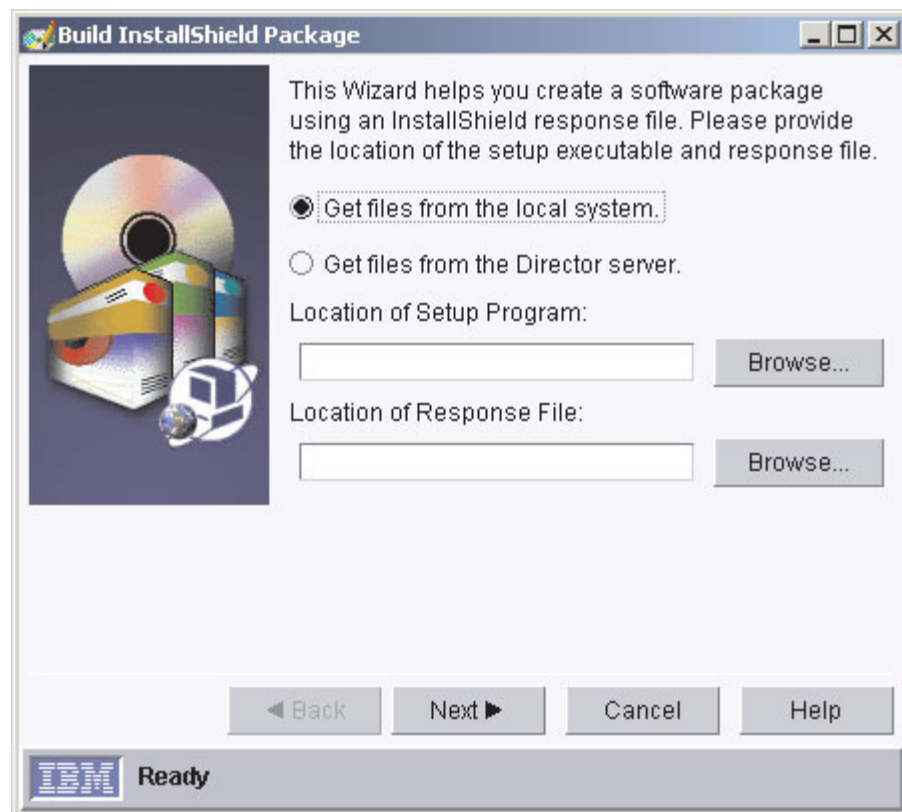


Figure 70. InstallShield Package wizard

3. Specify whether the files reside on the local management console or on the management server by clicking the applicable button. Then, type the location of the setup program and the response file in the applicable fields, or click **Browse** to locate the setup program or response file. Click **Next**.
4. In the **Package Name** field, the package name is filled in automatically. If you want to use a different name, type the package name.
5. (Optional) In the **Package Category** field, type a new package category name, or if you have created another package category previously, you can select it from the list.

6. (Optional) You can also specify additional command-line parameters that are specific to the application you are importing by typing the applicable command-line parameters.
7. (Optional) To install the software using a different user name and password, click **Advanced**. Type the applicable information and click **OK**.
8. Click **Finish**.

If you import only one software package, the package name is displayed in the IBM Director Console Tasks pane under the **All Software Distribution Packages** category. If you import more than one software package, a software-distribution category is created for each managed-system type. Individual software packages are displayed under the **All Software Distribution Packages** category.

You can distribute the software package or software-package category that contains this package now, or schedule a later time for distribution. See “Distributing a software package” on page 133.

### **Using the Microsoft Windows Installer Package wizard (Premium Edition only)**

Use this wizard to import the software and build a software package for an application that uses Microsoft Windows Installer as its installation utility. Using this wizard, you can change some installation parameters and use a Microsoft software transformation (MST) file. You can use this wizard to build software packages for distribution to managed systems running Windows only.

Complete the following steps to import the software and create a software package or packages:

1. In the IBM Director Console Tasks pane, double-click the **Software Distribution** task. The Software Distribution Manager window opens.
2. Expand the **Wizards** tree. Double-click **Microsoft Windows Installer Package**. The Microsoft Windows Installer Package wizard starts.



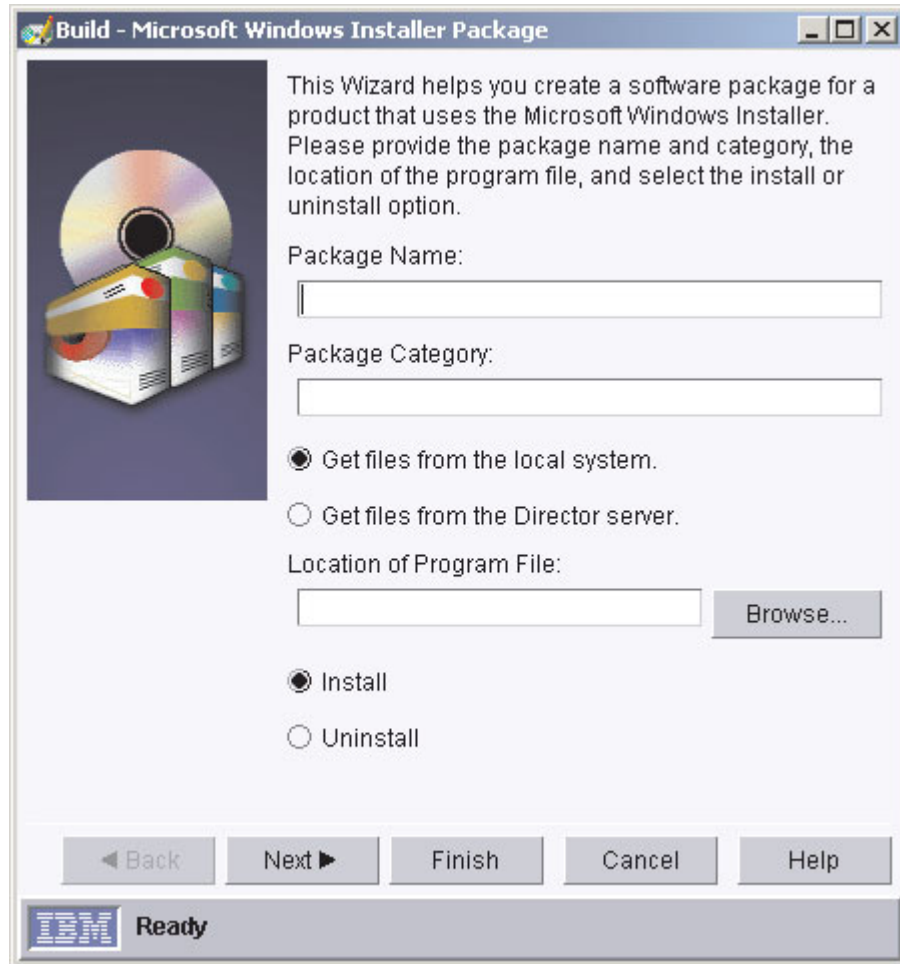


Figure 71. Microsoft Windows Installer Package wizard

3. In the **Package Name** field, type the package name.
4. (Optional) In the **Package Category** field, type a new package category name, or if you have created another package category previously, you can select it from the list.
5. Specify whether the files reside on the local management console or on the management server by clicking the applicable button. Then, type the location of the program file or, click **Browse** to locate it. Select whether to install or uninstall the software package by clicking the applicable button. Click **Next**.
6. (Optional) You can specify a transform file, such as a .mst file, by typing the location of the transform file in the applicable field, or clicking **Browse** to locate it. Also, you can specify additional Windows Installer parameters by typing the parameters in the applicable field.  
To install the software using a different user name and password, click **Advanced**. The Advanced Options window opens. Type the user ID and password in the applicable fields and click **OK**.
7. Click **Next**. A summary is displayed.
8. Click **Finish**.

If you import only one software package, the package name is displayed in the IBM Director Console Tasks pane under the **All Software Distribution Packages** category. If you import more than one software package, a software-distribution

category is created for each managed-system type. Individual software packages are also displayed under the **All Software Distribution Packages** category.

You can distribute the software package or software-package category that contains this package now, or schedule a later time for distribution. See “Distributing a software package” on page 133.

### Using the RPM Package wizard (Premium Edition only)

Use the RPM Package wizard to import the software and build a software package for an application that uses Red Hat Package Manager (RPM) for its installation utility. RPM is the common installer for all IBM Director-supported Linux operating systems. An RPM is an archive of files specific to an application. Using this wizard, you can create and distribute a single software package that contains one or more RPMs. You can use this wizard to build software packages for distribution to managed systems running Linux only.

Complete the following steps to import the software and create a software package:

1. In the IBM Director Console Tasks pane, double-click the **Software Distribution** task. The Software Distribution Manager window opens.
2. Expand the **Wizards** tree. Double-click **RPM Package**. The RPM Package wizard starts.

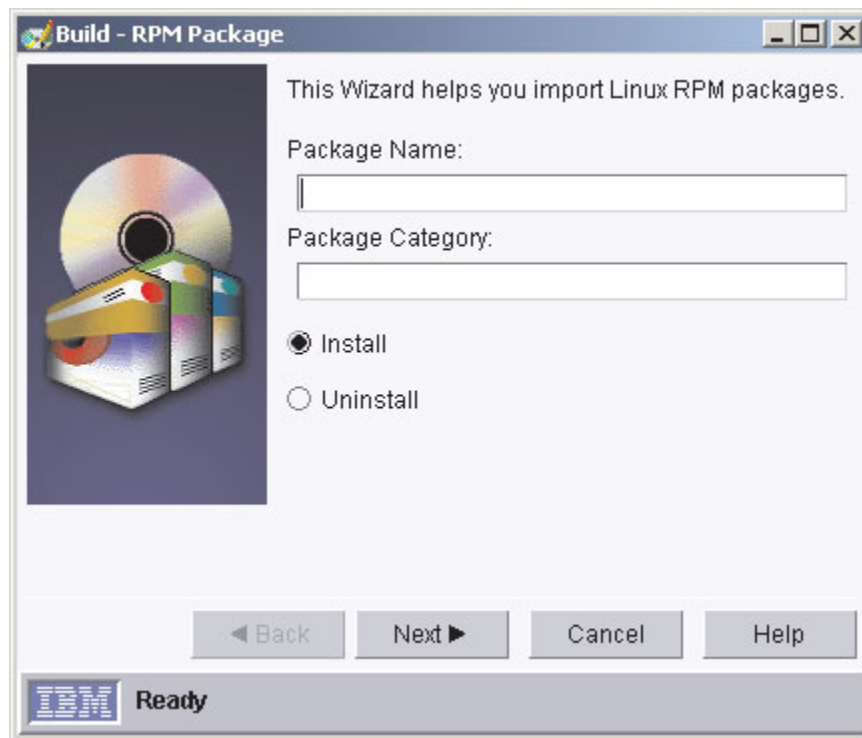


Figure 72. RPM Package wizard

3. In the **Package Name** field, type the package name.
4. (Optional) In the **Package Category** field, type a new package category name, or if you have created another package category previously, you can select it from the list.
5. Select whether to install or uninstall the software package.
6. Click **Next**.

7. Specify whether the files reside on the local management console or on the management server by clicking the applicable button. Then, select the RPMs you want to import by clicking **Add**. A separate window opens where you can choose the files you want to import. You can choose more than one file to import at a time.
8. Click **Finish**.

If you import only one software package, the package name is displayed in the IBM Director Console Tasks pane under the **All Software Distribution Packages** category. If you import more than one software package, a software-distribution category is created for each managed-system type. Individual software packages are also displayed under the **All Software Distribution Packages** category.

You can distribute the software package or software-package category that contains this package now, or schedule a later time for distribution. See “Distributing a software package” on page 133.

### **Using the Custom Package Editor (Premium Edition only)**

Use the Custom Package Editor to import the software and build a software package without using a wizard. That is, you specify the exact files, target directory names and paths, and installation programs or batch files that perform the software installation.

Complete the following steps to import and build a software package:

1. In the IBM Director Console Tasks pane, double-click the **Software Distribution** task. The Software Distribution Manager window opens.
2. Double-click **Custom Package Editor**. The Create Custom Package window opens.



Figure 73. Create Custom Package window

There are four tabs:

- General
  - Files
  - Linux
  - Windows 2000/XP
3. On the General page, specify the package name and package category (if any) and any distribution options and prerequisites.
  4. On the Files page, specify the files to use by navigating to the file in the Source File System pane and clicking **Add**. You can change whether the files are displayed from the local management console or the management server by selecting from the list at the top of the pane.
  5. Depending on the operating system, you can select to distribute a software package to a managed system running Linux, or Windows, or both by selecting the applicable check box on the applicable page.
  6. Click **File** → **Save**. The package name is displayed in the IBM Director Console Tasks pane under the **All Software Distribution Packages** category.

You can distribute the software package or software-package category that contains this package now, or schedule a later time for distribution. See “Distributing a software package” on page 133.

## Importing a previously created software package using Director File Package wizard (Premium Edition only)

The Director File Package wizard imports software package block (SPB) format files into IBM Director. These files are created by exporting an IBM Director software package. If you want to import a software package created in IBM Director, you must use this wizard.

**Note:** Previously created signed package (BFP) format software packages are not functional with this release of IBM Director.

Complete the following steps to import a software package:

1. In the IBM Director Console Tasks pane, double-click the **Software Distribution** task. The Software Distribution Manager window opens.
2. Expand the Wizards tree. Double-click **Director File Package**. The Director File Package wizard starts.

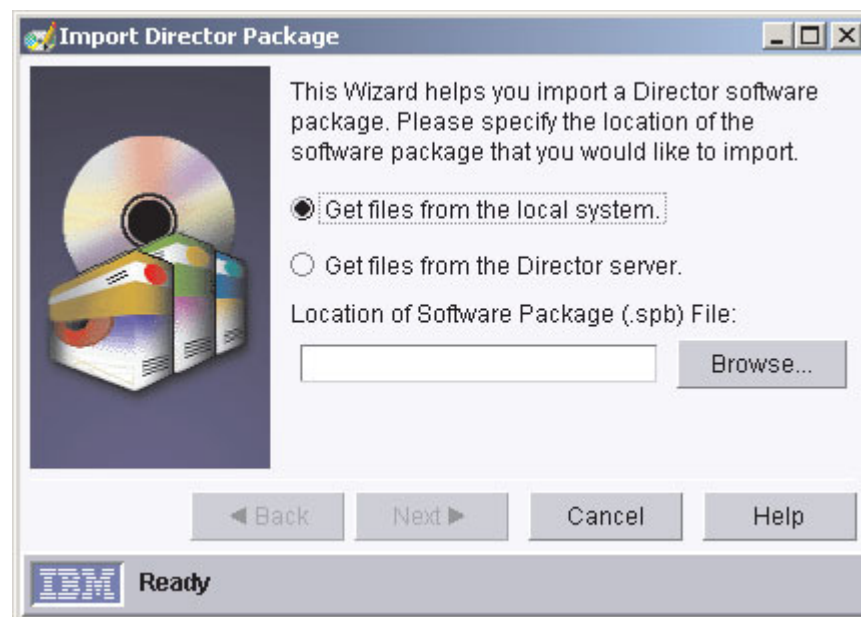


Figure 74. Director File Package wizard

3. Specify whether the files reside on the local management console or on the management server by clicking the applicable button. Then, type the location of the SPB 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 the **All Software Distribution Packages** category. You can distribute the software package or the software-package category that contains this package now, or schedule a later time for distribution. See “Distributing a software package”.

## Distributing a software package

You can distribute a software package or software-package category immediately, or schedule a later time for distribution.

Complete the following steps to distribute a software package or software-package category:

1. In the IBM Director Console Tasks pane, drag the software package or software-package category onto the managed system or group to which you want to distribute the package.
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 27.)

**Notes:**

1. 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.
2. If you distribute a software-package category to a group of managed systems, each software package within that category is delivered individually to each managed system in the group. The package listed first in the category is the first to be distributed. After the first package has been distributed, each succeeding package is delivered to each managed system until all software packages have been distributed.

## Creating and editing software-package categories

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

Complete the following steps to create a new software-package category:

1. In the IBM Director Console Tasks pane, right-click the **Software Distribution** task and click **New Package Category**. The New Package Category window opens.

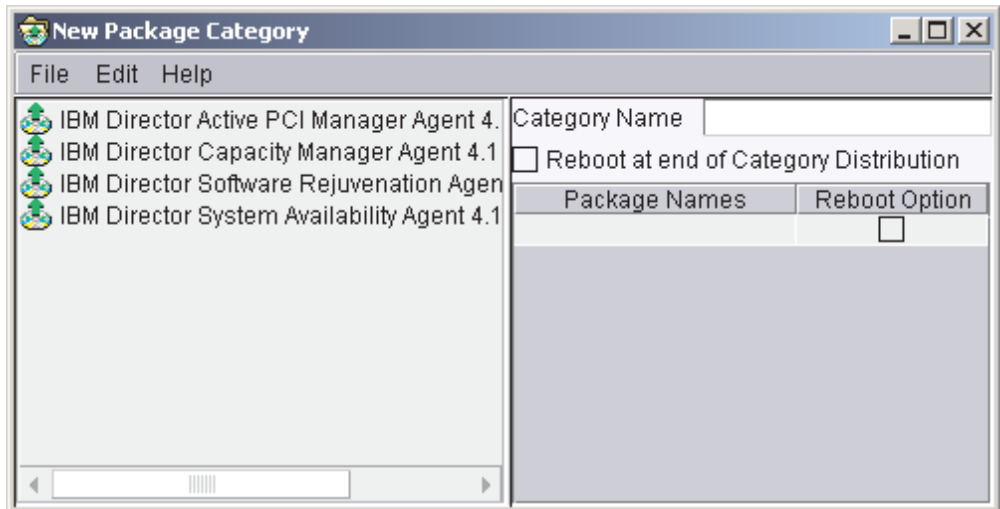


Figure 75. New Package Category window

2. Double-click a software package in the left pane to add the package to the category. The order in which the software packages are displayed in the right pane specifies the order of delivery when that category is distributed. To modify

the order in which software packages are delivered, in the right pane, click a package, then click **Edit** and the applicable option (**Move Package Up** or **Move Package Down**).

3. (Optional) You can set the managed system to restart after a particular software-package delivery by selecting the **Reboot Option** check box. Or, you can opt to restart the managed system upon completion of the distribution of all software packages in that category by selecting the **Reboot at end of Category Distribution** check box.
4. Click **File** → **Save** to save the new software-package category.

Complete the following steps to edit an existing software-package category:

1. In the IBM Director Console Tasks pane, expand the **Software Distribution** task.
2. Right-click the package category you want to edit and click **Open**. The Edit Package Category window opens.
3. Double-click a software package in the left pane to add the package to the category, or right-click a software package in the right pane and click **Delete** to delete it from the category. The order in which the software packages are displayed in the right pane specifies the order of delivery when that category is distributed. To modify the order in which software packages are delivered, in the right pane, click a package, then click **Edit** and the applicable option (**Move Package Up** or **Move Package Down**).
4. (Optional) You can set the managed system to restart after a particular software-package delivery by selecting the **Reboot Option** check box. Or, you can opt to restart the managed system upon completion of the distribution of all software packages in that category by selecting the **Reboot at end of Category Distribution** check box.
5. Click **File** → **Save** to save any changes made to an existing category.

## Working with software packages

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

### Viewing software-package contents

You can view the contents of a software 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. Then, right-click the package for which you want to see the contents, and click **Package Information**. The Package Summary window opens.

### Editing a software package

You can edit an existing software package by double-clicking the package. The applicable 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 software-package access

You can restrict access to a software package by specifying a user name and password combination that you must type to gain access to the package. To enable this option, right-click the package and click **Security**. Type a user ID and password for the user that you want to allow to modify this package, and click **OK**.

### Exporting a software package (Premium Edition only)

If you have IBM Director Software Distribution Premium Edition, you can export a software package for use on another management server or to back up a software package.

Complete the following steps to export a software package:

1. Right-click a software package and click **Export**. The Export Software Distribution window opens.
2. In the **File Name** field, type a file name and click **Save**.

### Viewing the software-distribution history for a software package

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

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

### Viewing software-package creation and distribution status

Using the Package Audit Log, you can determine the status of software 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.

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



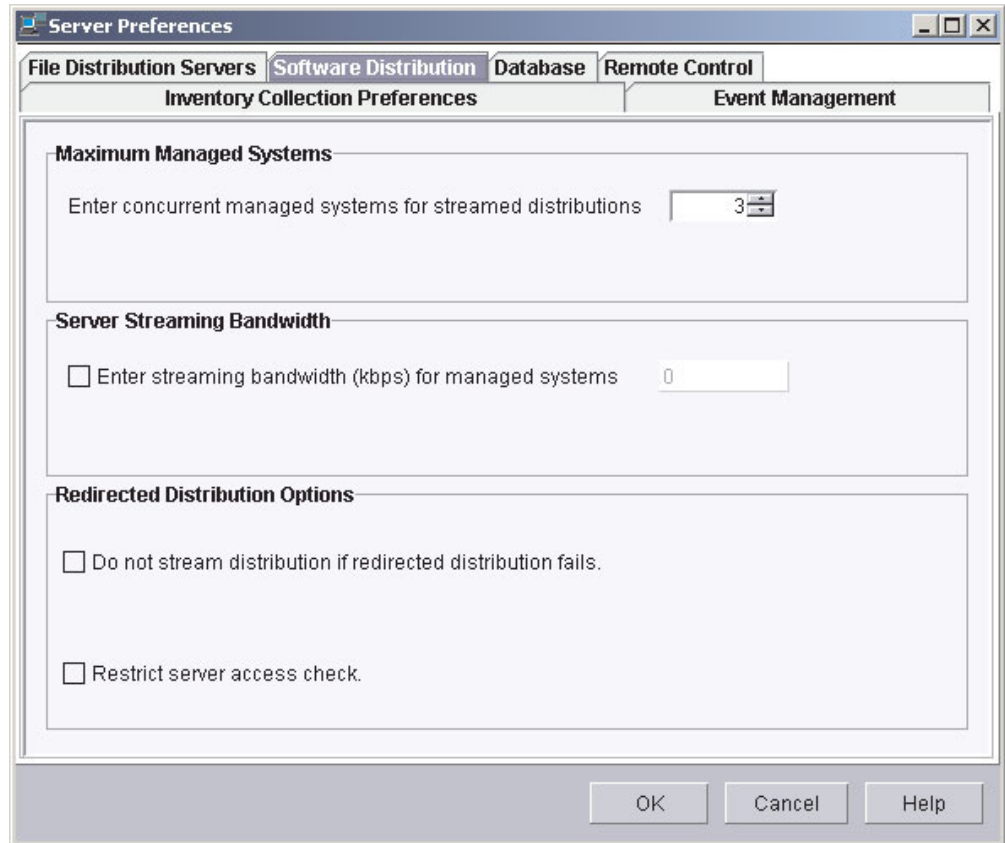


Figure 76. Server Preferences window

3. Change the applicable selections. Click **OK**.

## Viewing details about file-distribution servers and software packages

Using the File Distribution Servers Manager you can view details about file-distribution servers and the software packages stored on a file-distribution server.

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**.

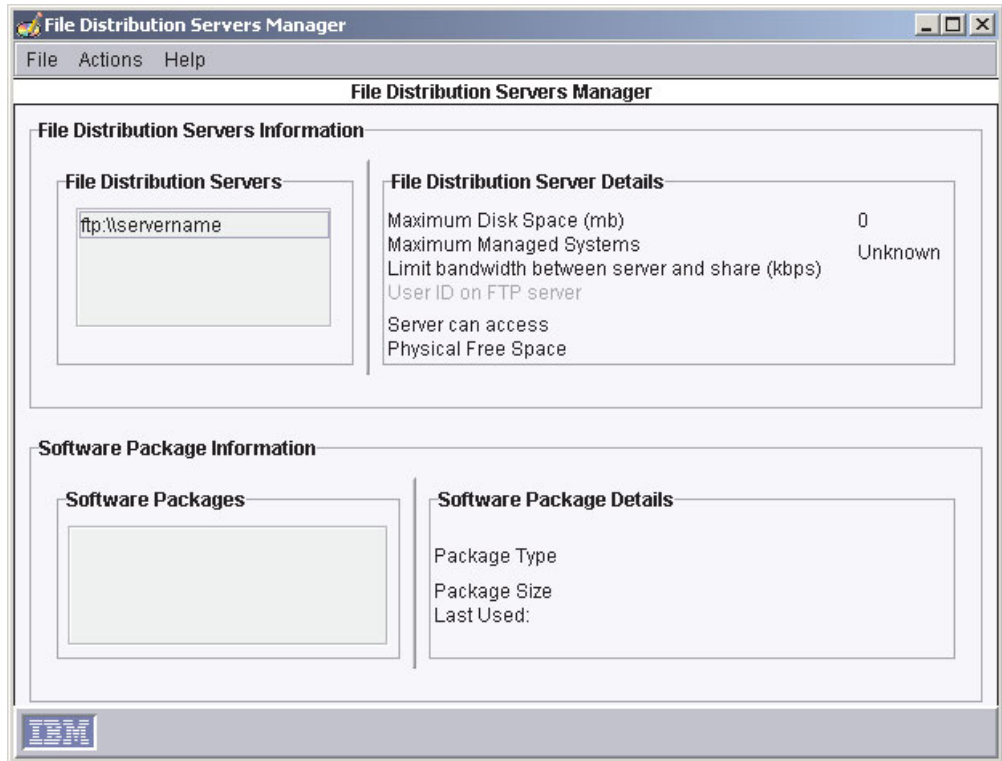


Figure 77. File Distribution Servers Manager

The software packages that are stored on the file-distribution server selected in the File Distribution Servers group box are displayed in the Software Packages group box.

You can perform the following tasks in the File Distribution Servers Manager window:

- To view the file-distribution maintenance log, click **File** → **Maintenance Log**.
- To test access to the file-distribution servers, click **Actions** → **Test Access to All File Distribution Servers**. To test access to an individual file-distribution server, click the file-distribution server in the File Distribution Servers group box; then, click **Actions** → **Test Access to Selected File Distribution Server(s)**.
- To refresh a software package from the file-distribution server, click the package in the Software Packages group box; then, click **Actions** → **Refresh Package on File Distribution Server**.
- To delete a software package from the file-distribution server, click the package in the Software Packages group box; then, click **Actions** → **Remove Package from File Distribution Server**.

## Software Rejuvenation

You can use the Software Rejuvenation task, part of the Server Plus Pack, to avoid unplanned system outages due to resource exhaustion. As software runs over long periods of time, operating systems steadily consume resources and fail to relinquish them properly. This phenomenon (known as resource exhaustion or software aging) can eventually lead to ineffective operation or even system failure. Software Rejuvenation monitors operating-system resources, predicts system outages, and generates resource exhaustion events; once notified, system administrators can take corrective action before a failure occurs. System administrators can also use

Software Rejuvenation to automate the process of restarting operating systems, at convenient times and in advance of actual failures.

Using Software Rejuvenation, you can:

- Schedule a rejuvenation to occur for one specific time or on a repeating interval, on an entire operating system or for a specific Windows service or Linux daemon.
- Configure Predictive Software Rejuvenation so that managed-system rejuvenations are scheduled automatically based on actual resource usage and trends.
- Receive notification when a managed system is predicted to exhaust a monitored resource or when a managed system is being rejuvenated.
- Prevent rejuvenations from occurring under certain conditions or on specified days.

## Starting the Software Rejuvenation task

To start the Software Rejuvenation task, in the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.

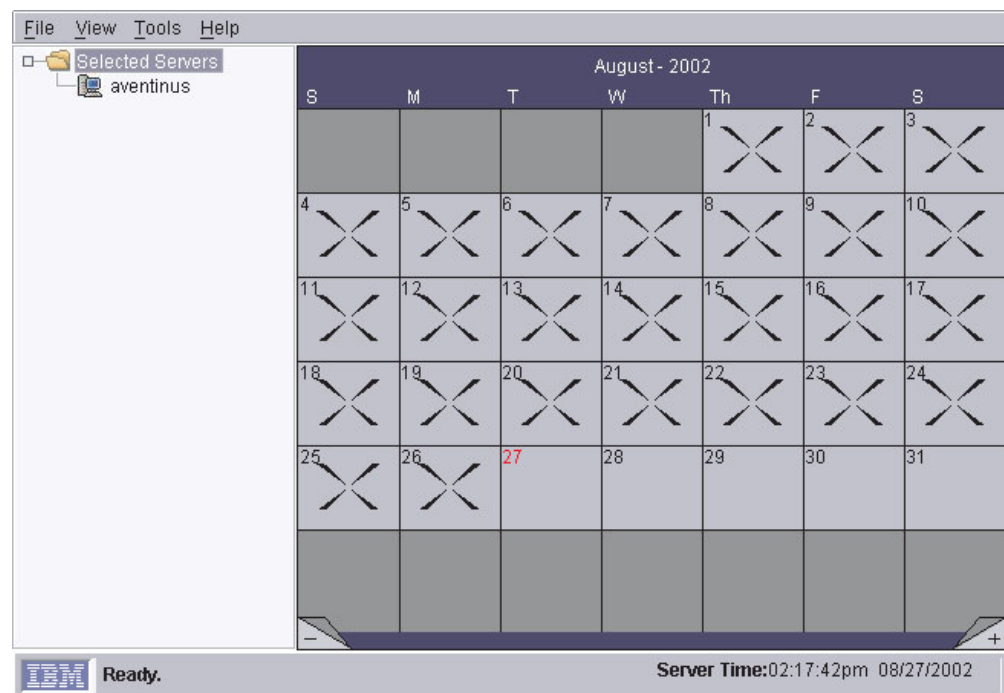


Figure 78. Software Rejuvenation window

The Software Rejuvenation window has two panes: the left pane is a tree view with server folders, and the right pane is a calendar.

## Configuring a service rejuvenation

You must configure Software Rejuvenation manually if you want to schedule the rejuvenation of a Windows service or Linux daemon. For a Windows service, service rejuvenation does not stop dependent services.

Complete the following steps to configure a service rejuvenation:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. Click **Tools** → **Service Rejuvenation**. The Service Rejuvenation window opens.

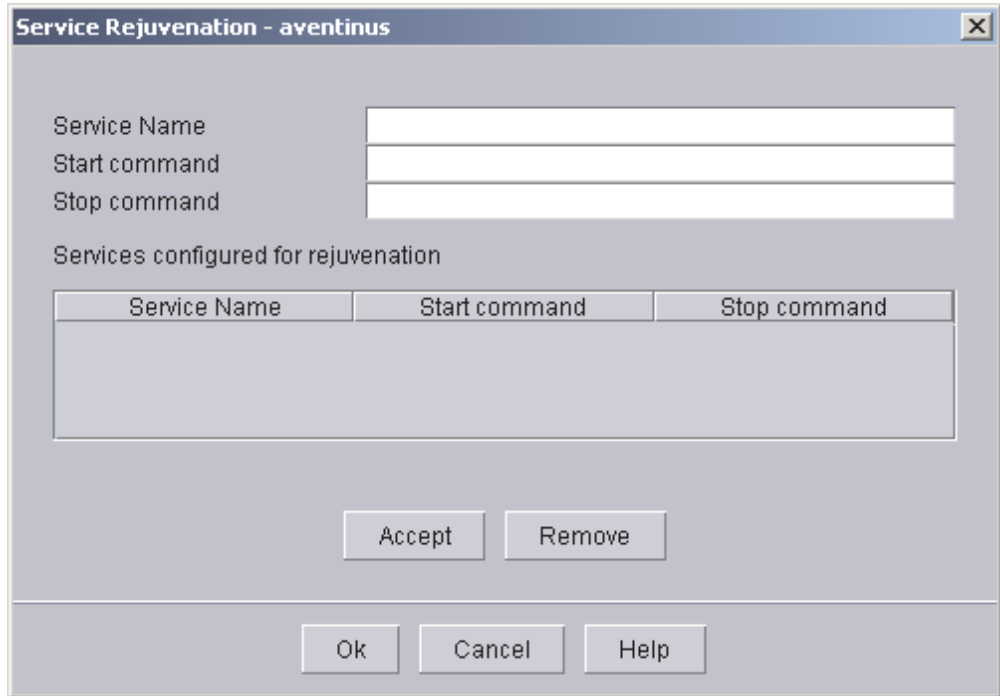


Figure 79. Service Rejuvenation window

3. In the **Service Name** field, type the name of a Windows service or Linux daemon. If you type the name of a Windows service, go to step 6.
4. In the **Start command** field, type the command used to start this daemon. (For Windows services, this field is automatically filled with net start and cannot be changed.)
5. In the **Stop command** field, type the command used to stop this daemon. (For Windows services, this field is automatically filled with net stop and cannot be changed.)
6. Click **Accept**. The Windows service or Linux daemon name, start command, and stop command are displayed in the list of services configured for rejuvenation.
7. Click **OK** to complete the configuration. In the Software Rejuvenation window, the Windows service or Linux daemon is displayed in the left pane under the applicable managed system.

You can schedule the Windows service or Linux daemon for rejuvenation now. Go to “Scheduling a software rejuvenation”.

## Scheduling a software rejuvenation

You can schedule a software rejuvenation to occur on a specific day, time, or frequency.

Complete the following steps to schedule a software rejuvenation to occur:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. In the left pane, click the managed system, Windows service, or Linux daemon on which you want to schedule a rejuvenation; then, drag the managed system onto the calendar date (in the right pane) on which you want the first rejuvenation to occur. The Repeat Schedule window opens.

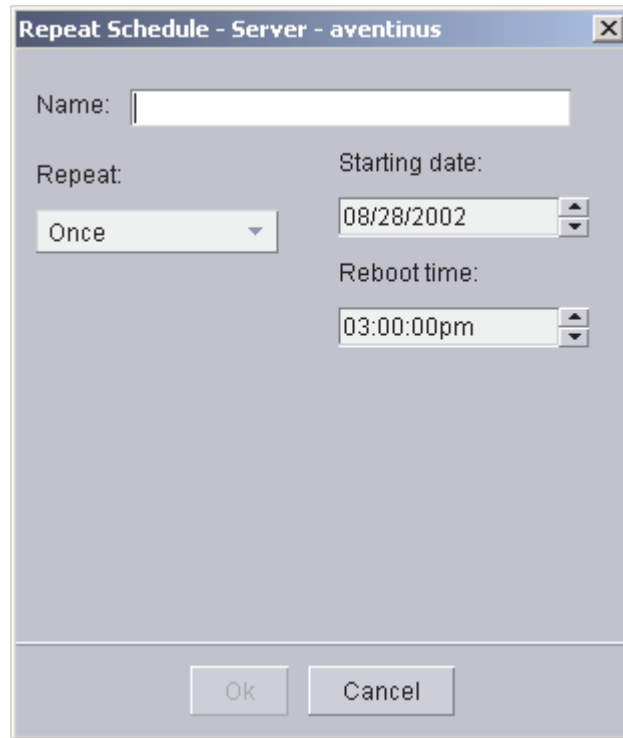


Figure 80. Repeat Schedule window

3. Type a name for the schedule.
4. From the **Repeat** list, select the frequency with which you want rejuvenations to occur.
5. From the **Starting date** list, select the date on which you want the first rejuvenation to occur.
6. From the **Reboot time** list, select the time for the rejuvenation to occur. Click **OK**.
7. Click **File** → **Save** to save the schedule.

## Editing a rejuvenation schedule

Complete the following steps to change the date, time, or frequency of a rejuvenation schedule:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. In the Calendar pane, right-click the schedule you want to edit, then click **Edit Schedule** → **Schedule *schedule name***. The Repeat Schedule window opens.
3. Edit the rejuvenation schedule settings. Click **OK**.
4. Click **File** → **Save** to save your changes.

## Deleting a rejuvenation schedule

Complete the following steps to delete a rejuvenation schedule:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. In the Calendar pane, right-click the schedule you want to delete; then, click **Delete Schedule** → **Schedule *schedule name***. The Verify Remove window opens.
3. Click **Yes** to delete the schedule.
4. Click **File** → **Save** to save your changes.

**Note:** If a managed system is scheduled for rejuvenation using a repeating schedule, such as every Tuesday, deleting the schedule for one date removes it from all other repeating dates. That is, the entire named schedule is deleted.

## Creating a schedule filter

You can prevent software rejuvenations from occurring on specific days by using a schedule filter. Use this function to prevent rejuvenations on peak usage days.

Complete the following steps to create a schedule filter:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. Click **Tools** → **Schedule Filter**. The Schedule Filter window opens.

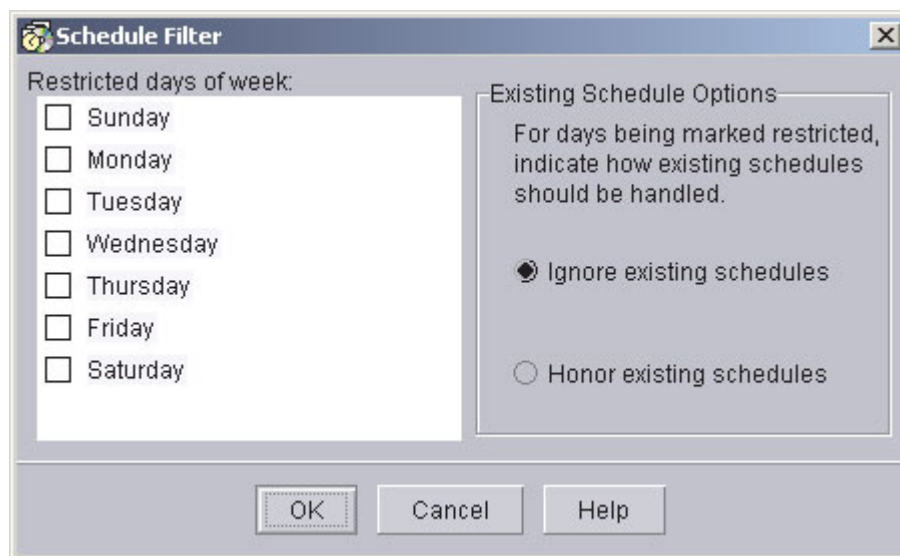


Figure 81. Schedule Filter window

3. Select the check boxes of the days of the week on which you want to prevent rejuvenations from occurring.
4. Under the Existing Schedule Options group box, specify if you want to honor or ignore already existing schedules. Click **OK**.

## Setting rejuvenation options for all managed systems

You can set options for software rejuvenation that apply to all managed systems. For example, you can specify a minimum number of days that must elapse between rejuvenations to prevent excessive rejuvenations from occurring.

Complete the following steps to set rejuvenation options:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. Click **Tools** → **Rejuvenation Options**. The Rejuvenation Options window opens.

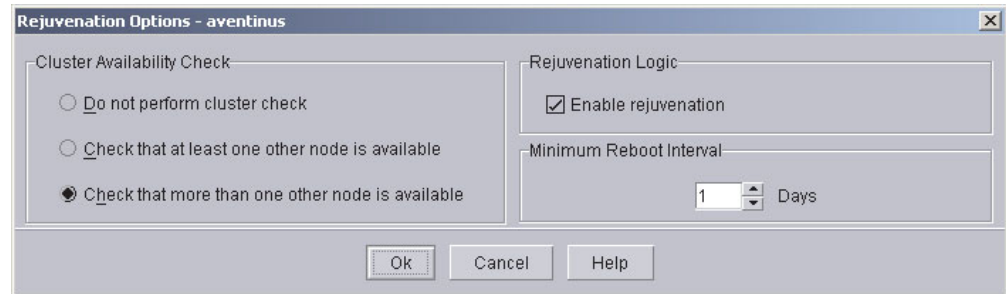


Figure 82. Rejuvenation Options window

You can set the following parameters:

### Cluster Availability Check group box

Specifies the rules for rejuvenating a member of a cluster. Rejuvenation occurs only if all the managed systems in the cluster meet the selected criteria.

- Do not perform cluster check
- Check that at least one other node is available
- Check that more than one other node is available

### Rejuvenation Logic check box

Selecting this check box enables all rejuvenations. This setting is maintained by IBM Director Server and applies to all rejuvenations scheduled through that management server.

### Minimum Reboot Interval

Specifies the number of days that must elapse between rejuvenations.

3. Complete the fields; then, click **OK**.

## Starting the Prediction Configuration wizard

You can predict resource exhaustion for a managed system or group based on trends in resource utilization. When resource exhaustion is predicted, an alert is generated and a rejuvenation can be scheduled automatically. Before you can start prediction, you must configure this function using the Prediction Configuration wizard.

Complete the following steps to configure a managed system or group for prediction:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. In the left pane, click a managed system.

3. Click **Tools** → **Prediction** → **Configure Wizard** to start the configuration wizard.

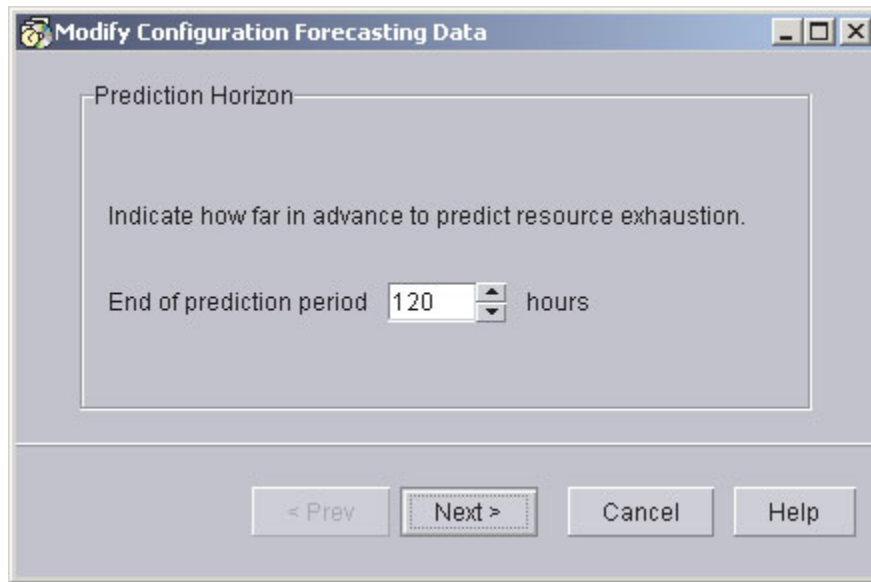


Figure 83. Prediction Configuration wizard

4. From the Modify Configuration Forecasting Data window, select the parameters for the prediction data.
5. Specify the Prediction Horizon. This value indicates how many hours into the future the prediction algorithms will forecast exhaustions. If a resource is predicted to exhaust between the current time and the prediction horizon, a notification, and optionally a rejuvenation schedule, is generated. Note that prediction horizons less than 24 hours might cause high CPU utilization on slower managed systems.
6. Click **Next**.
7. From the Modify Configuration Notification and Scheduling window, select the parameters that control alerts and rejuvenation schedules.
  - Select if you want both an alert and a rejuvenation schedule to be generated, or if you want a notification only.
  - Specify how software rejuvenation handles the case where an automatically generated rejuvenation schedule conflicts with a day that has been marked previously as restricted for rejuvenations.
    - Select **honor** if you want the restricted day setting to block the rejuvenation schedule.
    - Select **ignore** if you want the rejuvenation schedule to override the restricted day designation. Note that an alert will be sent and the system rejuvenated according to the schedule.
  - Specify the grace period, which is the amount of time between the notification and the initiation of the software rejuvenation. Note that the grace period should not exceed the prediction horizon.
8. Click **Next**.
9. Use the Modify Configuration Action Plan window to create simple event action plans that are executed when a resource exhaustion is predicted.



- Select **Console** if you want a pop-up message to display on IBM Director Consoles. You must enter the message you want to display, the user names of the individuals who should receive the message, and the delivery criteria for the message.
- Select **Ticker Tape** if you want a message to run along the ticker tape of IBM Director Console. You must enter the message you want to appear and the user names who should receive the message.
- Select **None** if you do not want a visual message to be generated and displayed.

**Note:** Regardless of which selection you make in this window, an event is sent to the IBM Director event log. You can use that event in an event action plan of your own design.

10. Click **Finish** to complete the configuration.

When you complete configuration, prediction starts automatically on the specified managed systems. Any managed systems for which prediction is enabled are displayed with a red background in the right pane of the Software Rejuvenation window.

### Ending prediction on a managed system

To end prediction on a managed system, click **Tools** → **Prediction** → **End Prediction**.

## Viewing resource utilization

You can view graphic representations of resource utilization and the prediction algorithms in real time using the Trend Viewer function. Before you can use the Trend Viewer, you must configure the managed system for prediction. See “Starting the Prediction Configuration wizard” on page 143 for information about how to do this.

Complete the following steps to start the Trend Viewer:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or group. The Software Rejuvenation window opens.
2. In the left pane, click a managed system.
3. Click **Tools** → **Trend Viewer**. The Trend Viewer window opens.
4. From the **Resource** list, select the resource you want to view. The selected resource displays.

## Creating an event filter for software-rejuvenation events

Using the Event Action Plan Builder, you can create an event action plan that notifies you when a software-rejuvenation event occurs. These steps only cover the process of creating an event filter specifically for a software-rejuvenation event. For more information about creating and implementing an event action plan, see “Event action plans” on page 20.

Complete the following steps to create a software-rejuvenation event filter:

1. In IBM Director Console, click **Tasks** → **Event Action Plan Builder**. The Event Action Plan Builder window opens.
2. Right-click in the Event Filter pane and click **New** → **Simple Event Filter**. The Event Filter Builder window opens.
3. On the **Event Type** page, clear the **Any** check box. Click **Software Rejuvenation** to expand the tree. Select one of the events listed.

4. Click **File** → **Save As** to save the filter. The new filter is displayed in the Event Filters pane of the Event Action Plan Builder window.

In order to be notified of a software-rejuvenation event, you must create a new event action plan, customize an event action, then associate the filter you just created with the event action and the event action plan. See “Event action plans” on page 20 for more information about how to do this.

## Using keyboard shortcuts

You can use the following keyboard shortcuts when working with Software Rejuvenation:

- **Ctrl+E**: After selecting a day in the calendar that contains a rejuvenation schedule icon, use this shortcut to open the Repeat Schedule window.
- **Ctrl+D**: Use this shortcut to delete a highlighted object. If you are deleting a rejuvenation schedule from a day where there are multiple schedules, a pop-up menu allows you to select which schedule to delete.
- **Ctrl+H**: Use this shortcut to highlight all of the days associated with a rejuvenation schedule.

---

## System Accounts

You can use the System Accounts task to view and change user and group security profiles on managed systems running Windows.

To start the System Accounts task, drag the **System Accounts** task onto a managed system or group that supports System Accounts. The System Accounts window opens.

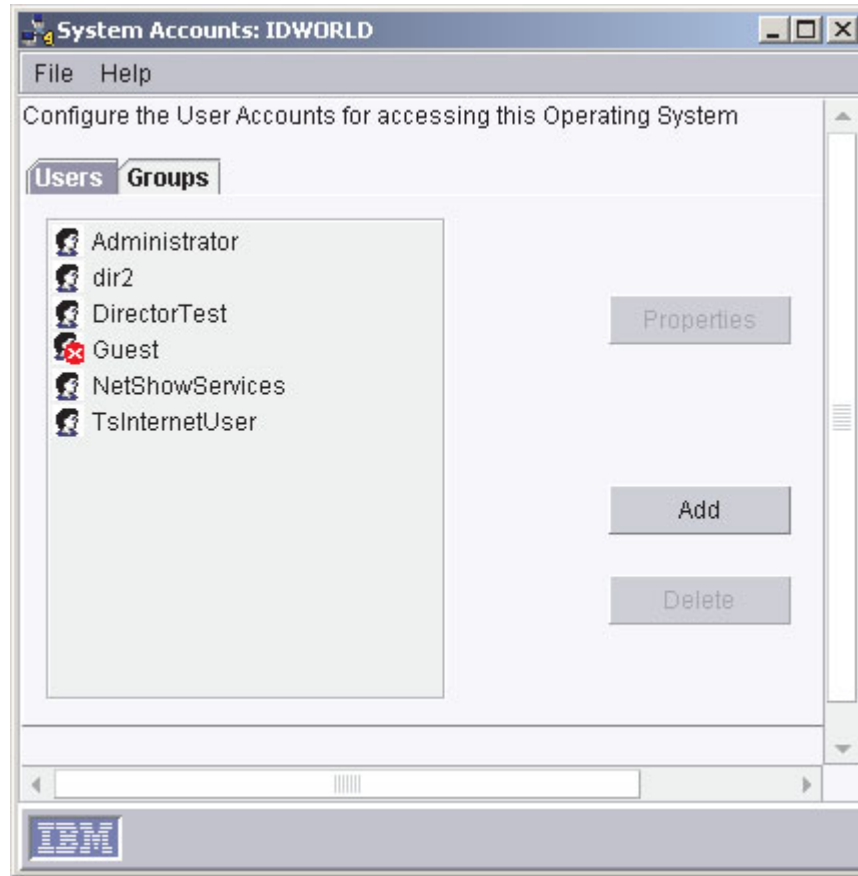


Figure 84. System Accounts window

---

## System Availability

You can use the System Availability task, part of the Server Plus Pack, to analyze the availability of a managed system or group. You can view statistics about managed system uptime and downtime through reports and graphical representations.

System Availability can identify problematic managed systems that have had too many unplanned outages over a specified period of time or a managed system that has availability data that is too old or fails to report data to IBM Director Server. When a System Availability report is generated, managed systems that meet the criteria you specify as being problematic are flagged as such.

To identify a managed system as problematic, the managed system must have the IBM Director Version 4.1 System Availability Agent installed.

**Note:** (Windows only) The System Availability task uses information from the system log file; a damaged, missing, or full log file affects this tool. If you clear the system log, all system availability information is lost as well.

### Starting the System Availability task

To start the System Availability task, in the IBM Director Console Tasks pane, drag the **System Availability** task onto a managed system or group that supports

System Availability. The System Availability window opens, displaying the Distribution of System Outages by default.

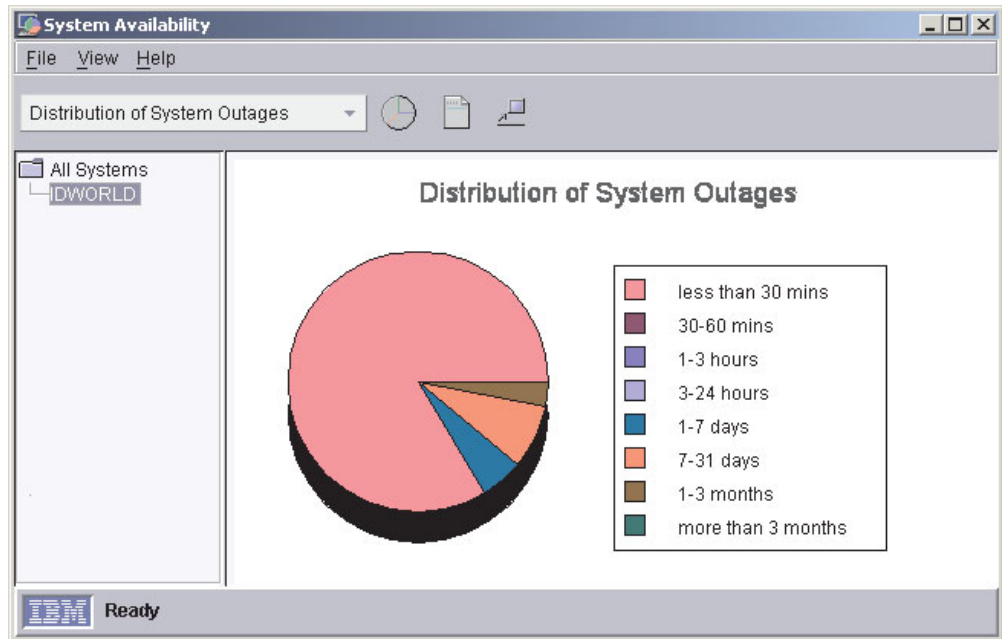


Figure 85. System Availability window

The list on the toolbar in the System Availability window has four options:

**Distribution of System Outages**

A pie chart representing the percentage of all system outages.

**Distribution of System Uptime**

A pie chart representing the percentage of all system uptime.

**System Outages by Day of Week**

A bar chart measuring the frequency of outages by day of the week, with planned and unplanned outages differentiated.

**System Outages by Hour of Day**

A bar chart measuring the frequency of outages by hour of the day, with planned and unplanned outages differentiated.

**Notes:**

1. (Windows only) This note affects all supported Windows operating systems that are configured to adjust automatically for daylight saving time. The event times specified in the system availability report might be off by one hour from the event times in the Windows event viewer, because the Windows event viewer adds or subtracts one hour to adjust for daylight saving time. Because this adjustment can cause duplicate entries in the System Availability database when the time adjustment is made, System Availability does not use the daylight saving time adjustments.
2. (Linux only) On IBM Director Agents where compression of message logs is the default, turn off compression of message logs to view system availability reports.

Also, you can view the availability report, which is an overall statistical summary with event and problematic details displayed, by clicking **View** → **Availability Report**.

The availability report is a snapshot of system availability. It provides measurements for the currently selected managed systems in a tree structure, or all managed systems if the root of the tree is selected. Problematic managed systems are listed in the detail section and are flagged in the tree structure by a red X.

In the System Availability window, you can detach the current view to compare and contrast different system availability views and timeframes. Click **View** → **Detach View**. The current view is separated as an independent window that does not reflect subsequent changes to the report.

With the exception of a detached view, you can print any window displayed in the System Availability task by clicking **File** → **Print**.

## Changing the graph dates

Complete the following steps to specify the time period for which data is graphed:

1. In the System Availability window, click **File** → **Set Time**. The Set Time window opens.
2. Choose the dates for which you want to view data. Click **OK**.

## Changing the settings criteria

System Availability uses a window of time to scan for problematic systems. The time begins a specified number of days in the past (the default is 30) and ends with the current time. The number of unplanned outages that occur in this timeframe is counted, and if the total number meets or exceeds the specified count, the managed system is marked as problematic. Or, you can specify a percentage of time that the managed system has unplanned outages as opposed to a specific number of outages by selecting the **Percentage** check box.

To specify the settings criteria, click **File** → **Settings**. The Settings window opens.

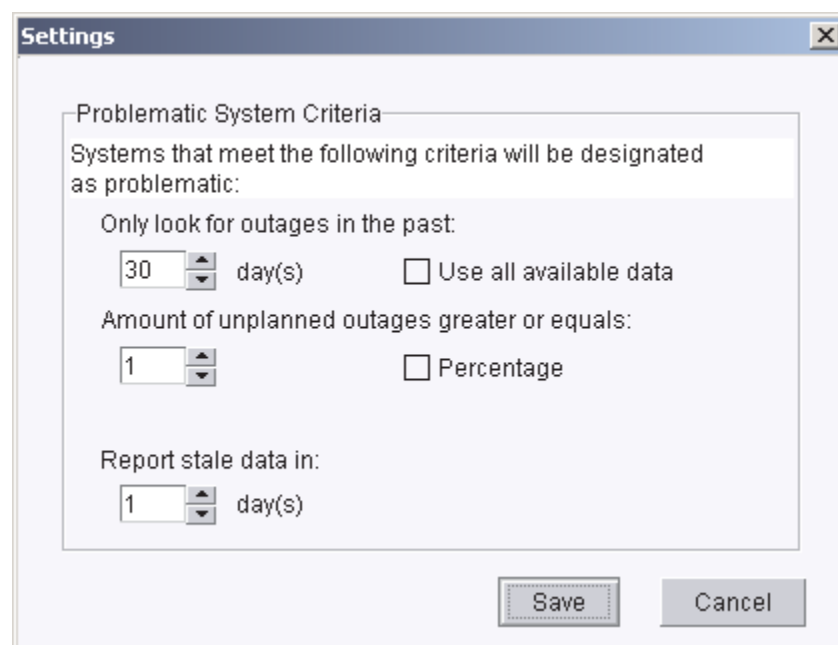


Figure 86. Settings window

Change any of the criteria; then, click **Save**.

## Saving the system-availability report

You can save the current report as a series of HTML and GIF files to a directory on the management console. Then, you can view the report in a Web browser at a later time.

Complete the following steps to export a report:

1. Follow the steps in “Starting the System Availability task” on page 147 to generate a system availability report.
2. After the report is generated, click **File** → **Export Availability Report**. The “Select a directory to save report files” window opens.
3. Type a file name and click **Select**. The Confirm Directory window opens.
4. Click **OK**. The files are saved to the location you specified.

---

## 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 and any related parameters
- One or more event actions, which occur in response to a filtered event

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

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

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

1. The managed system generates an event and forwards the event to all the management servers that have discovered the managed system (except for some events such as those generated through meeting or exceeding a Resource Monitor threshold, which are sent only to the management server where the thresholds are configured and applied).
2. IBM Director Server processes the message and determines which managed system generated the event and which group or groups the managed system belongs to.
3. IBM Director determines whether any event action plans are applied to the managed system or to any of the groups of which the managed system is a member.
4. If an event action plan has been applied, IBM Director Server determines whether any event filters match the event that was generated.
5. The management server performs any event actions for each matching event filter.

---

### Planning and designing event action plan implementations

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

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

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

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

- Consider all the managed systems of the same type as a whole. What would you want to monitor on most or all of these systems? This answer determines the grouping and event filters for your first event action plan.
- Consider your managed systems as smaller groups. Decide how you would group them based on the additional events for which you would want to monitor. The smaller groups are usually based on the following criteria:
  - Managed-system manufacturer, for vendor-specific events
  - Function of the managed system, for services and resources specific to that function
- What type of managed systems are you monitoring?
- What is the function of the managed system?
- What are the key monitors for the managed system?
- Are there other managed systems for which the same monitors are desirable?

## Grouping managed systems

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

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

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

#### **By manufacturer**

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

#### **By function**

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

#### **By resources**

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

#### **By management technology**

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

## Structuring event action plans

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



Consider the following examples of event action plan structures:

**A structure based on the areas of responsibility of each administrator**

Typically, servers are maintained and managed by one group of personnel, and desktop computers and mobile computers are maintained by another group of personnel.

**A structure based on administrator expertise**

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

**A structure based on managed-system function**

Servers performing different functions need to be managed differently.

**A structure based on the type of event**

Examples are monitoring a specific process, monitoring for hardware events, and monitoring nearly anything else.

**A structure based on work-day shifts**

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

## Structuring event filters

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

- All managed systems targeted for the filter are able to generate all events included in the filter. If the managed system does not generate the event for which the filter is defined, the filter is not going to be effective on that managed system.
- The event actions that will be used to respond to the event are the same for all targeted systems.
- The other event filter options besides the event type are common for all targeted systems. These settings include the times the event filter is active, the severity of the event, and other attributes.

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

---

## Building an event action plan

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

1. Using the Event Action Plan Builder, create a new event action plan.
2. Using the Event Action Plan Builder, create an event filter or filters, then drag the filter or filters onto the event action plan.
3. Using the Event Action Plan Builder, customize an event action or actions, then drag the action or actions onto the applicable event filter.

4. Activate the event action plan by applying it to a single managed system, more than one managed system, or a group.

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

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

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

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

## Event filters

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

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

There are four types of event filters:

### Simple event filter

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

Eleven filters of this type are predefined:

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

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

### Duplication event filter

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

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

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

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

### Threshold event filter

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

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

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

### Exclusion event filter

In addition to the simple event filter options, you can define event filtering criteria using the Event Type page and correlate another set of criteria using the Excluded Event Type page. The Excluded Event Type excludes specified types of events from the criteria. That is, you can filter on a specified group of events but exclude certain events that might occur within that group.

## Creating an event filter

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

### Event Type page

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

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

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

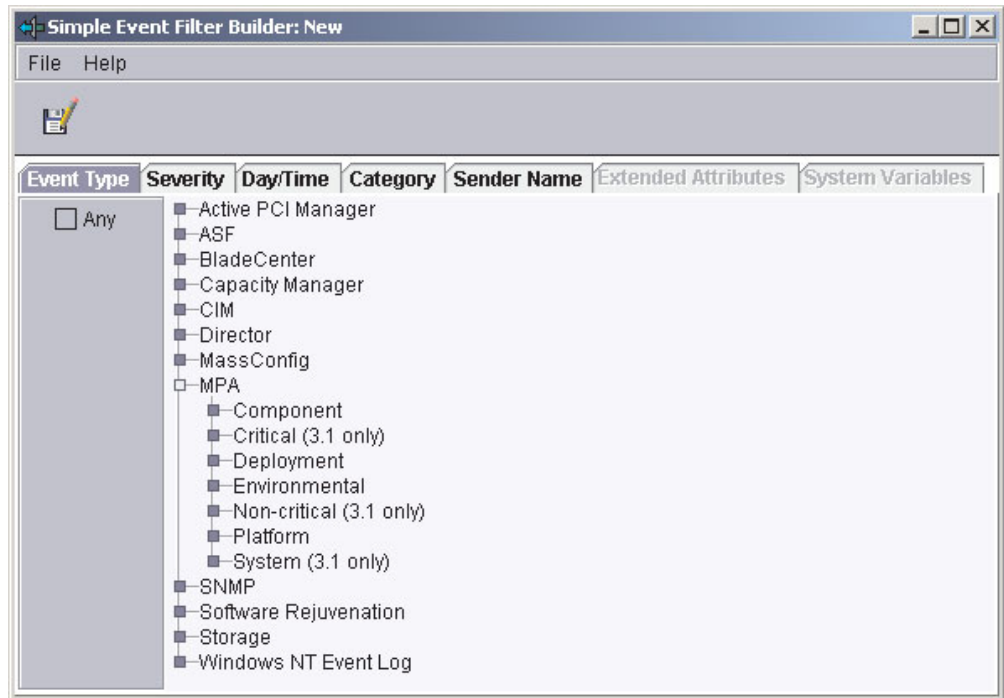


Figure 87. Simple Event Filter Builder window

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

### Severity page

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

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

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

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

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

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

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

### **Unknown**

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

### **Day/Time page**

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

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

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

### **Category page**

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

### **Sender Name page**

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

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

### **Extended Attributes page**

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

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

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

### **System Variables page**

This page is available only if there are one or more system variables. A system variable consists of a user-defined keyword and value that are stored in IBM

Director Server. You can create a system variable using the Set Event System Variable event action. For more details about this event action, see “Event data substitution variables” on page 162.

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:

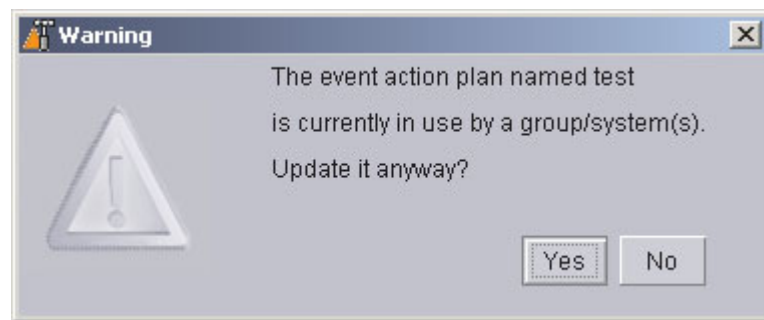


Figure 88. Prompt when modifying an existing event action plan

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

## Event actions

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

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

Event action names should be as descriptive as possible to reflect the action that will take place. The Event Action Plan Builder sorts all event actions alphabetically. For example, if the event action involves sending a message to a pager, start the event action name with Pager; if the event action involves sending a message to a phone, start the event action name with Phone. Using such a naming convention ensures entries are grouped conveniently in the Event Action Plan Builder window.

### Creating a pop-up message notification event action

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

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

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

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

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

where

- `cmd /c` is part of the command line that indicates to the Windows operating system on the management server to close the window automatically when the command is completed.
- `C3PO` is the managed system on which you want the message to be displayed.
- `&system` is an event data substitution variable that in the message is substituted with the name of the managed system that generated the event. See "Event data substitution variables" on page 162 for more information.
- `&severity` is an event data substitution variable that in the message is substituted with the event severity.
- `&category` is an event data substitution variable that in the message is substituted with the event category (either Alert or Resolution).

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

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

### Creating an e-mail notification event action

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

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

1. In the Actions pane, right-click **Send an Internet (SMTP) E-mail** and click **Customize**.
2. Complete the fields. See Figure 89 on page 160 for example values.

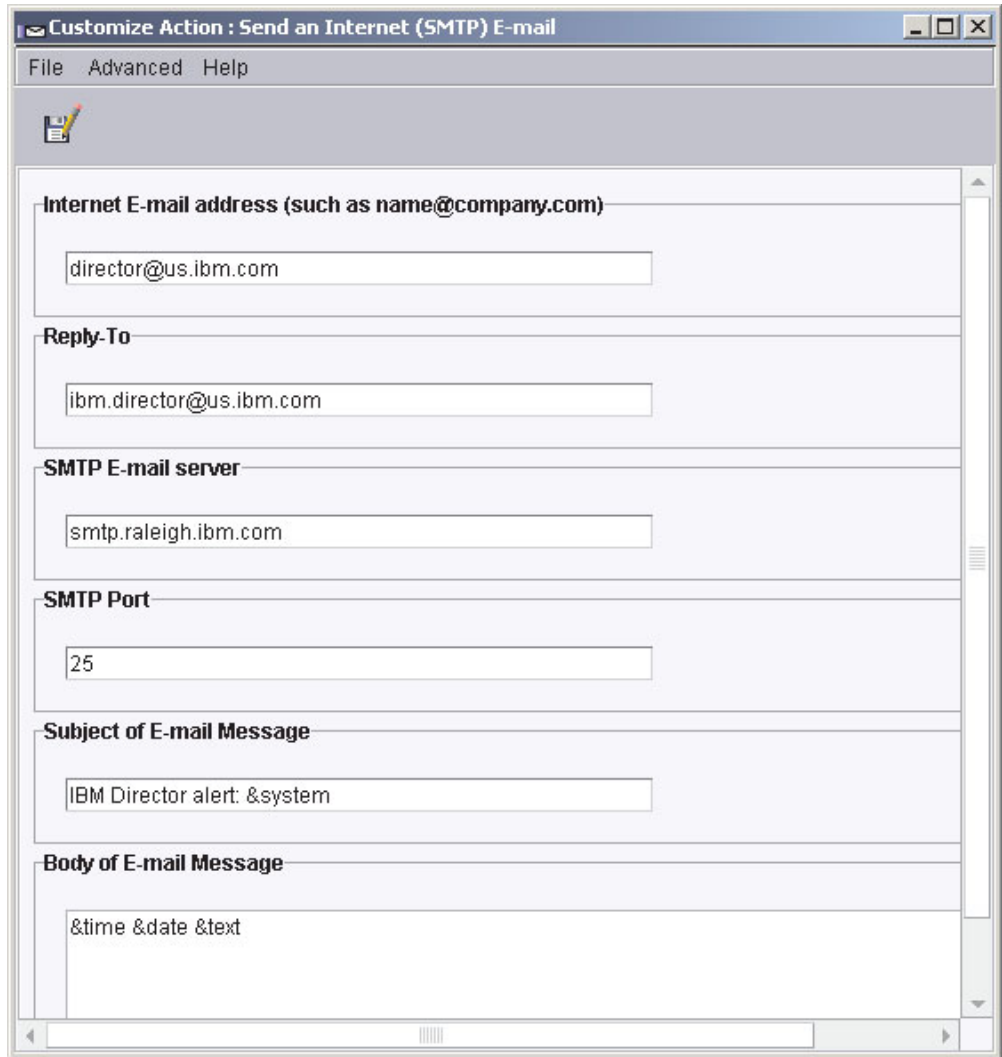


Figure 89. Customize Action window displaying example values

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

3. Click **File** → **Save As** to save the event action. The Save Event Action window opens.

4. Type a name for the event action. In this example, E-mail: director@us.ibm.com generic is used.

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

5. Click **OK**. The new event action is displayed in the Actions pane as a subentry under the **Send an Internet (SMTP) E-mail** event action type.



## Available event action types

The following table describes all the available event action types.

Table 5. Event action types

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

Table 5. Event action types (continued)

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.

Table 6. Event data substitution variables

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

Table 6. Event data substitution variables (continued)

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



---

## Chapter 5. Working with management servers using the command-line interface (DIRCMD)

This chapter provides information about installing and using the IBM Director command-line interface (DIRCMD). Command Line Interface is the command-line interface for IBM Director Server. System administrators can use a command-line prompt to access, control, and gather information from IBM Director Server.

---

### Installing and accessing DIRCMD

The IBM Director command-line interface is automatically installed with IBM Director Server, IBM Director Agent, and IBM Director Console. It is available on all operating systems supported by IBM Director 4.1, except Novell NetWare.

The system from which a system administrator invokes DIRCMD is a *DIRCMD client*.

Access to DIRCMD is limited to IBM Director super-users (members of the DirSuper group). By default, the connection between the DIRCMD client and the management server is a nonsecure TCP/IP data link. Secure socket layers (SSL) can be used to secure the data transmission.

---

### DIRCMD syntax

The DIRCMD syntax adheres to the following conventions:

- Commands are shown in lowercase letters.
- Variables are shown in italics and explained immediately afterward.
- Optional commands or variables are enclosed in brackets.
- Where you can type one of several commands, the values are separated by slashes.
- Default values are underlined>.
- Repeatable parameters are enclosed in braces.

The general syntax for DIRCMD is:

`dircmd management [options] bundle command arguments`

where:

- *management* specifies the management server and IBM Director user account.
- *options* specifies optional commands that direct the DIRCMD client behavior.
- *bundle* specifies the bundle you want to invoke, for example:
  - server (server management)
  - native (managed system)
  - event (event management)
  - monitor (resource monitor)
  - procmon (process monitor)
  - snmp (snmp device)
- *command arguments* are used by the individual bundle during processing.

## Management

The following table describes the management commands. These commands are all required.

Table 7. Management commands

Command	What it does	Syntax
<b>server</b>	This command specifies the management server	-s <i>server</i>  where <i>server</i> is one of the following: <ul style="list-style-type: none"><li>• DNS-resolvable host name of the management server</li><li>• TCP/IP address of the management server</li></ul>
<b>userID</b>	This command specifies the IBM Director user.	-u <i>userID</i>  where <i>userID</i> is a valid IBM Director super-user account on the management server.
<b>password</b>	This command specifies the password for the IBM Director user account.	-p <i>password</i>  where <i>password</i> is the password for the IBM Director super-user account on the management server.

To begin a DIRCMD session, a user might type the following text at a command prompt:

```
dircmd -s IDworld -u infodeveloper -p passw0rd ...
```

where IDworld is the host name of the management server, infodeveloper is the user ID of an IBM Director super-user (member of the DirSuper group), and passw0rd is the password associated with the infodeveloper account.

## Options

The following table describe the DIRCMD options. These commands are all optional.

Table 8. DIRCMD options

Command	What it does	Syntax
<b>bundle</b>	This command lists all of the DIRCMD bundles.	-b  <b>Notes:</b> <ol style="list-style-type: none"><li>1. When this command is issued, no other commands can be run.</li><li>2. The help is provided from the management server, not the DIRCMD client.</li></ol>
<b>help</b>	This command provides help about DIRCMD usage and syntax.	-h  <b>Notes:</b> <ol style="list-style-type: none"><li>1. When this command is issued, no other commands can be run.</li><li>2. The help is provided from the management server, not the DIRCMD client.</li></ol>

Table 8. DIRCMD options (continued)

<b>log</b>	This command displays and manages the DIRCMD log. This log contains a sequential record of <i>all</i> DIRCMD commands issued against the specified management server. The log is reset when either the management server or IBM Director Server is restarted.	-l [clear / size= <i>N</i> ]  where <ul style="list-style-type: none"> <li>• clear resets the DIRCMD log.</li> <li>• <i>N</i> is the maximum number of entries in the DIRCMD log. By default, this is set to 100.</li> </ul> <b>Notes:</b> 1. Only one log action (list <i>or</i> clear <i>or</i> size) can be performed at a time. 2. When this command is issued, no other commands can be run.
<b>filename</b>	This command specifies a file that is passed to the bundle command as an input argument. The contents of the file are read into the buffer <i>after</i> all the command arguments supplied at the command prompt.	-f <i>filename</i>  where <i>filename</i> is the path and name of the file.
<b>pipe</b>	This command directs the DIRCMD client to receive command-argument data from an input pipe. The data is read <i>after</i> any command arguments provided on the command line. This option enables the DIRCMD client to use output from the previously issued DIRCMD command or another DOS or UNIX command.	-r
<b>k</b>	This command directs the DIRCMD client to override the default TCP/IP data link connection class, com.tivoli.twg.libs.TWGTCPILink.	-k <i>datalink</i>  where <i>datalink</i> is the data link connection class. <b>Note:</b> If this command is used, you might need to specify data link parameters in order to properly configure the data link.
<b>o</b>	This command specifies data link parameters. (The default TCP/IP data link parameters are “2034,” which sets the socket port for com.tivoli.twg.libs.TWGTCPILink.)	-o <i>datalinkparms</i>  where <i>datalinkparms</i> are valid data link parameters.

The pipe command allows a user to pipe data from one command into another. For example, a user might type the following text at a command prompt:

```
dircmd -s IDWorld -u infodeveloper -p passwd0rd serverlistgroupmembers -t 17D
| dircmd -r -s IDWorld -u infodeveloper -p passwd0rd event listevents
```

In this example, an IBM Director super-user connects to the management server with the host name “IDWorld,” using the user ID “infodeveloper” and the password “passwd0rd.” By invoking the ListGroupMembers function of the server-management bundle, the first command specifies the object ID of each member of group 17D. The second command (and the use of the optional -r parameter) pipes the object IDs specified by the first command into the ListEvents function of the event-management bundle. The script generates a list of all events from the IBM Director group 17D.

## Server-management bundle

The following information explains how to use the server-management bundle, which provides general access to managed objects. You can invoke the server-management bundle to discover managed objects, list managed objects, list attributes of managed objects, perform a presence check on managed objects, delete managed objects, list group members, list dynamic group criteria, list inventory values, and create dynamic groups.

All server-management bundle functions must be preceded by the server command.

### Syntax

The following table contains information about the syntax for invoking the server-management bundle:

Table 9. Server-management bundle syntax

Function	What it does	Command arguments
<b>Help</b>	This function lists an overview of the bundle usage.	help
<b>List</b>	This function lists the function set for the bundle.	list
<b>DiscoverAll</b>	This function discovers all managed systems.	discoverall
<b>ListObjects</b>	This function lists all objects (systems, SNMP devices, and others) managed by IBM Director.	listobjects [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> <li>-r or -report lists the object name, object ID, type, state, whether encryption is enabled, whether access is denied, operating system, IP address, and host name.</li> <li>-t or -terse displays the object ID.</li> </ul> If you do not issue the report or terse parameter, this function returns the object ID and object name.
<b>ListObjectAttributes</b>	This function lists the managed object attributes.  This function lists data that can be used as parameters for the ListObjectsByAttribute function.	listobjectattributes [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> <li>-r or -report lists the name, data type, and value range for each managed object attribute.</li> <li>-t or -terse lists the name for each managed object attribute.</li> </ul> If you do not issue the report or terse parameter, this function returns the name and type of each attribute.



Table 9. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<b>ListObjectsByAttribute</b>	This function lists information about managed objects that meet the specified criteria.	listobjectsbyattributes [-r/-report/-t/-terse] {attribute=value}  where: <ul style="list-style-type: none"> <li>• -r or -report lists the object name, object ID, type, state, whether encryption is enabled, whether access is denied, operating system, IP address, and host name.</li> <li>• -t or -terse displays the object ID.</li> <li>• <i>attribute</i> is the name of the managed object attribute.</li> <li>• <i>value</i> is the value of the managed object attribute. (The attribute value is case-sensitive.)</li> </ul> <p>If you do not issue the report or terse parameter, this function returns the object name and object ID.  <b>Note:</b> You can determine valid managed-object attributes and the range of possible values by using the ListObjectsAttributes function.</p>
<b>AccessObjects</b>	This function requests access to managed systems.	accessobjects <i>userid password {systemID}</i>  where: <ul style="list-style-type: none"> <li>• <i>userid</i> is an IBM Director user ID that is authorized to access the managed system.</li> <li>• <i>password</i> is the password for the IBM Director user account that is authorized to access the managed system.</li> <li>• <i>systemID</i> is the unique system ID for the managed system.</li> </ul>
<b>PingObjects</b>	This function performs a presence check on the specified managed objects.	pingobjects { <i>systemID</i> }  where <i>systemID</i> is the unique object ID for the managed object.
<b>DeleteObjects</b>	This function deletes the managed object from the IBM Director Server environment. This is equivalent to deleting a managed object from IBM Director Console.	deleteobjects { <i>systemID</i> }  where <i>systemID</i> is the unique object ID for the managed object.
<b>ListGroups</b>	This function lists the IBM Director groups.	listgroups [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report lists the group name, group ID, type (static or dynamic), and criteria for each group.</li> <li>• -t or -terse lists the group ID for each group.</li> </ul> <p>If you do not issue the report or terse parameter, this function returns the group name and group ID for each group.</p>

Table 9. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<b>ListGroupAttributes</b>	<p>This function lists the attributes of the IBM Director groups.</p> <p>This function lists data that can be used as parameters for the ListGroupByAttribute function.</p>	<p>listgroupattributes [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> <li>• -r or -report lists the name, data type, and value range for each attribute.</li> <li>• -t or -terse lists the name for each attribute.</li> </ul> <p>If you do not issue the report or terse parameter, this function returns the type and name for each attribute.</p>
<b>ListGroupByAttribute</b>	<p>This function lists the IBM Director groups that meet the specified criteria.</p>	<p>listgroupsbyattribute [-r/-report/-t/-terse] {attribute=value}</p> <p>where:</p> <ul style="list-style-type: none"> <li>• -r or -report lists the name, ID, type, and criteria for each group that meets the conditions specified.</li> <li>• -t or -terse lists the ID for each group that meets the conditions specified.</li> <li>• <i>attribute</i> is the name of the attribute.</li> <li>• <i>value</i> is the value of the attribute.</li> </ul> <p>If you do not issue the report or terse parameter, this function returns the ID and name for each group that meets the specified conditions.</p> <p><b>Note:</b> You can determine valid group attributes and the range of possible values by using the ListGroupAttributes function.</p>
<b>ListGroupMembers</b>	<p>This function lists the members of specified groups.</p> <p><b>Note:</b> Managed objects are displayed only once, even if they are members of multiple specified groups.</p>	<p>listgroupmembers [-r/-report/-t/-terse] {groupID}</p> <p>where:</p> <ul style="list-style-type: none"> <li>• -r or -report lists the object name, object ID, type, state, whether encryption is enabled, whether access is denied, operating system, IP address, and host name for each member of the specified group.</li> <li>• -t or -terse lists the object ID of the each member of the specified group.</li> <li>• <i>groupID</i> is the group ID.</li> </ul> <p>If you do not issue the report or terse parameter, the function returns the object ID and object name for each member of the specified group.</p>
<b>ListDynamicGroupCriteria</b>	<p>This function lists the criteria available for creating dynamic groups. The criteria is based on database inventory.</p>	<p>listdynamicgroupcriteria [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> <li>• -r or -report lists the database, table, column, identifier, data type, whether multiple rows are supported per entity, and whether operators are supported. The database, table, and column name are language-translated strings.</li> <li>• -t or terse lists the identifier.</li> </ul> <p>If you do not issue the report or terse parameter, the function returns the identifier, database, table, and column.</p> <p>The identifiers are returned in the following format: <i>DatabaseToken.TableToken.ColumnToken.</i></p>

Table 9. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<b>ListInventoryValues</b>	This function lists the database inventory value for the specified identifiers.	<p>listinventoryvalues [-r/-report/-t/-terse] {<i>identifier</i>}</p> <p>where:</p> <ul style="list-style-type: none"> <li>• -r or -report lists the database, table, column, identifier, data type, whether multiple rows are supported per entity, whether operators are supported, and the inventory value for the identifier.</li> <li>• -t or -terse displays the identifier and inventory value.</li> <li>• <i>identifier</i> is the unique inventory identifier. It must be in the form <i>DatabaseToken.TableToken.ColumnToken</i></li> </ul> <p>If you do not issue the report or terse parameter, the function returns the identifier, database, table, column, and the inventory value.</p>
<b>CreateDynamicGroup</b>	This function creates a dynamic group.	<p>createdynamicgroup [-f] <i>groupname groupcriteria</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• -f forces an equality relationship with a value that cannot be verified with the current database.</li> <li>• <i>groupname</i> is the name of the dynamic group.</li> <li>• <i>groupcriteria</i> specifies the criteria for the dynamic group. <i>groupcriteria</i> must be one of the following forms: <ul style="list-style-type: none"> <li>– <i>identifier "symbol" value</i></li> <li>– {<i>identifier "symbol" value relationship identifier "symbol" value</i>}</li> </ul> </li> </ul> <p>where:</p> <ul style="list-style-type: none"> <li>– <i>identifier</i> is the unique inventory identifier. It must be in the following form: <i>DatabaseToken.TableToken.ColumnToken</i>.</li> <li>– <i>symbol</i> is one of the following symbols: =, !=, &lt;, &lt;=, &gt;, &gt;=.</li> <li>– <i>value</i> is an inventory value of the same type as the unique inventory identifier. It must be either an existing inventory data, or, if the optional -f command is issued, an unknown value can be used.</li> <li>– <i>relationship</i> is one of the following: <ul style="list-style-type: none"> <li>- AND (all true)</li> <li>- OR (any true)</li> <li>- ALL (all true for the same row)</li> <li>- EACH (at least one true)</li> </ul> </li> </ul>
<b>CreateStaticGroup</b>	This function creates a new static group.	<p>createstaticgroup <i>staticgroupname</i></p> <p>where <i>staticgroupname</i> is the name of the new static group.</p>
<b>AddToStaticGroup</b>	This function adds one or more managed systems to a static group.	<p>addstaticgroup <i>staticgroupID</i> {<i>systemID</i>}</p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>staticgroupID</i> is the object ID of the static group.</li> <li>• <i>systemID</i> is the object ID of the managed system.</li> </ul>

Table 9. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<b>RemoveFromStaticGroup</b>	This function removes one or more managed systems from a static group.	removefromstaticgroup <i>staticgroupID</i> { <i>systemID</i> }  where: <ul style="list-style-type: none"> <li>• <i>staticgroupID</i> is the object ID of the static group.</li> <li>• <i>systemID</i> is the object ID of the managed system.</li> </ul>
<b>DeleteGroups</b>	This function deletes one or more groups from the IBM Director environment.	deletegroups { <i>groupID</i> }  where <i>groupID</i> is the unique group ID.
<b>ListNoninteractiveTasks</b>	This function returns a list of noninteractive tasks. The list includes the job name, the task category (if known), and the job ID.	listnoninteractivetasks
<b>RunTask</b>	This function immediately runs a noninteractive task against one or more managed objects.	runtask <i>jobID</i> { <i>systemID</i> }  where: <ul style="list-style-type: none"> <li>• <i>jobID</i> is the job ID.</li> <li>• <i>systemID</i> is the unique object ID of the managed object.</li> </ul>

## Examples

The following table contains examples of invoking the server-management bundle.

<pre>dircmd -s IDWorld -u InfoDeveloper -p passw0rd server listobjects</pre> <p>In this example, an IBM Director super-user connects to the management server with the host name "IDWorld," using the user ID "InfoDeveloper" and the password "passw0rd." By invoking the ListObjects function of the server bundle, issuing this command returns a list of all managed objects.</p>
<pre>dircmd -s IDWorld -u InfoDeveloper -p passw0rd server listobjectsbyattribute -r AgentVer=4.10</pre> <p>In this example, the above user invokes the ListObjectsByAttribute function to generate an expanded list of all managed systems running IBM Director Agent 4.10.</p>

## Managed-system bundle

The following information explains how to use the managed-system bundle, which provides general access to managed systems. You can invoke the managed-system bundle to discover managed systems, list all managed systems, and add a managed system on the management server.

All managed-system functions must be preceded by the native command.

### Syntax

The following table contains information about the syntax for invoking the managed-system bundle:

Table 10. Managed-system bundle syntax

Function	What it does	Arguments
<b>Help</b>	This function lists an overview of the bundle usage.	help

Table 10. Managed-system bundle syntax (continued)

Function	What it does	Arguments
<b>List</b>	This function lists the function set for the bundle.	list
<b>StartDiscovery</b>	This function discovers managed systems.	startdiscovery
<b>ListSystems</b>	This function lists all managed systems.	listsystems [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report lists the system name, object ID (OID), unique ID (UID), MAC address, universal unique ID (UUID), IBM Director Agent version, state, whether access is denied, operating system information, IP address, and host name for each managed system.</li> <li>• -t or -terse displays the object ID of each managed system.</li> </ul> If you do not issue the report or terse parameter, the function returns the system name and object ID for each managed system.
<b>AddSystems</b>	This function creates a managed-system object on the management server. It is equivalent to right-clicking on the Group Contents pane of IBM Director Console, then clicking <b>New</b> → <b>IBM Director Systems</b> .	addsystem <i>systemname protocol netaddress</i>  where: <ul style="list-style-type: none"> <li>• <i>systemname</i> is the name of the new managed system.</li> <li>• <i>protocol</i> is the network protocol.</li> <li>• <i>netaddress</i> is a domain name system (DNS) resolvable host name or a TCP/IP address.</li> </ul>

## Examples

The following table contains examples of invoking the managed-system bundle.

<pre>dircmd -s IDWorld -u InfoDeveloper -p passw0rd native listsystems</pre> <p>In this example, an IBM Director super-user connects to the management server with the host name "IDWorld," using the user ID "InfoDeveloper" and the password "passw0rd." By invoking the ListSystems function of the managed-system bundle, issuing this command returns a list of all managed systems.</p>
<pre>dircmd -s IDWorld -u InfoDeveloper -p passw0rd native addsystems TechWriter2 TCP/IP 160.0.0.27</pre> <p>In this example, the above user invokes the AddSystems function to add a managed-system object to the IBM Director environment. The new managed system appears in IBM Director Console as "TechWriter2," is using TCP/IP as the network protocol, and has an IP address of 160.0.0.2.</p>

## Event-management bundle

The following information explains how to use the event-management bundle, which provides general access to events. You can invoke the event-management bundle to list event filters and event actions, list events, view the event log, list event action plans, and create and apply an event action plan.

All event-management functions must be preceded by the event command.

### Syntax

The following table contains information about the syntax for invoking the event-management bundle:

Table 11. Event-management bundle syntax

Function	What it does	Arguments
<b>Help</b>	This function lists an overview of the bundle usage.	help
<b>List</b>	This function lists the function set for the bundle.	list
<b>ListFilters</b>	This function lists all event filters.	listfilters [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report lists the names, keys, and read-only boolean status of the event filters.</li> <li>• -t or -terse displays the names of the event filters.</li> </ul> If you do not issue the report or terse parameter, the function returns the keys and names of the event filters.
<b>ListEventTypes</b>	This function lists the published event list.	listeventtypes
<b>ListEvents</b>	This function lists the contents of the event log.	listevents [-r/-report/-t/-terse] [-f <i>filtername</i> ] [-h <i>hours</i> ] [ { <i>systemID</i> } ]  where: <ul style="list-style-type: none"> <li>• -r or -report lists event type, event date and time, event system, severity, category, sending system, and associated text description.</li> <li>• -t or -terse lists the event and system.</li> <li>• <i>filtername</i> is a specific event filter.</li> <li>• <i>hours</i> specifies a time frame for the events.</li> <li>• <i>systemID</i> is the unique system ID for the managed object.</li> </ul> If you do not issue the report or terse parameter, the function returns the event type, event date/time, event system, severity, and category.  Issuing this function without arguments will generate a list of <i>all</i> managed system events that occurred during the preceding 24 hours.
<b>ListEventActions</b>	This function lists all event actions.	listeventactions [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report lists the name and key of the event actions. It also lists the boolean status of the read-only, runnable, and logging properties of the event actions.</li> <li>• -t or terse lists the event action names.</li> </ul> If you do not issue the report or terse parameter, the function returns the names and keys of the event actions.
<b>ListEventActionPlans</b>	This function lists all event action plans.	listeventactionplans [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report lists the name, key, and read-only value of the event action plan.</li> <li>• -t or -terse lists the name of the event action plan.</li> </ul> If you do not issue the report or terse parameter, the function returns the name and key of the event action plan.

Table 11. Event-management bundle syntax (continued)

Function	What it does	Arguments
<b>CreateEventActionPlan</b>	This function creates an event action plan.	createeventactionplan <i>planname</i> {-f <i>{filtername}</i> } <i>{actionname}</i> }  where: <ul style="list-style-type: none"> <li>• <i>planname</i> is the unique event action plan name. It is user-chosen.</li> <li>• <i>filtername</i> is an event filter.</li> <li>• <i>actionname</i> specifies the action plan name.</li> </ul>
<b>ApplyEventActionPlan</b>	This function applies an event action plan to a managed object or group.	applyeventactionplan <i>planname</i> [-s <i>{systemID}</i> ]   -g <i>{groupID}</i> ]  where: <ul style="list-style-type: none"> <li>• <i>planname</i> is an event action plan name.</li> <li>• <i>systemID</i> is an object ID</li> <li>• <i>groupID</i> is a group ID.</li> </ul>

## Examples

The following table contains examples of invoking the event-management bundle.

<pre>dircmd -s IDworld -u infodeveloper -p passw0rd event listevents -f "Fatal Events" -h 8</pre> <p>In this example, an IBM Director super-user connects to the management server with the host name "IDWorld," using the user ID "infodeveloper" and the password "passw0rd." By invoking the ListEvents function of the events-management bundle, issuing this command returns a list of all fatal events that occurred in the previous eight hours.</p>
<pre>dircmd -s IDworld -u infodeveloper -p passw0rd event listeventtypes   grep -i "security"</pre> <p>In this example, the above user invokes the ListEventTypes function in combination with a grep command to list all IBM Director event types associated with security.</p>

## Resource-monitor bundle

The following information explains how to use the resource-monitor bundle, which provides general access to resource monitors. You can invoke the resource-monitor bundle to list and apply resource-monitor threshold tasks.

All resource-monitor functions must be preceded by the monitor command.

### Syntax

The following table contains information about invoking the resource-monitor bundle.

Table 12. Resource-monitor bundle syntax

Function	What it does	Arguments
<b>Help</b>	This function lists an overview of the bundle usage.	help
<b>List</b>	This function lists the function set for the bundle.	list

Table 12. Resource-monitor bundle syntax (continued)

Function	What it does	Arguments
<b>ListThresholds</b>	This function lists all the resource-monitor threshold tasks.	listthresholds [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report displays the name and object ID of the threshold tasks in a tabular report form.</li> <li>• -t or -terse lists the object ID for the threshold tasks.</li> </ul> If you do not issue the report or terse parameter, the function returns the threshold name and task object ID.
<b>ApplyThreshold</b>	This function applies a resource-monitor threshold task to a managed system or group.	applythreshold <i>taskID</i> {-s <i>systemID</i>   -g <i>groupID</i> }  where: <ul style="list-style-type: none"> <li>• <i>taskID</i> is the object ID of the resource-monitor threshold task.</li> <li>• <i>systemID</i> is the object ID of the managed object.</li> <li>• <i>groupID</i> is object ID of the group.</li> </ul>

## Examples

The following table contains examples of invoking the resource-monitor bundle.

<pre>dircmd -s IDworld -u infodeveloper -p passwd monitor listthresholds -r</pre> <p>In this example, an IBM Director super-user connects to the management server with the host name "IDWorld," using the user ID "infodeveloper" and the password "passwd." By invoking the ListThresholds function, issuing this command lists all previously-created threshold tasks.</p>
<pre>dircmd -s IDworld -u infodeveloper -p passwd monitor applythreshold 196 -g 191</pre> <p>In this example, the above user invokes the ApplyThreshold function to apply the threshold task associated with OID 196 ("CPU utilization," in this case) to group 191 ("Systems with Windows 2000," in this case).</p>

## Process-monitor bundle

The following information explains how to use the process-monitor bundle, which provides general access to process monitors. You can invoke the process-monitor bundle to list process-monitor tasks, and create and apply a process-monitor task.

All process-monitor functions must be preceded by the procmon command.

### Syntax

The following table contains information about the syntax of the process-monitor bundle.

Table 13. Process-monitor bundle syntax

Function	What it does	Arguments
<b>Help</b>	This function lists an overview of the bundle usage.	help
<b>List</b>	This function lists the function set for the bundle.	list



Table 13. Process-monitor bundle syntax (continued)

Function	What it does	Arguments
<b>ListPMtasks</b>	This function lists all the process-monitor tasks.	listpmtasks [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report lists the name and object ID of the process-monitor task. It also lists every program in the process monitor and the boolean status of the following program attributes: start monitor, stop monitor, fail monitor, and fail timeout seconds.</li> <li>• -t or -terse lists the object ID of the process monitor task.</li> </ul> If you do not issue the report or terse parameter, the function returns the name and object ID of the process monitor task.
<b>CreatePMtask</b>	This function creates a process-monitor task for a program.	createpmtask { <i>programname</i> [+S][+E][+Fn] }  where: <ul style="list-style-type: none"> <li>• <i>programname</i> specifies the path and name of the application, for example, c:\windows\notepad.exe.</li> <li>• +S generates an event when the program begins.</li> <li>• +E generates an event when the program ends.</li> <li>• +Fn generates an event when the program does not start correctly or fails after <i>n</i> seconds.</li> </ul>
<b>ApplyPMtask</b>	This function applies a process-monitor task to a managed system.	applypmtask <i>taskId</i> { <i>systemID</i> }  where: <ul style="list-style-type: none"> <li>• <i>taskId</i> is the object ID of the process-monitor task.</li> <li>• <i>systemID</i> is the object ID for the managed system.</li> </ul>

## Examples

The following table contains examples of invoking the process-monitor bundle.

<pre>dircmd -s IDworld -u infodeveloper -p passwd procmon createPMtask "Notepad monitor" c:\winnt\notepad.exe+s+f5</pre> <p>In this example, an IBM Director super-user connects to the management server with the host name "IDWorld," using the user ID "infodeveloper" and the password "passwd." By invoking the CreatePMtask function, issuing this command creates a process-monitor task with the name "Notepad monitor" that generates an event if the program does not start properly or fails after 5 seconds.</p>
<pre>dircmd -s IDworld -u infodeveloper -p passwd procmon listPMtasks</pre> <p>In this example, the above user invokes the ListPMtasks function to lists all process-monitor tasks.</p>

## SNMP-device bundle

The following information explains how to use the SNMP-device bundle, which provides general access to SNMP devices. You can invoke the SNMP-device bundle to discover SNMP devices, list SNMP devices, create an SNMP device, perform a Get request, a Get Next request, a Set request, a Get Bulk request, or an Inform request against an SNMP device, send an SNMP trap to an SNMP device, and perform an SNMP walk on a branch of the MIB tree of an SNMP device.

All SNMP-device functions must be preceded by the snmp command.

## Syntax

The following table contains information about the syntax for invoking the SNMP-device bundle.

Table 14. SNMP-device bundle syntax

Function	What it does	Arguments
<b>Help</b>	This function lists an overview of the bundle usage.	help
<b>List</b>	This function lists the function set for the bundle.	list
<b>StartDiscovery</b>	This function discovers all SNMP devices.	startdiscovery
<b>ListSystems</b>	This function lists all SNMP devices.	listsystems [-r/-report/-t/-terse]  where: <ul style="list-style-type: none"> <li>• -r or -report lists the system name, object ID, state, IP address, host name, MAC address, MIB2 system name, MIB2 system contact, MIB2 system location, MIB2 system object ID, and MIB2 system uptime for each SNMP device.</li> <li>• -t or -terse displays the object ID of each SNMP device.</li> </ul> If you do not issue the report or terse parameter, the function returns the system name and object ID for each SNMP device.
<b>AddSystems</b>	This function creates an SNMP device on the management server.  It is equivalent to right-clicking on the Group Contents pane of IBM Director Console, then clicking <b>New → SNMP Devices</b> .	addsystem <i>IPaddress communityname seed</i>  where: <ul style="list-style-type: none"> <li>• <i>IPaddress</i> is the IP address of the SNMP device.</li> <li>• <i>communityname</i> is the community name of the SNMP device.</li> <li>• <i>seed</i> is one of the following:               <ul style="list-style-type: none"> <li>– true if you want the SNMP device to be a seed for SNMP discovery.</li> <li>– false if you do not want the SNMP device to be a seed for SNMP discovery.</li> </ul> </li> </ul>
<b>Get</b>	This function performs an SNMP Get request against the SNMP device.	get <i>version systemOID {objectIdentifier}</i>  where: <ul style="list-style-type: none"> <li>• <i>version</i> is the version of SNMP. Valid choices are either 1 or 2.</li> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.1.0 for sysDescr.</li> </ul>
<b>GetNext</b>	This function performs an SNMP Get Next request against the SNMP device.	getnext <i>versionsystemOID {objectIdentifier}</i>  where: <ul style="list-style-type: none"> <li>• <i>version</i> is the version of SNMP. Valid choices are either 1 or 2.</li> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.1.0 for sysDescr.</li> </ul>

Table 14. SNMP-device bundle syntax (continued)

Function	What it does	Arguments
<b>Set</b>	This function performs an SNMP Set request against the SNMP device.	<p>set <i>version systemOID {objectIdentifier type value}</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>version</i> is the version of SNMP. Valid choices are either 1 or 2.</li> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact.</li> <li>• <i>type</i> is the type of the object identifier. Valid choices are bits, counter, counter64, gauge, integer, ipaddress, nsapaddress, octets, oid, opaque, timeticks, and unsigned32.</li> <li>• <i>value</i> is the value to which you want to set the object identifier, for example, administrator.</li> </ul>
<b>GetBulk</b>	This function performs an SNMP Get Bulk request against the SNMP device.	<p>getbulk <i>max non-repeaters systemOID {objectIdentifier}</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>max</i> is the maximum number of repetitions.</li> <li>• <i>non-repeaters</i> is the number of non-repeaters.</li> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.1.0 for sysDescr.</li> </ul>
<b>Inform</b>	This function performs an SNMP Inform request against the SNMP device.	<p>inform <i>systemOID {objectIdentifier type value}</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact.</li> <li>• <i>type</i> is the type of the object identifier. Valid choices are bits, counter, counter64, gauge, integer, ipaddress, nsapaddress, octets, oid, opaque, timeticks, and unsigned32.</li> <li>• <i>value</i> is the value of the object identifier.</li> </ul>

Table 14. SNMP-device bundle syntax (continued)

Function	What it does	Arguments
<b>Trap</b>	This function sends an SNMPv1 trap to the SNMP device.	<p>trap 1 <i>systemOID uptime IPaddress type enterpriseOID {objectIdentifier type value}</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>uptime</i> is the system uptime of trap sender.</li> <li>• <i>IPaddress</i> is the IP address of the trap destination.</li> <li>• <i>type</i> is the type of the trap being sent. It is one of the following: <ul style="list-style-type: none"> <li>– 0 = coldStart</li> <li>– 1 = warmStart</li> <li>– 2 = linkDown</li> <li>– 3 = linkUp</li> <li>– 4 = authenticationFailure</li> <li>– 5 = egpNeighborLoss</li> <li>– 6 = <i>specificNumber</i>, where <i>specificNumber</i> is the specific number for the trap.</li> </ul> </li> <li>• <i>enterpriseOID</i> is the enterprise object ID of the trap.</li> <li>• <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact.</li> <li>• <i>type</i> is the type of the object identifier. Valid choices are bits, counter, counter64, gauge, integer, ipaddress, nsapaddress, octets, oid, opaque, timeticks, and unsigned32.</li> <li>• <i>value</i> is the value of the object identifier.</li> </ul>
<b>Trap</b>	This function sends an SNMPv2 trap to the SNMP device.	<p>trap 2 <i>systemOID {objectIdentifier type value}</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact.</li> <li>• <i>type</i> is the type of the object identifier. Valid choices are bits, counter, counter64, gauge, integer, ipaddress, nsapaddress, octets, oid, opaque, timeticks, and unsigned32.</li> <li>• <i>value</i> is the value of the object identifier.</li> </ul>
<b>Walk</b>	This function performs an SNMP walk on a branch of the MIB tree of the SNMP device.	<p>walk <i>version systemOID oid</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>version</i> is the version of SNMP. Valid choices are either 1 or 2.</li> <li>• <i>systemOID</i> is the managed object ID of the SNMP device.</li> <li>• <i>oid</i> is the object identifier of the branch, for example, 1.3.6.1.2.1.1 to walk through all of the items in the system subtree.</li> </ul>

---

## Chapter 6. Working with managed systems using Web-based Access (Windows only)

You can use Web-based Access to view managed system information, change alert standard format (ASF) alerts, change system settings and configurations, and more.

**Note:** If you use Web-based Access to view a managed system that is running Windows NT 4.0 and IBM Director Agent, version 3.1. or 3.1.1, see the *IBM Director 3.1 User's Guide*.

Web-based Access is useful in the following situations:

- You do not want to install IBM Director Console.
- You plan to manage only a few servers, desktop computers, or other devices.
- You want to remotely access managed systems when using a Web browser.
- You want to view the most up-to-date information about the assets, health, and operating-system state of a managed system.

If you installed Web-based Access when you installed IBM Director Agent, you can access the managed system by using the following Web browsers:

- Microsoft Internet Explorer, version 4.1 or later
- Netscape Navigator, version 4.x or 7.01

**Notes:**

1. Your browser must support Java<sup>®</sup> applets.
2. (Microsoft Internet Explorer and Windows XP only) You must install Service Pack 1 for Windows XP to run Java applets in Internet Explorer.

If the system from which you want to use Web-based Access is running Windows 2000 or Windows XP, you can use the Microsoft Management Console (MMC), version 1.1 or later.

**Note:** Systems using a Web browser or MMC to access a managed system require 64 MB of RAM to function properly.

Also, if IBM Director Agent is integrated by way of an upward integration module (UIM), you can use Web-based Access from the management console. For more information, see the *IBM Director 4.1 Upward Integration Module Guide*.

---

### Starting Web-based Access

You can start Web-based Access using either:

- A Web browser
- MMC

### Starting Web-based Access using a Web browser

Complete the following steps to start Web-based Access on a local or remote system using a Web browser:

1. Click **Start** → **Programs** → **IBM Director** → **IBM Director Agent Browser**. The default Web browser starts and opens at the following Web address for the local system:

`http://localhost:port_number`

where *port\_number* is the port number that is assigned for use by Web-based Access during IBM Director Agent installation. Port number 411 is the default for initial access and port number 423 is the default for secure access (<https://localhost:423/index.html>). If you chose different values during configuration you must use those values instead.

2. In the IBM Director Agent User ID and Password window, type your operating-system user ID and password.
3. (Optional) To view a remote system, type the following in the Web browser address field:

```
http://system:port_number
```

where:

- *system* is the TCP/IP address of the managed system or the system name of the managed system, as returned by Domain Name System (DNS).
- *port\_number* is the port number that is assigned for use by Web-based Access during IBM Director Agent installation. Port number 411 is the default for initial access and port number 423 is the default for secure access (<https://localhost:423/index.html>). If you chose different values during configuration you must use those values instead.

The Web browser redirects the Web address to a secure port. A security alert message might be displayed. This is normal when accessing a secure socket layer (SSL) Web site for the first time. IBM Director Agent uses SSL to encrypt the data stream between the Web-based Access system and the target managed system. This security precaution ensures that others cannot easily see important information such as user login identification and passwords.

4. (Optional) If you do not want to see the security alert message each time you start Web-based Access, install the certificate for the target managed system in the Web browser.
5. Click **OK** to accept the secure connection. A second security alert message might be displayed that warns the address was not validated by a trusted Certificate Authority. Web browsers typically use SSL to validate the identity of a Web site, but IBM Director Agent uses SSL to protect the password. You can ignore this security alert.
6. Click **Yes** to dismiss the security alert message.
7. In the IBM Director Agent User ID and Password window, type your operating-system user name and password associated with the targeted managed system.

If the managed system is accessible using domain accounts, you can type your user name using either of the following syntax:

- *domain\_account\_name\user\_name*
- *user\_name@domain\_account\_name*

where *domain\_account\_name* is the name of the domain and *user\_name* is your user name.

Your level of access to the managed system is determined by the group membership of the user account you use to login. If the user account is a member of the system's local Administrators group, you have full access by default. If the user account is a member of the system's local Users group, you have read access. Otherwise, access is denied. You can configure this access policy. See your system administrator for more information.

**Note:** (Windows XP only) The operating system is configured by default to deny network access to user accounts with blank passwords. You cannot access the managed system running Windows XP using such an account unless you change the security policy on the managed system. It is a best practice to leave the Microsoft default policy in place and establish secure passwords for accounts you wish to access remotely.

8. A message stating that the Web browser requires Java support might be displayed.
9. A message stating that the Web browser requires the Java Foundation Class/Swing library (JFC/Swing) might be displayed.

IBM provides the Java Foundation Class/Swing library (JFC/Swing) with IBM Director Agent. You must install JFC/Swing for your Web browser before you access IBM Director Agent data. The first time you use the Web browser for Web-based Access, a Web page is displayed. Complete the following steps to install JFC/Swing:

- a. Read and follow the instructions on the Web page. The File Download window opens.
- b. Select the **Open** check box.
- c. Click **OK**. The Save As window opens.
- d. Click **Save**. The JFC/Swing library is downloaded and installed. When the installation is complete, the Download window closes.
- e. (Internet Explorer only) Exit Internet Explorer; then, start Internet Explorer and start Web-based Access. If the JFC/Swing library was successfully installed, Web-based Access opens in the Web browser.

Depending on your user account system access, you gain read/write or read-only access to the IBM Director Agent function on the managed system. If you have read-only access, some text boxes are unavailable, **Apply** buttons are disabled, and some functions will notify you that you do not have sufficient privilege to access them.

## Starting Web-based Access using MMC

If IBM Director Agent and Windows 2000 or Windows XP is installed on the managed system, you can use MMC for Web-based Access. Complete the following steps to start Web-based Access using MMC:

1. Click **Start** → **Programs** → **IBM Director** → **IBM Director Agent MMC browser**.
2. In the Director Agent Systems pane, right-click a managed system and click **New** → **System**. A window opens.
3. Type a name for the managed system, the system name of the managed system, and its *port\_number* where *port\_number* is the port number that is assigned for use by Web-based Access during IBM Director Agent installation. Port number 411 is the default for initial access and port number 423 is the default for secure access (<https://localhost:423/index.html>). If you chose different values during configuration you must use those values instead.
4. In the IBM Director Agent User ID and Password window, type your operating-system user ID and password.

## Understanding the Web-based Access interface

When you have connected to a managed system, Web-based Access opens in your Web browser or MMC. Two panes are displayed.

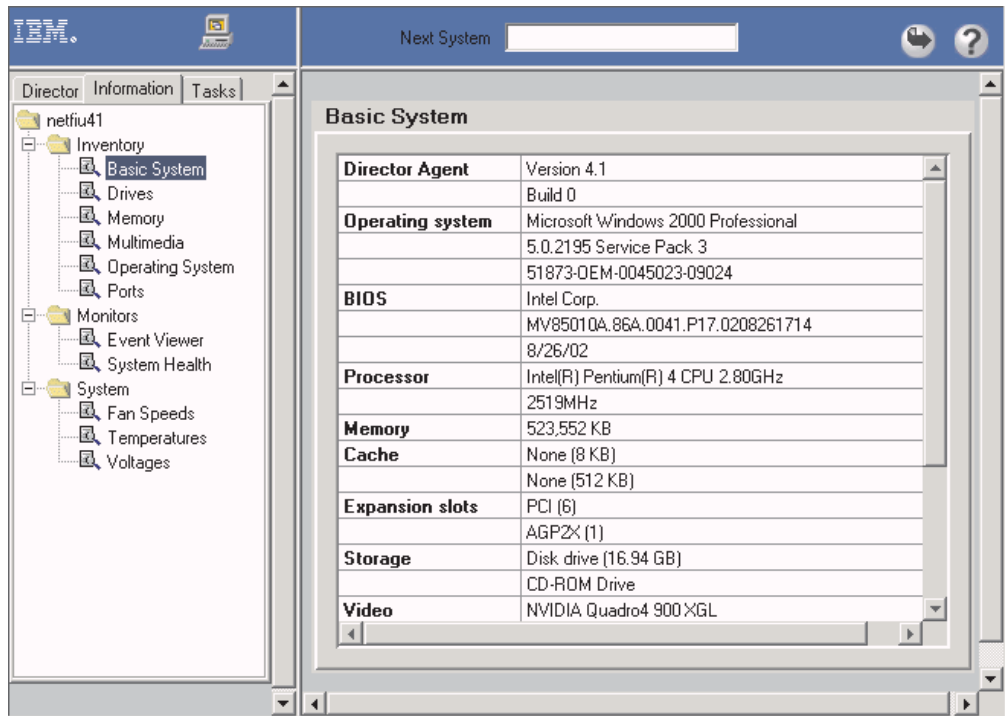


Figure 90. Web-based Access user interface

The left pane lists IBM Director Agent services that are available on the managed system. The pane can contain the following pages:

### Director

An expandable tree view of the Hardware Status service. This page is available only when you view a management server. See “Viewing Hardware Status using the Director page” on page 185.

### Information

An expandable tree view of IBM Director Agent services that lists hardware and software information from the managed system. See “Viewing managed-system information using the Information page” on page 186.

### Tasks

An expandable tree view of IBM Director Agent services that perform system-management and system-configuration tasks on the managed system. See “Working with managed systems using the Tasks page” on page 195.


When you click a service in the Director, Information, or Tasks page, the right pane lists the information or pages that are associated with the service.

**Note:** (Web browser only) You can use a Web browser window to access multiple managed systems. In the **Next System** field, type the TCP/IP address or the system name of another managed system; then, press Enter. The new managed system is displayed in the Web browser.



With IBM Director Agent, you can create comma-separated-value (CSV) data files from the hardware and software data that is collected by the Web-based Access services. You can import these CSV files into simple database and spreadsheet programs and create a centralized data repository.

Complete the following steps to create a CSV file:

1. Click a service in the left pane. Web-based Access loads the data.
2. Click  (Export). A File window opens.
3. Select the directory where you want to save the file.
4. Click **Save**.

The Web-based Access online help provides definitions for the information tables and services.

---

## Viewing Hardware Status using the Director page

The Hardware Status service is available from the Director page when you view a management server.



Figure 91. Director page in the left pane

The Hardware Status service is displayed in the right pane and identifies managed systems in the IBM Director Server environment.

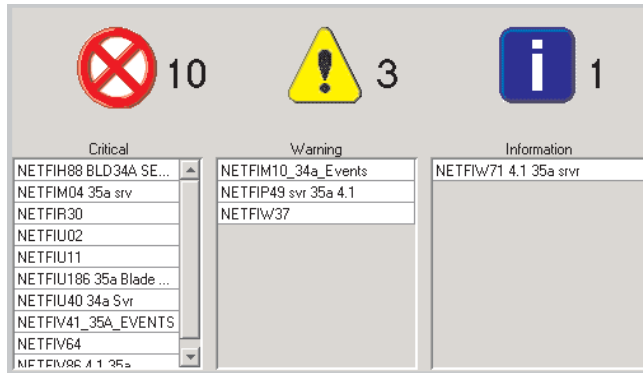


Figure 92. Hardware Status pane

Each managed system that requires attention is identified under the applicable status icon. The number of events is listed to the right of the displayed icon. The status icons categorize the hardware status into three groups:

- (Critical). A critical event requires immediate attention and action.
- (Warning). A warning event requires attention soon.
- (Information). An information event reports information but does not necessarily require attention.

When an event is recorded, a status icon is activated for the applicable severity, and the system is identified in a list under the applicable icon. When there are no events, the icon is outlined.

To access additional information, click an icon to see a list of managed systems being monitored, or double-click a listed system to receive data specific to that system.

Hardware Status monitors systems for changes in the following environments:

- Generic
- Network
- Storage
- Environmental
- Security
- Other

---

## Viewing managed-system information using the Information page

The information services gather hardware information and software information from a managed system. For most of the information services, you cannot change or configure the data that is displayed in the right pane. The operating-system service does provide some information that you can change. See “Operating System” on page 189.

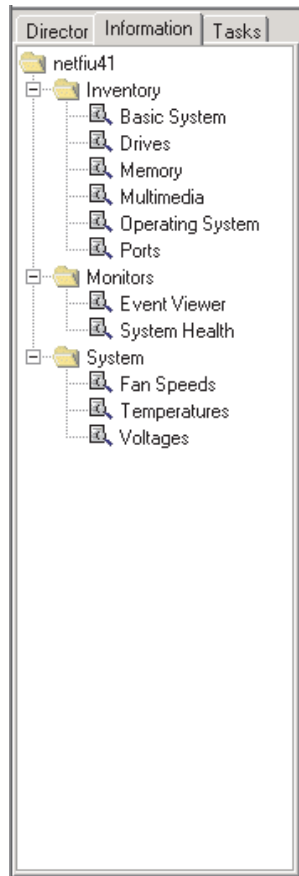


Figure 93. Information page in the left pane

The Information page might contain the following types of services:

- Inventory (see page 187)
- Monitor (see page 191)
- System (see page 194)

## Inventory services

Inventory services gather information about the operating system or physical devices that make up the managed system, such as disk drives, multimedia adapters, video adapters, and memory. The following inventory services are available:

- Basic System
- Drives
- FRU Numbers
- Memory
- Multimedia
- Operating System
- Ports

### Basic System

The Basic System service displays general information about the managed-system hardware and operating system.

**Note:** If a managed system does not have a particular item, the field that is associated with that item is not displayed in the right pane.

To start the Basic System service, click **Basic System** from the expanded tree in the left pane. The information is displayed in the right pane.

## Drives

The Drives service displays information about the physical and logical disk drives that are installed in the managed system. To start the Drives service, click **Drives** from the expanded tree in the left pane. The Drives notebook is displayed in the right pane and has a **Logical Drives** tab and a **Physical Drives** tab.

The Logical Drives page is displayed by default. This page contains information about the logical drives that are configured on the managed system. Click any row on the Logical Drives page for additional information. A pie chart shows used space and free space on the selected logical drive. Used space contains the applications and files that are on the disk, and free space is available for adding files or applications.

When you click the **Physical Drives** tab, information about the physical drives that are installed in the managed system is displayed. To view whether a physical hard disk has partitions, click any disk row. If the selected disk has partitions, information about the partitions is displayed in the **Partition information** section of the **Physical Drives** page. The partition information is displayed as a pie chart, showing the portion of the total physical disk that is used by each partition.

## FRU Numbers

The FRU Numbers service displays information about the field-replaceable unit (FRU) components installed on the managed system. The FRU information is specific to the model type of the system.

**Note:** FRU information is available for xSeries servers that currently are supported by IBM.

To start the FRU Numbers service, click **FRU** from the expanded tree in the left pane. The FRU numbers information for the following system components is displayed in the right pane:

- RAID drives and tapes
- CPUs (microprocessors)
- Dual inline memory modules (DIMMs)
- Keyboard
- System board
- CD-ROM drive
- Diskette drive
- Service processor
- Fans
- Backplanes
- (Only system with a Remote Supervisor Adapter) System board, power supplies, and PCI adapters. The availability of this information varies by the model type of the system.
- (Only systems with a ServeRAID-4x or later installed with ServeRAID firmware version 4.84 or later) RAID physical drives and trays.

**Note:** This item does not include tape drives.

The FRU Numbers service uses FRU data files from the IBM Support FTP site. For more information about these data files, see Appendix B, "Obtaining FRU data files using the GETFRU command", on page 215.

**Note:** 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. For example, if you have ServeRAID adapters, ServeRAID FRU data that is on the adapter is displayed.

## Memory

The Memory service gathers information about the physical memory that is installed in the managed system and provides information about memory upgrade options that are available for the managed system. To start the Memory service, click **Memory** from the expanded tree in the left pane. The Memory notebook is displayed in the right pane and contains the **Physical Memory** tab and **Upgrade Options** tab.

The Physical Memory page is displayed by default. This page contains information about the physical memory that is installed in the managed system.

### Notes:

1. On servers that support memory compression, the message Note: Memory compression is enabled is displayed in the right pane.
2. Information about total spare memory is displayed for some servers, such as the IBM xSeries 252 server.

When you click the **Upgrade Options** tab, information about (current) memory upgrade options for the managed system is displayed. If you want to install additional memory in the managed system, click the amount of memory that will be your new memory total in the **Show upgrade options for** list. Additional information is displayed on memory configuration.

### Notes:

1. All of these options might not be supported. For more information, see your server documentation.
2. The Upgrade Options page recommendations default to using the smallest DIMMs possible. For example, you have a system with four DIMM sockets that are currently filled with 128 MB DIMMs. If you ask for configuration of 2 GB total RAM, the recommendation will be to populate the four DIMM sockets with 512 MB DIMMs, even though two 1 GB DIMMs is a valid recommendation also.
3. The Upgrade Options page recommendations do not take into account requirements for memory that must be added in matching banks. For example, the recommendation might suggest adding 3 DIMMs of different size, but the managed system requires that pairs of equal size be added.

## Multimedia

The Multimedia service displays information about multimedia adapters that are installed in the managed system.

**Note:** If an audio or video adapter is not installed in the managed system or if information from the adapter is unavailable, the field that is associated with the missing data is not displayed.

To start the Multimedia service, click **Multimedia** from the expanded tree in the left pane. The information is displayed in the right pane.

## Operating System

The Operating System service displays information about the operating system that is running on the managed system. To start the Operating System service, click **Operating System** from the expanded tree in the left pane. The Operating System

notebook is displayed in the right pane and contains the **Operating System**, **Process**, **Environment**, **Drivers**, and **Services** tabs.

The **Operating System** page is displayed by default. This page contains information about the operating system installed on the managed system.

When you click the **Process** tab, information about the processes or tasks that are currently running on the managed system is displayed.

When you click the **Environment** tab, information about the environment variables that are used by the operating system running on the managed system is displayed.

When you click the **Drivers** tab, information about the device drivers that are used by the managed system is displayed. To start a device driver, select the device driver and click **Start**. To stop a device driver, select the device driver and click **Stop**. To change the start mode, click **Start Mode** and make a selection in the window that opens.

**Note:** You must have administrator privileges to start or stop a device driver or to update its start mode.

The following table shows details available on the **Drivers** page.

Item	Description
Name	The name of each device driver in the operating-system directory.
Start Mode	The start mode that is assigned to each device driver. Depending on which mode is selected, a device driver is incorporated or not incorporated into the operating environment. <b>Disabled</b> The device driver is not added to the operating environment. <b>Auto</b> The device driver is started automatically when the operating system is started. <b>Boot</b> The device driver is initialized during the operating-system startup (boot) sequence. <b>Manual</b> The device driver is started by the user. <b>System</b> The device driver is started by the lolnitSystem method.
State	The current run state of each device driver (Running or Stopped).
Command line	The complete path to the device driver, such as C:\System Root\System32\adapti.sys. To view the complete command line, move the horizontal scroll bar to the right.

When you click the **Services** tab, information about the current state and start mode of services that are installed on the managed system is displayed. The information and configuration available on this page are the same as provided on the Drivers page.

## Ports

The Ports service displays information about the input/output ports on the managed system. To start the Ports service, click **Ports** from the expanded tree in the left pane. The information is displayed in the right pane.

## Monitor services

The Monitor services use system-monitoring hardware and software that is included with IBM Director Agent to gather data about the current operational state of the managed system, such as temperature, battery time remaining, and contents of the Windows 2000 or Windows XP event log on the managed system. The following Monitor services are available:

- Event Viewer (see page 191)
- Battery (see page 192)
- System Health (see page 192)

### Event Viewer

The Event Viewer service displays the contents of the Windows event log. Applications, device drivers, operating systems, and IBM Director Agent record hardware events and software events in the Windows 2000 and Windows XP event logs. To start the Event Viewer service, click **Event Viewer** from the expanded tree in the left pane. The event-log contents are displayed in the right pane.

The event log can contain a large number of entries. The Event Viewer provides event-log categories and event types to filter the event-log entries that are displayed in the Event Viewer. The Event Viewer service displays the 30 most recent event-log entries that fulfill the event-log category and event-type criteria. Depending on the filter you select, fewer than 30 entries might be displayed.

To change the event-log category, click the category from the Log list that corresponds to the event-log entries you want to display. The following event-log categories are available:

#### Application

(Default) Displays the 30 most recent log entries that result from software issues or application issues, faults, and problems.

#### System

Displays the 30 most recent log entries that result from system issues or hardware issues, faults, and problems.

#### Security

Displays the 30 most recent log entries that result from security problems, such as invalid user ID or password entries and other attempted security violations.

To filter the event-log entries by event type, select the check boxes at the bottom of the Event Viewer window. The event type provides a general description of the severity of the event. The following event types are available:

#### Information

Displays rows of informational entries that are related to the event-log category that you selected (Application, System, or Security).

#### Warning

Displays rows of warning entries that are related to the event-log category that you selected.

**Error** Displays logs that result from security issues, such as password or user ID failures or other access problems, or attempted security violations. It also displays log errors for application and system.

#### Success Audit

Displays information about successful events.

## Failure Audit

Displays information about unsuccessful events.

Only event-log entries that correspond to selected check boxes are displayed in the Event Viewer. For example, if you want to view only entries that result from system errors, click **System** in the **Log** list; then, select the **Error** check box and leave the other check boxes cleared. The 30 most recent entries that fulfill these criteria are displayed.

If you select an event-type check box and no information is displayed, there are no event-log entries that correspond to the selected event type.

To display *all* the event-log entries that fulfill the event-type criteria, click **Load All Events**.

**Note:** The event log can contain thousands of entries. Clicking **Load All Events** can result in significant delays while the entries are loaded into the Event Viewer.

When an event log is very large, clicking **Load All Events** displays the following error message: Loading data... please wait. After 5 minutes, the loading stops, but only the 30 most recent event-log entries are displayed and Load All Events is disabled.

You can use the Event Viewer to display additional information about any event-log entry when you double-click the log entry, a window opens, containing additional information about the event.

## Battery

The Battery service displays information about battery power sources in mobile computers. To start the Battery service, click **Battery** from the expanded tree in the left pane. The information is displayed in the right pane.

## System Health

IBM Director Agent automatically monitors managed systems for changes in a variety of system-environment factors, including temperature and voltage. Each monitored value has a system-health normal range. If the monitored value stays within normal range, the assumption is that the system health is normal. However, if any of these monitored values falls outside of acceptable system-health parameters, IBM Director Agent can generate output automatically to alert the system administrator of this state change. To configure the output generated, you must use the Health service from the Tasks page. See "Health" on page 198 for more information.

IBM Director Agent can generate the following alert output:

- System Health service in Web-based Access
- Indication notification message windows
- Alert messages that are sent as SNMP traps
- Alert messages that are sent as System Management Server (SMS) status messages
- CIM events
- Alert messages that are sent as Tivoli Enterprise Console® events
- Alert messages that are sent as IBM Director Server events
- Windows event log events



You can use the System Health service to check the status of all health monitors that are supported by the managed system. To start the System Health service, click **System Health** from the expanded tree in the left pane. The information is displayed in the right pane.

System Health reports are gathered from a variety of system devices. One of these devices is the LM sensor, which performs environmental monitoring. The health reports that are available on a managed system are dependent on the availability of components that contribute to health reports. The following list shows some of the system-health event messages that can be generated and the circumstances that cause them:

**Chassis intrusion**

If the system chassis has been opened, a Critical system-health event is generated, regardless of the reason.

**Fan failure**

If the system cooling fan fails, a Critical system-health event is generated. This might be the only prediction of a temperature-related event.

**Memory PFA**

This is available on some servers. Indicates a Predictive Failure Analysis<sup>®</sup> (PFA) event from a memory DIMM.

**Processor PFA**

This is available on some servers. Indicates a Predictive Failure Analysis event from a microprocessor.

**LAN Leash**

LAN Leash detects if a managed system is disconnected from the LAN, even when the computer is off. A Critical system-health event is generated if a managed system is disconnected from the LAN.

**Low disk space**

If free disk space is low, a Warning or Critical system-health event is generated.

**Processor removed**

If the microprocessor is removed from the managed system, a Warning system-health event is generated.

**Temperature out of specification**

If the microprocessor temperature is out of the specified range, a Warning system-health event is generated.

**Voltage out of specification**

If there is a dramatic change in the voltage that is supplied to any part of the managed system or if the voltage is out of the specified range, a Warning or Critical system-health event is generated.

**Hard Disk Drive Predictive Failure Alert**

Predictive Failure Alert events are generated if operational thresholds on the hard disk drive are exceeded. This information can be generated only for SMART drives.

**Power Supply Failure**

If the system power supply fails, a Critical system-health event is generated.

**Redundant NIC**

(Windows 2000 and Windows XP only) If a system has multiple network

interface cards (NICs) configured for automatic failover and a failover or switchback event occurs, a Warning system-health event is generated.

**NIC Failure**

(Windows 2000 and Windows XP only) If a system NIC fails, a Critical system-health event is generated.

**NIC Offline**

(Windows 2000 and Windows XP only) If a system NIC is offline, a Warning system-health event is generated.

**NIC Online**

(Windows 2000 and Windows XP only) If a system NIC is online an Informational system-health event is generated.

## System services

On systems that have a service processor or the applicable sensors, the System service displays current information about the physical devices and their environmental status. If a server has more than one service processor, then only one of the processors provides information to the System service:

- If a server has an Advanced Systems Management (ASM) processor only (either on the system board or on an ASM PCI adapter), the ASM processor provides the information. If the server also has a Remote Supervisor Adapter, the ASM processor still provides the information.
- If a server has a Remote Supervisor Adapter only, the adapter provides the information.
- If a server has an integrated systems management processor (ISMP) only, the ISMP provides the information. If the server also has a Remote Supervisor Adapter, the adapter provides the information.

The following System services are available for any server that has the applicable sensors:

- Fan Speeds
- Temperatures
- Voltages

**Note:** The real-time sensor information displayed by these services corresponds to the fan failure, temperature out of specification, and voltage out of specification threshold status provided by the System Health service (see “System Health” on page 192 for more information).

The Mgmt Processor Vital Product Data (VPD) System service is available for any server that has an ISMP, ASM, ASM PCI adapter, Remote Supervisor Adapter, or Remote Supervisor Adapter II service processor.

The following System services are available for any server that has an ASM, ASM PCI adapter, Remote Supervisor Adapter, or Remote Supervisor Adapter II service processor:

- Mgmt Proc Event Log
- Power/Restart Activity
- Server Timeouts

**Note:** When installing IBM Director Agent, you must select the **Management Processor Agent** check box to use the Mgmt Proc Event Log, Mgmt

Processor VPD, Power/Restart Activity, and Server Timeouts services. You do not have to select the check box to use the Fan Speeds, Temperatures, and Voltages services.

### **Mgmt Proc Event Log**

The Mgmt Proc (Management Processor) Event Log service displays entries currently stored in the system-management event log which is associated with the service processor. These entries are stored in the nonvolatile random access memory (NVRAM) on the service processor. To start the Event Log service, click **Mgmt Proc Event Log** from the expanded tree in the left pane. The information is displayed in the right pane.

**Note:** All events are informational unless noted as an Error or Warning event.

### **Fan Speeds**

The Fan Speeds service displays information about fan speeds in the managed system. To start the Fan Speeds service, click **Fan Speeds** from the expanded tree in the left pane. The information is displayed in the right pane.

### **Power/Restart Activity**

The Power/Restart Activity service displays power and restart information for the managed system. To start the Power/Restart Activity service, click **Power/Restart Activity** from the expanded tree in the left pane. The information is displayed in the right pane.

### **Server Timeouts**

The Server Timeouts service displays the settings for the POST, loader, operating system, and power-off delay timeouts for the managed system. To start the Server Timeouts service, click **Server Timeouts** from the expanded tree in the left pane. The information is displayed in the right pane.

### **Temperatures**

The Temperatures service displays the current temperature readings for various hardware components and various thresholds configured for the managed system. You cannot alter these thresholds. All temperature readings are in degrees Celsius. To start the Temperatures service, click **Temperatures** from the expanded tree in the left pane. The information is displayed in the right pane.

### **Voltages**

The Voltages service displays the current voltage readings for the system board and voltage regulator modules (VRMs) and various thresholds configured for the managed system. You cannot alter these thresholds. Each voltage threshold is defined as a low-high value pair. To start the Voltages service, click **Voltages** from the expanded tree in the left pane. The information is displayed in the right pane.

### **Mgmt Processor Vital Product Data (VPD)**

The Mgmt (Management) Processor VPD service displays information about the firmware and device driver currently installed for the service processor. To start the Mgmt Processor VPD service, click **VPD Management Product Service** from the expanded tree in the left pane. The information is displayed in the right pane.

---

## **Working with managed systems using the Tasks page**

System administrators can use the services that are available on the Tasks page to manage the managed systems. Users with less than system-administrator authority can view the available pages, but only system administrators can change or update system configurations and use the available tools.

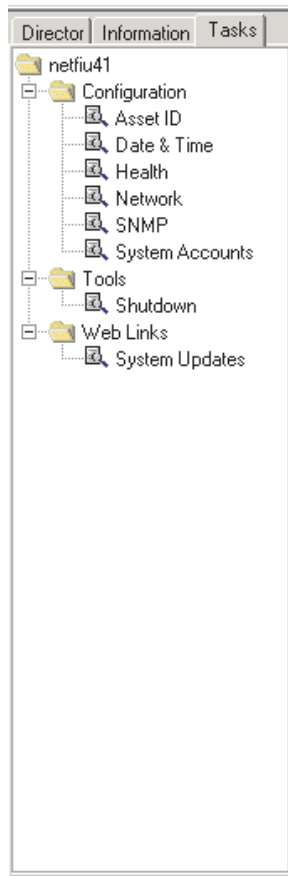


Figure 94. Task services in the left pane

Web-based Access displays only the tasks that are associated with the components that are installed on a managed system. For example, if SNMP is not installed on a managed system, the SNMP service (under **Configuration**) is not displayed for that system. Requirements and optional installations are noted under each task heading. Certain security levels are required so that users can view or edit selected services in Web-based Access. The following tasks are available:

- Configuration (see page 196)
- Tools (see page 200)
- Web Links (see page 200)

## Configuration

The Configuration task provides the following services:

- Asset ID
- Date and Time
- Health
- Network
- SNMP
- System accounts

### Asset ID

The Asset ID service displays hardware information for the managed system.

**Note:** Any information entered in Asset ID fields is stored as inventory data in the IBM Director database. You can make queries, take actions, create groups, and generate reports that are based on this inventory data.

To start the Asset ID service, click **Asset ID** from the expanded tree in the left pane. The Asset ID notebook is displayed in the right pane and contains the **Serialization, System, User, Lease, Asset, Personalization, and Warranty** tabs. The information on the User, Lease, Asset, Personalization, and Warranty pages is editable and can be whatever you type. The Asset ID service stores the information you type in the IBM Director database. If the managed system has EEPROM, the information is stored in the EEPROM, too. However, data space on the EEPROM is limited; therefore, the Asset ID service limits the amount of information you can type for managed systems with EEPROM. Not all IBM systems have EEPROM. Systems that do have EEPROM include, but are not limited to, NetVista and ThinkPad computers.

While the fields on these pages are labeled for specific information, you do not have to provide the specific information indicated by the label. The labels are suggestions for information you can provide.

The Serialization page is displayed by default. The information displayed on the page is reported from a number of sources, including but not limited to the system, the system board, hard disk drives, and the microprocessor. You cannot edit the information on this page.

When you click the **System** tab, the information includes the system name, message authentication code (MAC) address, login name ("" indicates the system is logged off), operating system, system globally unique identifier (GUID), and Remote Deployment Manager (RDM) profile. You can edit only the **RDM Profile** field.

When you click the **User** tab, information about the user of the managed system is displayed and you can edit this information.

When you click the **Lease** tab, the lease agreement information is displayed and you can edit this information. Use the Lease page to track lease contract information, including start date, end date, term (in months), amount, and lessor. You can use the specified end date as a source for an alert.

When you click the **Asset** tab, the inventory information about the managed system is displayed and you can edit this information. Use the Asset page to track asset information, including the purchase date, last inventoried (the date of the last physical inventory of the system), and asset number. Additionally, IBM Director automatically saves the date of the last inventory update for each managed system.

Click the **Personalization** tab. It is a free-form window where you can type information about your users or systems. Use the Personalization page to track any additional information about the managed system. Five fields and their labels are available for customizing. For example, you can customize a field to track the primary function of each managed system.

**Note:** The number of characters that you can type in these fields is limited and is affected by how many fields you choose to use. The Asset ID service provides a **Data space remaining** indicator along the bottom of the window. Use this indicator to determine how many characters you can still type. If a managed system has EEPROM, the available data space is significantly less than the data space for a managed system that does not have EEPROM.

You cannot enter as many characters for a managed system with EEPROM because space is limited on the EEPROM.

Click the **Warranty** tab. The information about the warranty on the managed system is displayed and you can edit this information. Use the Warranty page to track warranty data for this system, including duration (in months), cost, and end date. You can use the specified end date as a source for an alert. If these dates expire, you can choose to have these alerts sent to your management server. The alerts are displayed in the Other category of the Health services page.

### **Date and Time**

Use the Date and Time service to set the date and time that are displayed on the managed system. To start the Date and Time service, click **Date and Time** from the expanded tree in the left pane. Separate fields for the month, day, year, and local time are displayed in the right pane.

### **Health**

Use the Health service to set Warning and Critical threshold values for space remaining on the managed system hard disk drives and to enable and disable event bindings for various event consumers. You *cannot* edit temperature thresholds if the managed system has an ASM processor, an ASM PCI adapter, or a Remote Supervisor Adapter.

To start the Health configuration service, click **Health** from the expanded tree. The right pane is subdivided into two subpanes. The left subpane contains selectable items in a tree, and the right subpane contains descriptive text or health configuration controls for the item selected on the left. The tree is divided into two categories: Thresholds and Bindings.

You can specify a threshold of remaining hard disk drive space. Expand the disk drive tree and select the applicable drive letter. Specify the Warning and Critical thresholds (percentage-based or in MB) and click **Apply**.

Use bindings to enable or disable different severities of alerts from being sent to a variety of destinations, including event logs and IBM Director Server. You cannot select the severity of different alerts, but you can select which severities are sent. If you do not want Warning or Critical alerts to be sent, you can turn off the alerts.

### **Network**

The Network service provides information about your network. This service is useful for remote configuration. To start the Network service, click **Network** from the expanded tree in the left pane. The Network notebook is displayed in the right pane and contains the **IP Address**, **DNS**, **WINS**, **Domain/Workgroup**, and **Modem** tabs.

The **IP Address** page is displayed by default. The routing information for your network is displayed on the IP Address page.

When you click the **DNS** tab, the Domain Name System (DNS) page is displayed. DNS is the distributed database system that is used to map domain names to IP addresses.

When you click the **WINS** tab, the Windows Internet Naming Service (WINS) page is displayed. If you make changes to this page, you must click **Apply** to save the changes.

When you click the **Domain/Workgroup** tab, the information about the managed system and its associated domain or workgroup is displayed on the Domain/Workgroup page. If you make changes to this page, you must click **Apply** to save the changes.

When you click the **Modem** tab, the modem information is displayed.

## SNMP

The SNMP service provides the ability to work with community strings that are used in network communication and to set trap destination addresses.

**Note:** The SNMP task is displayed in the task list only if the SNMP service is installed on the operating system running on the managed system.

To start the SNMP service, click **SNMP** from the expanded tree in the left pane. The information is displayed in the right pane.

## System accounts

The System Accounts service provides remote administration of user security and group security within a Windows operating system. To start the System Account service, click **System Accounts** from the expanded tree in the left pane. The System Accounts notebook is displayed in the right pane and contains the **Users** and **Groups** tabs.

Click the **Users** tab to review and edit users. Administrators can click the **Groups** tab to review and edit members within the group.

The Users and Groups pages display a list of global users and groups, respectively. When you click an item in the list, the **Properties** and **Delete** buttons are enabled. Use the **Properties** button to edit or view user or group properties. If you make changes on these pages, you must click **Apply** to save the changes. If you click **Add**, the Add notebook is displayed in the right pane and contains the **General**, **Member Of**, **Profile**, and **Password** tabs.

The **General** page is displayed by default. Use this page to give system users the appropriate security levels and password options.

When you click the **Member Of** tab, the Member Of page displays a group membership list. Members are listed on the left pane, and nonmember groups are listed in the right pane. Clicking the **<** and **>** buttons will move user names to and from the **Member groups** and **Non-member groups** lists.

Click the **Profile** tab. Use the Profile page to configure user profiles. You must provide the following information on this page.

Item	Description
Path	The network path to the user's profile folder. Type a network path in the form <code>\\server_name\profile_folder_name\user_name</code> .
Logon script	A script assigned to a user account that runs each time the user logs on.

Click the **Password** tab. Use the Password page to type a new password or change an existing password. You must provide the following information on this page.

Item	Description
New password	The user's new password (32 character maximum, case sensitive).
Confirm password	This field must contain the same character string as the <b>New Password</b> field (32 character maximum, case sensitive).

## Tools

The Tools task provides the Shutdown service. You must have Administrator privileges to use this service.

### Shutdown

The Shutdown service provides the following options for shutting down a managed system:

#### Shutdown and Power Off

Shut down and turn off the computer.

**Note:** Shutdown and Power Off is available only on systems that support and have enabled Advanced Power Management.

#### Restart

Shut down and restart the computer without turning it off.

To start the Shutdown service, click **Shutdown** from the expanded tree in the left pane. The Shutdown options are displayed in the right pane.

## Web Links

The Web Links task provides the System Updates service.

### System Updates

The System Updates service connects to an IBM Web site that provides the latest device drivers and news about your selected managed system. This service works only if the system can access the Internet.

To start the System Updates service, click **System Updates** from the expanded tree in the left pane. The System Updates page is displayed in the right pane. A table reports machine information for the managed system, including model number, serial number, operating system, and version number. To access the latest device drivers, technical information, and news about the managed system, click **Drivers**.



## Chapter 7. Solving IBM Director problems

The following table lists some of the problem symptoms and suggested solutions for IBM Director 4.1.

Table 15. Solving IBM Director problems

Symptom	Suggested action
<b>Active PCI Manager</b>	
The Active PCI Manager appears to be available and included after upgrading to IBM Director 4.1, but might not be working.	To resolve this problem, use the following procedure: <ol style="list-style-type: none"> <li>1. From Add/Remove Programs, remove all previous versions of Active PCI Manager.</li> <li>2. Reinstall IBM Director 4.1, and be sure to select the Active PCI Manager option from the IBM Director Server Plus Pack.</li> </ol>
<b>Alert Standard Format (ASF)</b>	
ASF cannot be configured on an xSeries 345.	Complete the following steps to configure ASF on an xSeries 345: <ol style="list-style-type: none"> <li>1. Disable ASF from the IBM Director Agent Web-based Access or the management console.</li> <li>2. Disable the network interface card for the adapter.</li> </ol> ASF cannot be configured if the network interface card is disabled.
<b>Common Information Model (CIM)</b>	
When attempting to enumerate a system, large amounts of CIM data are returned causing errors in the CIM Browser.	Do not attempt to enumerate the instances of the <pre>root/cimv2:CIM_DirectoryContainsFile</pre> <pre>root/cimvw:Win32_Subdirectory</pre> class on Windows. Those CIM classes have instances for every file and directory on every disk in your server. If you attempt to enumerate these classes, your managed system or management server might run out of memory.
<b>Databases</b>	
The Microsoft Jet database is full.	Migrate to a larger database such as IBM DB2®, Oracle, or Microsoft SQL.
Errors occur 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.
The database application failed on a BladeCenter unit. If you change the database application after configuring a BladeCenter unit, inventory errors might occur.	To resolve this problem use one of the following two procedures: <ul style="list-style-type: none"> <li>• Use the TWGRESET command and change the database application before configuring the IBM Director database. Then, reconfigure the BladeCenter unit.</li> <li>• Uninstall IBM Director and delete any remaining files. Next, reinstall IBM Director and use a new database application. Then, reconfigure the BladeCenter unit.</li> </ul>
When using Telnet to access a Linux environment through a Windows operating system, and then running the cfgdb utility, messages overlay. This is a result of a small screen size.	To resolve this problem, use the following procedure: <ol style="list-style-type: none"> <li>1. Set the environmental variable term to vt100 before running the cfgdb utility.</li> <li>2. Maximize the Telnet window to its largest size possible.</li> </ol>
<b>Dialog boxes</b>	
Tables appear too small in a pane.	Change the table settings to enlarge the table in the pane. <b>Note:</b> Modified table settings are not saved.

Symptom	Suggested action
<b>Discovery</b>	
A BladeCenter discovery does not function properly when multiple network interface cards are enabled.	<p>To resolve this problem, try one of the following:</p> <ul style="list-style-type: none"> <li>You can change the network interface card that is attached to the BladeCenter unit network. You might have to search to find the working network interface card.</li> <li>Disable the network interface cards that are not connected to the management module and then perform the discovery. When the discovery is complete, enable the network interface cards. You will need to do this each time you perform a discovery.</li> </ul>
<b>Dynamic groups criteria</b>	
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 meet that criterion are returned.	<p>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,</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
<b>Encryption</b>	
Certain managed systems cannot be managed.	<ul style="list-style-type: none"> <li>If encryption keys or encryption algorithms are changed using the Encryption Administration window, some systems might not be able to be managed. When new keys or a new cipher algorithm are requested, a presence check is forced by IBM Director. The presence check might not be completed immediately. There might be some delay between the requested operation and the time the managed system receives the new key.</li> <li>If encryption is disabled on the management server, encrypted managed systems are no longer able to be managed. These systems will relock after a short period of time. Request a presence check to force the managed system to relock.</li> </ul>
<b>Event action plans</b>	
Group event action plans are not displayed.	<p>Verify that a managed system or group has an event action plan assigned to it:</p> <ol style="list-style-type: none"> <li>In IBM Director Console, click <b>Associations</b> → <b>Event Action Plans</b>.</li> <li>In the Groups pane, click <b>All Groups</b>.</li> <li>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.</li> </ol> <p>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.</p>

Symptom	Suggested action
<b>Event log message</b>	
An event ID 2003 warning message appears in the application event log.	<p>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:</p> <p>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.</p> <p>The functions in this library are not recognized as trusted. Microsoft previously identified that this is a problem in these products.</p>
<b>Field-replaceable unit</b>	
FRU information does not appear when inventory is collected.	Verify that the GETFRU command can reach the IBM Support FTP site through your firewall. For the GETFRU command to succeed, the managed system must have firewall access through a standard FTP port. For more information, see Appendix B, "Obtaining FRU data files using the GETFRU command", on page 215.
<b>Hard disk drives geometry reporting</b>	
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.	<p>The following hard disk drives are not supported by a Windows operating system:</p> <ul style="list-style-type: none"> <li>• Optical</li> <li>• Iomega</li> <li>• Jaz</li> </ul> <p>This is previously identified by Microsoft as a Windows Management Instrumentation (WMI) problem.</p>
<b>Hot plugs</b>	
When using the hot-plug feature the status of the slot does not update.	To update the status of the hot plug, the server must be restarted. This is a limitation of the CIM provider.
<b>IBM Director Agent</b>	
A managed system running an operating system cannot be accessed.	If the password encryption method is set to MD5 (message digest 5) when you install IBM Director Agent, salt values containing only two characters might be generated. IBM Director requires that the salt values be eight characters in length. Issue the passwd command to reset the password for the account that is used to access the managed system.
A problem occurs on a managed system running IBM Director Agent and NetWare 6.0 with Service Pack 2, and is using a Broadcom Gigabit Ethernet network interface card.	<p>Complete the following steps to resolve this problem:</p> <ol style="list-style-type: none"> <li>1. Open the AUTOEXEC.NCF file.</li> <li>2. Change CHECKSUM=OFF to the following: <pre>LOAD B57.LAN SLOT=10012 FRAME=ETHERNET_II NAME=B57_1_EII LOAD B57.LAN SLOT=10012 FRAME=ETHERNET_802.2 NAME=B57_1_E82</pre> </li> </ol>

Symptom	Suggested action
<b>IBM Director Console</b>	
Managed systems are unavailable on the management console.	<ul style="list-style-type: none"> <li>Verify that: <ul style="list-style-type: none"> <li>The system is turned on.</li> <li>IBM Director Agent is running.</li> <li>The network connection is reliable.</li> </ul> </li> <li>Check or modify the network timeout value. Click <b>Start</b> → <b>Programs</b> → <b>IBM Director</b> → <b>Network Configuration</b>.</li> <li>Check the network timeout value for the management server or the managed system. To change the network timeout value using: <ul style="list-style-type: none"> <li><b>Windows:</b> Go to twgipccf.exe and change the timeout value</li> <li><b>Linux:</b> 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.</li> </ul> </li> </ul> <p>If you are using UNIX or Linux and IBM Director Agent is installed in the default directory, you must restart IBM Director Agent. At a command prompt, type</p> <pre>/opt/IBM/director/bin/twgend -r</pre> <p>to stop and restart IBM Director Agent.</p>
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 occur during attempts to log on to the management server using IBM Director Console	<p>For Windows, verify that:</p> <ul style="list-style-type: none"> <li>The management server name, user ID, and password are valid.</li> <li>The management server is running.</li> <li>You have a connection from the management console to TCP port 2033 on the management server.</li> </ul> <p>For Linux: A green circle is not displayed in the task bar, but there is a Linux command-line command that you can use called twgstat. This reports the status of the management server. You can log on to the management console when twgstat returns a status of Active. The twgstat command returns the following statuses:</p> <ul style="list-style-type: none"> <li>Active: Server is fully active and ready for work.</li> <li>Starting: Server is starting but not yet ready for work.</li> <li>Ending: Server was requested to end but has not yet ended.</li> <li>Inactive: Server has ended or was never started.</li> <li>Error: Server has ended abnormally.</li> </ul>
A request for access fails, and the managed systems remain locked.	<ul style="list-style-type: none"> <li>Determine whether the managed system and management server accept encrypted communications only.</li> <li>Ensure that the server has encryption enabled through the Encryption Administration window.</li> <li>If the managed system has a UNIX or Linux operating system, ensure that the password encryption method is set to Message Digest 5 (MD5).</li> </ul>

Symptom	Suggested action
Through the use of imaging, a system was added and is displayed on the management console as a duplicate of a system that was previously added.	Verify that the Unique ID attribute is enabled.
<b>IBM Director Server</b>	
IBM Director Server is not starting on a Windows operating system.	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Verify that the IBM Director Server service ID password and user account are valid. You always must use the same administrator password and user account for IBM Director Server and the IBM Director Server service. Complete the following steps to change the user account or password for the service: <ol style="list-style-type: none"> <li>1. Click <b>Start</b> → <b>Programs</b> → <b>Administrative Tools</b>.</li> <li>2. Double-click <b>Services</b>.</li> <li>3. Right-click <b>IBM Director Server</b>.</li> <li>4. Select <b>Properties</b>. Click <b>Log On</b>.</li> <li>5. Select the <b>This account</b> check box, and modify and confirm the password.</li> <li>6. Click <b>OK</b>, and then restart the IBM Director Server service.</li> </ol> </li> </ul>
A problem occurs on servers running Microsoft Windows 2000 when the NetBIOS protocol is present and IBM Director is installed. Errors are generated until the event log is full.	To resolve this problem, uninstall and then reinstall the network interface card device driver.
After IBM Director Server is installed on a server running Microsoft Windows 2000 Server, an error is displayed in the event log when the server is restarted.	<p>The open procedure for service PerfDisk in the DLL "C:\WINNT\System32\perfdisk.dll" has taken longer than the established wait time to complete. There might be a problem with one of the following:</p> <ul style="list-style-type: none"> <li>• The extensible counter</li> <li>• The service from which the counter is collecting data</li> <li>• The system might have been busy when the call was attempted.</li> </ul> <p>To resolve this problem, use the REGEDIT command and modify the following key entry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance key "Open Timeout" Change the Decimal value to 30000. This gives the system enough time to complete the start up task before starting the PERF counters.</p>
<b>IBM ThinkPad</b>	
IBM Director Agent installation process is not completed on an IBM ThinkPad computer.	When you install IBM Director Agent on a ThinkPad computer, you must restart the computer twice to complete the installation. Otherwise, Windows Management Instrumentation (WMI) does not function properly.

Symptom	Suggested action
<b>Installation</b>	
When installing IBM Director Server, the following message is displayed: Error 1722. There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor.	A possible reason for this error is that the display for a system running IBM Director Server or IBM Director Console must support at least 256 colors. Increase the display color palette to more than 256 colors, uninstall the previous partial install and reinstall IBM Director Server.
<b>Java Runtime Environment (JRE) Exceptions</b>	
Intermittent JRE exceptions occur	Verify that you have sufficient 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 <i>IBM Director 4.1 Installation and Configuration Guide</i> .
<b>Mass Configuration</b>	
When using Mass Configuration to configure Asset ID, a problem can develop if the system being configured is low on data space.	When the size of the configuration is larger than that of the data space remaining, the configuration fails without any indication that this failure occurs. This is a limitation of the data save area. Ensure that for each byte of data you have the same amount of space in your data save area.
<b>Pre-Advanced Configuration and Power Interface (ACPI) servers (Netfinity 7000)</b>	
When <b>Shut Down</b> is selected from the <b>Start</b> menu, a power off message is displayed.	Shutdown might fail on a Netfinity 7000 server running Windows 2000. This does not power off the system automatically.
<b>SNMP devices</b>	
SNMP devices are not being discovered.	Verify that: <ul style="list-style-type: none"> <li>• 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.</li> <li>• The seed devices or other devices to be discovered are running an SNMP agent.</li> <li>• 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.ip.ipNetToMediaTable on seed devices.</li> <li>• The correct network masks have been configured for all managed systems that must be discovered.</li> <li>• 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 <b>Options</b> → <b>Discovery Preferences</b>. 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.</li> </ul>

Symptom	Suggested action
An attribute value for a MIB file cannot be changed.	Verify that: <ul style="list-style-type: none"> <li>• IBM Director is using a community name that allows write access to the MIB file that has a value that you want to change.</li> <li>• The MIB file is writable.</li> <li>• The MIB file has a value you can set to be displayed in the SNMP Browser.</li> <li>• The compiled MIB file is associated with the value to change.</li> </ul>
When a MIB file attribute value is set to a hexadecimal, octal, or binary value, the file fails.	Verify that all of the values have been converted and are being added in a decimal format.
<b>SNMP traps</b>	
Trap destinations are missing from the SNMP agent table. <b>Note:</b> 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).
<b>Security</b>	
<b>Load All Events</b> does not function.	When the security log gets very large (approximately 4000 records), clicking <b>Load All Events</b> produces the Loading data...please wait message. After approximately 5 minutes, the message stops, and only the 30 most recent events are displayed. The <b>Load All Events</b> button is not enabled.
<b>Software Distribution</b>	
The software-package creation fails.	Check the available disk space on the management console. Packages are created on the management console before being written to the target system. If disk space is insufficient on the management console, the package creation fails.
Remote Control fails when distributing software packages to managed systems that are behind a firewall.	Remote Control and Software Distribution both use session support to increase data transmission. Session support within TCP/IP causes data to flow through a nonreserved port that is different from the one that IBM Director typically uses for communication. Most firewalls do not allow the data to be transmitted through this other port. You can disable session support by creating an INI file on the managed system. In the IBM\Director\bin directory on the managed system, create a file named tcpip.ini that contains the following command line: <code>SESSION_SUPPORT=0</code>  If more than one TCP/IP option is selected in the Network Driver Configuration of the managed system, you must create an INI file for each entry. Name these files tcpip.ini, tcpip2.ini, tcpip3.ini, and so on. After creating the files, restart the managed system.
An error message is displayed 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 packages from the management server. The redirector cache can be maintained only through the File Distribution Server Manager interface. This is accessed by right-clicking the <b>Software Distribution</b> task. Errors occur if you manipulate the cache through any means other than IBM Director Console.

Symptom	Suggested action
Software 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.
Software-package installation failed, and the location of the package must be changed.	Reinstall IBM Director Agent, and specify a different drive and directory.
<b>Sun Java plug-ins</b>	
After you login to Microsoft Internet Explorer, a Java security warning is displayed.	If you are using Microsoft Internet Explorer with the Sun Java plug-in for Web-based Access, there are additional prompts that appear when you login to a managed system. After you login to Microsoft Internet Explorer, a Java Security Warning is displayed. Select <b>Grant this session</b> . The Java plug-in requires authentication information. Enter the same information that you used for the Microsoft Internet Explorer login.
<b>Time zone</b>	
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.
<b>Uninstalling IBM Director</b>	
The following message is displayed: Error 1306: Another application has exclusive access to the C:\Program Files\IBM\Director\log\esnt evt.dat	Shut down all other applications; then, click <b>Retry</b> . Cancel the uninstallation and restart the server. Then, start the uninstallation again.



Symptom	Suggested action
<b>Web-based Access</b>	
<p>Web-based Access is unavailable and an error message is displayed indicating that the page cannot be found.</p>	<p>If you install Web-based Access on a managed system that is running Apache Web Server, you must modify the Web-based Access configuration files. Web-based Access and Apache Web Server use the same default connector ports.</p> <ol style="list-style-type: none"> <li>1. Stop the IBM Director Agent Web Server service.</li> <li>2. Open the server.xml file. If you installed IBM Director in the default location, this file is located at c:\Program Files\IBM\Director\websrv\conf, where c is the hard disk drive where IBM Director is installed.</li> <li>3. Change the server port: Server port="8005"  You must specify a port that is not already in use by another application.</li> <li>4. Change the connector port: port="8009"  You must specify a port that is not already in use by another application.</li> <li>5. Save the modified server.xml file.</li> <li>6. Open the workers.properties file. If you installed IBM Director in the default location, this file is located at c:\Program Files\IBM\Director\websrv\conf, where c is the hard disk drive where IBM Director is installed.</li> <li>7. Change the connector port: port="8009"  You must specify a port that is not already in use by another application.</li> <li>8. Save the modified worker.properties file.</li> <li>9. Open the tomcat.conf file. If you installed IBM Director in the default location, this file is located at c:\Program Files\IBM\Director\websrv\conf, where c is the hard disk drive where IBM Director is installed.</li> <li>10. Change the connector port: port="8009"  You must specify a port that is not already in use by another application.</li> <li>11. Save the modified tomcat.conf file.</li> <li>12. Restart the IBM Director Agent Web Server service.</li> </ol>
<p>A system running Microsoft Windows XP that does not have Java installed displays a message that the Java Virtual Machine (JVM) is needed to view a managed system.</p>	<p>To resolve this problem, install Microsoft Windows XP Service Pack 1.</p>

Symptoms	Suggested actions
<b>Windows NT</b>	
<p>Printing problems occur when IBM Director 3.1 Agent is installed on managed systems that are using a Windows NT operating system.</p>	<p>Using a print server or printer with IBM Director 3.1 Agent installed and a Windows NT operating system might require a setup that specifically uses local queues. When the printer configuration of the management console is connected directly to a network print queue (if the printer is not associated with a port), you will probably encounter errors when printing from IBM Director Console. If printer errors are encountered, complete the following steps to set up a printer that uses a local printing queue:</p> <ol style="list-style-type: none"> <li>1. Set up a local device that points to the network printer.</li> <li>2. Map the local LPT device to the network printer and create a local print queue. From a command prompt type  <pre>NET USE LPT1: \\printer_server\printer/persistent:yes</pre> <p>Where printer_server is the network server and printer is the local printer.</p> </li> <li>3. Add the local printer.</li> <li>4. Specify the local device (LPT1), and configure the new printer.</li> </ol>

## Appendix A. Resource-monitor attributes

You can use the Resource Monitors 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 113.

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 109.

Table 16. Resource-monitor attributes

Attribute	Windows XP	Windows 2000	Linux	UNIX	NetWare
<b>CPU monitor</b>					
CPU utilization	X	X	X	X	X
CPU 'x' utilization (on SMP devices)	X	X			X
Process count	X	X	X	X	X
Thread count					X
<b>Disk monitor</b>					
<b>Notes:</b>					
1. The disk drive monitor attributes are repeated for each local nonremoveable logical drive found.					
2. (Linux and UNIX only) The list of file-system attributes is displayed first; then, the disk monitor attributes are displayed under each file system.					
3. (NetWare only) The disk volume monitor attributes are repeated for each volume detected.					
Disk 1 workload	X	X			
Drive C: % space used	X	X			
Drive C: Space remaining	X	X			
Drive C: Space used	X	X			
Blocks available			X	X	
Blocks used			X	X	

Table 16. Resource-monitor attributes (continued)

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

Table 16. Resource-monitor attributes (continued)

Attribute	Windows XP	Windows 2000	Linux	UNIX	NetWare
<b>File system monitor</b>					
<b>Note:</b> (UNIX only) The file system monitor attributes for specific directories are provided for typical UNIX directories. If one of these directories does not exist, the attribute is not displayed.					
/			X	X	
/bin			X	X	
/dev			X	X	
/etc			X	X	
/home			X	X	
/lib			X	X	
/lost+found			X	X	
/sbin			X	X	
/tmp			X	X	
/usr			X	X	
/var			X	X	
<b>List of directory contents</b>					
Directory attributes			X	X	
Directory exists			X	X	
Directory owner			X	X	
Directory size (bytes)			X	X	
Last modified			X	X	
Object type			X	X	
<b>Memory monitor</b>					
Locked memory	X	X			
Memory usage	X	X			
Available (bytes)			X	X	
Used (bytes)			X	X	
Cache blocks in use					X
Percent of cache in use					X
<b>TCP/IP monitor</b>					
Interface x - Broadcast packets received	X	X			
Interface x - Broadcast packets sent	X	X			
Interface x - Bytes received	X	X			
Interface x - Bytes sent	X	X			
Interface x - Unicast packets received	X	X			
Interface x - Unicast packets sent	X	X			
IP packets received	X	X			
IP packets received with errors	X	X			
IP packets sent	X	X			
TCP connections	X	X			
UDP datagrams received	X	X			

Table 16. Resource-monitor attributes (continued)

Attribute	Windows XP	Windows 2000	Linux	UNIX	NetWare
UDP datagrams sent	X	X			
<b>Process monitor</b>					
<b>Note:</b> 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	X	X	X
Maximum running at once	X	X	X	X	X
Maximum running yesterday	X	X	X	X	X
New executions counted	X	X	X	X	X
Times failed to start	X	X	X	X	X
Time started	X	X	X	X	X
Time stopped	X	X	X	X	X
Total execution time	X	X	X	X	X
Yesterday's execution time	X	X	X	X	X
Yesterday's new executions	X	X	X	X	X

---

## Appendix B. Obtaining FRU data files using the GETFRU command

You can obtain information about the field-replaceable unit (FRU) components installed on a managed system using the GETFRU command. The FRU information is specific to the model type of the system.

**Note:** FRU information is available for xSeries servers that currently are supported by IBM.

When you restart a managed system after installing IBM Director Agent, IBM Director uses the GETFRU command to make one attempt to copy the FRU data file from the IBM Support FTP site. The data file contains the FRU information for that managed system server model. For the copy to succeed, the managed system must have firewall access through a standard FTP port. By default, the GETFRU command attempts to reach `ftp://ftp.pc.ibm.com/pub/pccbbs/bp_server` on FTP port 21.

After the GETFRU command successfully copies the FRU data file to the managed system, GETFRU processes the FRU data file and stores the FRU information in the CIM server. Then, GETFRU deletes the FRU data file from the managed system.

If the managed system cannot access the IBM Support FTP site, you can copy the FRU files to your network from the IBM Support FTP site.

1. Access the IBM Support FTP site (`ftp.pc.ibm.com`) using the FTP protocol. This FTP site uses an anonymous login.
2. Change to the directory `/pub/pccbbs/bp_server`.
3. Perform a `get` to copy a FRU data file from the IBM Support FTP site to your network. To retrieve a FRU data file for a system, you must provide the applicable FRU data filename. These filenames use the following syntax:

*machine\_type\_number*ums.txt

where *machine\_type\_number* is the machine type number for your system. For example, if a server has a machine type number of 1234, the filename is `1234ums.txt`. You can use the Inventory task to determine the four-digit machine type number of your system.

**Note:** You can retrieve only one FRU data file at a time.

4. Copy the FRU data files to a server and directory on your network. This server is your internal FTP site repository for the FRU data files. Your FTP site must use an anonymous login.
5. Write a script that uses the GETFRU command to retrieve FRU data files from your FTP site. Use the GETFRU command which is in either of the following directories:

---

**For Windows**     `\IBM\Director\cimom\bin`

---

**For Linux**        `/IBM/director/CIMOM/bin`

---

To use the GETFRU command in your script, observe the applicable syntax:

---

**For Windows**     `getfru -s ftp_server_name -d directory_of_fru_files`

---

---

**For Linux**      `./getfru -s ftp_server_name -d directory_of_fru_files`

---

where:

- *ftp\_server\_name* is the FTP address of the network server to which you copied the FRU data files. If you do not specify a address, the command uses a default of ftp.pc.ibm.com.
  - *directory\_of\_fru\_files* is the directory that stores the FRU data files. If you do not specify a directory, the command uses a default of /pub/pccbbs/bp\_server.
6. Use the Process Management task to run the script to access the FRU data files located on your network. See “Process Management” on page 96 for more information.



---

## Appendix C. Terminology summary and abbreviation list

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

---

### IBM Director terminology summary

The following terminology is used in the IBM Director publications.

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

IBM Director software is made up of three main components:

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

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

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

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

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

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

---

### Abbreviation and acronym list

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

Table 17. Abbreviations and acronyms used in IBM Director

Abbreviation or acronym	Definition
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI adapter
BIOS	basic input/output system
CIM	Common Information Model
CIMOM	CIM Object Manager
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management
CSV	comma-separated value

Table 17. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
DES	data encryption standard
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DMI	Desktop Management Interface
DNS	Domain Name System
DSA	Digital Signature Algorithm
EEPROM	electrically erasable programmable read-only memory
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	file transfer protocol
GB	gigabyte
Gb	gigabit
GUI	graphical user interface
GUID	globally unique identifier
HTML	hypertext markup language
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPX	internetwork packet exchange
ISDN	integrated services digital network
ISMP	integrated system management processor
JVM	Java Virtual Machine
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JFC	Java Foundation Classes
JRE	Java Runtime Environment
KB	kilobyte
Kb	kilobit
Kpbs	kilobit per second
KVM	keyboard/video/mouse
LAN	local area network
LED	light-emitting diode
MAC	media access control
MB	megabyte
Mb	megabit
Mbps	megabits per second
MD5	message digest 5
MDAC	Microsoft Data Access Control

Table 17. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
MHz	megahertz
MIB	Management Information Base
MIF	Management Information Format
MMC	Microsoft Management Console
MPA	Management Processor Assistant
MSCS	Microsoft Cluster Server
MST	Microsoft software transformation
NIC	network interface card
NNTP	Network News Transfer Protocol
NVRAM	nonvolatile random access memory
ODBC	Open DataBase Connectivity
OID	object ID
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PFA	Predictive Failure Analysis
RAM	random access memory
RDM	Remote Deployment Manager
RPM	Red Hat Package Manager
SID	(1) security identifier (2) Oracle system identifier
SLP	service location protocol
SMBIOS	System Management BIOS
SMI	System Management Information
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SNMP	Simple Network Management Protocol
SNA	Systems Network Architecture
SPB	software package block
SQL	Structured Query Language
SSL	Secure Sockets Layer
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
UDP	User Datagram Protocol
UID	unique ID
UIM	upward integration module
UNC	universal naming convention
UUID	universal unique identifier

Table 17. Abbreviations and acronyms used in IBM Director (continued)

<b>Abbreviation or acronym</b>	<b>Definition</b>
VPD	vital product data
VRM	voltage regulator module
WAN	wide area network
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
XML	extensible markup language

---

## Appendix D. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM® products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation® system, and whom to call for service, if it is necessary.

---

### Before you call

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

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

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

---

### Using the documentation

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

---

### Getting help and information from the World Wide Web

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

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

---

## Software service and support

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

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

---

## Appendix E. 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

© COPYRIGHT INTERNATIONAL BUSINESS MACHINES CORPORATION, 2003.  
All rights reserved.

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:

Active PCI	Predictive Failure Analysis
Asset ID	Redbooks
BladeCenter	ServeRAID
DB2	ServerProven
e-business logo	SurePOS
@server	ThinkPad
IBM	Tivoli
IntelliStation	Tivoli Enterprise
Light Path Diagnostics	Tivoli Enterprise Console
Netfinity	TotalStorage
NetView	xSeries
NetVista	UpdateXpress
OS/2 WARP	Wake on LAN

Pentium is a trademark of Intel 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.



---

# Glossary

## A

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

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

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

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

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

**ASF.** See alert standard format.

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

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

**Advanced System Management (ASM) PCI adapter.** An IBM service processor. It is built into the system board of Netfinity 700 M10 and 8500R servers; it also was available as an option that could be installed in a server that contained an ASM processor. When an ASM PCI adapter is used in conjunction with an ASM processor, the ASM PCI adapter acts as an Ethernet gateway, while the ASM processor retains control of the server. When used as an ASM gateway, the ASM PCI adapter can communicate with other ASM PCI adapters and ASM processors only.

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

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

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

## B

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

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

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

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

configure new BladeCenter chassis when they are added to the IBM Director environment.

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

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

## C

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

**CIM.** See Common Information Model.

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

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

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

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

## D

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

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

**DES.** See data encryption standard.

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

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

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

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

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

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

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

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

**discovery.** The process by which IBM Director Server identifies and establishes connections with systems on which IBM Director Agent is installed. In a discovery

operation, the management server sends out a discovery request and waits for responses from managed systems. The managed systems wait for this request and respond to the management server.

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

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

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

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

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

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

**DMI.** See Desktop Management Interface.

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

**dynamic group.** See group, dynamic.

## E

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

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

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

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

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

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

**extension.** See IBM Director extension.

## F

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

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

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

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

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

**FRU.** See field-replaceable unit.

**FTMI.** See Fault Tolerant Management Interface.

## G

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

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

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

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

**GUID.** See Universal Unique Identifier.

## H

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

## I

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

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

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

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

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

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

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

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

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

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

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

**interprocess communication (IPC).** A system that lets threads and processes transfer data and messages among themselves; it is used to offer services to and receive services from other programs. Interprocess communication is used to transfer data and messages

between IBM Director Server and IBM Director Agent, as well as IBM Director Server and service processors. It is also called in-band communication

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

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

**IPC.** See interprocess communication.

**ISMP.** See integrated systems management processor.

## J

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

## K

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

**KVM.** See keyboard/video/mouse.

## L

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

## M

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

**managed device.** An SMNP device managed by IBM Director.

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

**managed object.** An item managed by IBM Director. Managed objects include managed systems, Windows NT clusters, BladeCenter chassis, management processors, SNMP devices, multi-node servers (complexes), system partitions, physical platforms, nodes, and remote I/O enclosures. In IBM Director

Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or complex, for example).

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

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

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

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

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

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

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

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

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

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

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

**Microsoft Cluster Browser task.** An IBM Director task that can be used to display the structure, nodes, and resources associated with a Microsoft Cluster

Server (MSCS) cluster; determine the status of a cluster resource, and view the associated properties of the cluster resources.

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

**MMC.** See Microsoft Management Console.

**MPA.** See Management Processor Assistant.

**multicast discovery.** See discovery, multicast.

## N

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

**notification.** See alert.

## O

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

## P

**PCI.** See Peripheral Component Interconnect.

**PCI-X.** See Peripheral Component Interconnect-Extended.

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

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

**PFA.** See Predictive Failure Analysis.

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

**plug in.** See IBM Director extension.

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

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

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

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

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

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

sends it back to the managed system. The managed system then uses the public key to verify the validity of the signature.

## R

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

**RDM.** See Remote Deployment Manager.

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

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

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

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

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

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

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

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

## S

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

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

**Server Plus Pack.** See IBM Director Server Plus Pack.

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

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

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

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

**SLP.** See service location protocol.

**SMBIOS.** See systems management BIOS.

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

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

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

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

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

**SNMP discovery.** See discovery, SNMP.

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

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

**SSL.** See secure sockets layer.

**static group.** See group, static.

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

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

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

**System Health Monitoring.** An IBM Director Agent feature that handles in-band communication and alert notification for managed systems running Windows. In

addition to providing active monitoring of critical system functions, it also facilitates upward integration.

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

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

## T

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

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

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

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

**TTL.** See time to live.

## U

**unicast discovery.** See discovery, unicast.

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

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

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

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



higher-level systems-management console, as well as collect IBM Director inventory data, and view IBM Director alerts.

**UUID.** See Universal Unique Identifier.

## V

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

**VPD.** See vital product data.

## W

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

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



---

# Index

## A

- Active PCI Manager 6
  - hardware, supported 7
  - operating systems, supported 7
  - overview 7
  - prerequisites 7
  - subtasks 7
- Active PCI Manager task 40
  - Fault Tolerant Management Interface (FTMI) 41
    - CIM queries 44
    - FTMI operations, performing 43
    - FTMI subtask, starting 41
  - Slot Manager 45
    - adapters, adding 52
    - event filtering 52
    - PCI performance, analyzing 50
    - Slot view 46
    - slots and buses, working with 49
    - starting 45
    - Table view 47
    - Tree view 47
- Agent 4
  - features 5
    - IBM Director Remote Control Agent 5
    - MPA Agent 5
    - ServeRAID Manager 5
    - SNMP Access and Trap Forwarding 6
    - System Health Monitoring 5
    - Web-based Access 5
    - Web-based Access help files 5
  - license 4
  - operating systems, supported 4
- alert notification
  - in-band 5
  - managed systems running Windows 6
  - SNMP traps 6
- alerts, understanding 20
- anonymous command execution
  - restricting 101
- APC PowerChute Extension for IBM Director 9
- Application Workload Management (Aurema) 9
- ASM PCI adapter 5
- ASM processor 5
- Asset ID
  - System tab 197
  - User tab 197
- Asset ID (Web-based Access)
  - Asset tab 197
  - Serialization tab 197
  - Warranty tab 198
- Asset ID task 53
- Asset tab 197
- associations
  - viewing 19
  - viewing event action plan 26

## B

- Basic System service 215
  - BladeCenter Assistant task 54
    - BladeCenter Configuration subtask 55
      - alert-forwarding profile, configuring 56
      - login profiles, creating and changing 56
      - network settings for the service processor, configuring 56
      - service processor data, viewing 56
      - service processor, restarting 56
    - BladeCenter Management subtask 57
      - blade server 58
      - blade server start (boot) options 59
      - blue indicator light, viewing 57
      - component data, viewing 57
      - environmental data, viewing 57
      - event log, viewing 57
      - hardware status summary, viewing 57
      - KVM assignment, viewing and changing 58
      - KVM policy, viewing and changing 58
      - Light Path Diagnostics, viewing 57
      - local power control, viewing and changing 59
      - power supply status, viewing 57
      - switch IP configuration, viewing and changing 59
      - switch settings, viewing and changing 59
      - switch vital product data, viewing 59
      - USB media assignment, viewing and changing 59
      - USB policy, viewing and changing 58
    - Deployment wizard 60
    - Switch Management LaunchPad subtask 60
  - bottlenecks
    - automatic notification of 63
    - identifying using Capacity Manager task 61
- ## C
- Capacity Manager 6
    - overview 7
  - Capacity Manager task 60
    - bottlenecks
      - creating an event filter for identifying 64
      - identifying 61
      - receiving automatic notification of 63
    - forecasting 69
      - performance forecast graph, viewing 70
    - monitors, viewing and activating 60
    - reports
      - generating 64
      - report definition, creating 65
      - report details, viewing 68
      - saving and printing 68
      - viewing previously generated 69
    - settings, changing 71
  - Category Editor 17
  - CIM Browser task 71

- CIM Browser task (*continued*)
  - CIM class instance
    - executing a method for 73
    - setting a property value for 72
  - shortcuts for classes and methods, creating 73
  - starting 71
  - viewing information in 72
- Closing an application (process) 97
- Cluster Systems Management 9
- command-line interface 165
- Communications Configuration subtask 90
- configuration tasks (Web-based Access)
  - Date and Time 198
  - Network 198
  - SNMP 199
- Configure Alert Standard Format task 74
- Console 4
  - alerts 20
  - associations, viewing 19
  - events 20
  - groups 13
  - license 4
  - managed objects 12
  - managed systems 12
  - physical platforms 13
  - requesting access to a managed system 11
  - starting tasks 12
  - supported operating systems 4
  - tasks 39
  - tasks and BladeCenter products 39
  - toolbar 12
  - understanding the interface 11
- Custom Package Editor 131
- customer support xv

## D

- Date and Time task (Web-based Access) 198
- Deployment wizard 60
- device services
  - starting and stopping 97
- DIRCMD 165
  - event
    - apply event action plan 175
    - create event action plan 175
    - list 174
    - list event action plans 174
    - list event actions 174
    - list events 174
    - list filters 174
    - list types 174
  - monitor
    - apply threshold 176
    - list 175
    - list thresholds 176
  - native
    - add systems 173
    - list 173
    - list systems 173
    - start discovery 173
  - options 166

- DIRCMD (*continued*)
  - procmon
    - apply PM task 177
    - create PM task 177
    - list 176
    - list PM tasks 177
  - server
    - access objects 169
    - add to static group 171
    - create dynamic group 171
    - create static group 171
    - delete groups 172
    - delete objects 169
    - discover all 168
    - list 168
    - list dynamic group criteria 170
    - list group attributes 170
    - list group by attribute 170
    - list group members 170
    - list groups 169
    - list inventory values 171
    - list noninteractive tasks 172
    - list object attributes 168
    - list objects 168
    - list objects by attribute 169
    - ping objects 169
    - remove from static group 172
    - run task 172
  - server command syntax 168
  - SNMP device
    - create 178
    - discover 178
    - Get Bulk request 179
    - Get Next request 178
    - Get request 178
    - Inform request 179
    - list all 178
    - list function set 178
    - perform an SNMP walk 180
    - send SNMPv1 trap 180
    - send SNMPv2 trap 180
    - Set request 179
  - syntax 165
- Director
  - database 3
  - environment (illustration) 2
  - extensions 9
    - APC PowerChute Extension for IBM Director 9
    - Application Workload Management (Aurema) 9
    - Cluster Systems Management 9
    - Electronic Service Agent 9
    - Real Time Diagnostics 9
    - Remote Deployment Manager 8
    - Software Distribution Premium Edition 8
  - hardware, supported 2
  - network protocols, supported 4
  - publications xiv
  - Redbooks xiv
  - Remote Control Agent 5
  - Server Plus Pack 6
  - software components (illustration) 3

- Director (*continued*)
  - systems running Agent 3.x, managing 6
  - terminology
    - extensions 6
    - managed system 1
    - management console 2
    - management server 1
    - SNMP device 1
  - upgrading from IBM Director 3.x 6
  - Web sites xv
- Director Agent, see Agent 1
- Director Console, see Console 1
- Director File Package wizard 133
- Director Server, see Server 1
- Director Update Assistant 123
- DMI Browser task 74
  - attribute value for a DMI group, setting 75
  - component information, viewing 75
  - shortcut, creating a group class 75
  - starting 75
- DNS tab 198
- Domain/Workgroup tab 199
- duplication event filter 22
- dynamic groups 14

## E

- eFixes xv
- Electronic Service Agent 9
- Encryption Administration 37
- event
  - apply event action plan (DIRCMD) 175
  - create event action plan (DIRCMD) 175
  - list (DIRCMD) 174
  - list event action plans (DIRCMD) 174
  - list event actions (DIRCMD) 174
  - list events (DIRCMD) 174
  - list filters (DIRCMD) 174
  - list types (DIRCMD) 174
- event action history 26
- Event Action Plan Builder 21, 154
- event action plans 20
  - associations, viewing 26
  - event actions
    - customizing 158
    - types of 161
  - event data substitution variables 162
- event filters
  - Category page 157
  - creating 155
  - Day/Time page 157
  - Event Type page 155
  - explanation of 154
  - Extended Attributes page 157
  - Sender Name page 157
  - structuring 153
  - System Variables page 157
- event type 23
- exporting 26
- grouping systems to effectively implement 152
- implementing 21

- event action plans (*continued*)
  - importing 27
  - modifying 158
  - planning and designing 151
  - restricting 26
  - structuring 152
- event actions
  - customizing 158
  - types of 161
- Event data substitution variables 162
- event filters
  - Category page 157
  - creating 155
  - Day/Time page 157
  - duplication 22, 155
  - exclusion 22, 155
  - explanation of 154
  - Extended Attributes page 157
  - Sender Name page 157
  - simple 22, 154
  - structuring 153
  - System Variables page 157
  - threshold 22, 155
- Event Log task 76
  - display options, viewing and changing 77
  - exporting events from 77
- event management 151
- event types 23
- events, understanding 20
- exclusion event filter 22
- execution history 100
- extended attributes 157
- extensions
  - definition 6

## F

- Fault Tolerant Management Interface 7
- Fault Tolerant Management Interface (FTMI), see Active PCI Manager task 41
- field-replaceable unit
  - troubleshooting 203
- File Transfer task 77
  - directories, synchronizing 79
  - drives, synchronizing 79
  - files
    - synchronizing 79
  - transferring between managed systems 79
  - starting 77
  - target system, changing 79
- file-distribution servers, viewing details about 137

## G

- groups
  - Category Editor 17
  - dynamic 14
  - exporting 18
  - importing 18
  - static 16
  - task-based 15

groups (*continued*)  
types of 13

## H

Hardware Status task 80  
help xv  
help files, Web-based Access 5

## I

IBM Active PCI Software for Microsoft Windows 7  
IBM Director Agent, see Agent 1  
IBM Director Console, see Console 1  
IBM Director Server, see Server 1  
IBM Director service account, see Director service account 1  
in-band communication 5  
InstallShield Package wizard 125  
inventory software dictionary 85  
Inventory task 82  
inventory data, viewing 83  
inventory queries  
creating custom 84  
editing custom 85  
exporting results to a file 85  
predefined 83  
inventory software dictionary 85  
adding an entry to 85  
matches 87  
software inventory, viewing 85  
IP Address tab 198  
ISMP 5

## L

license  
IBM Director Agent 4  
IBM Director Console 4  
IBM Director Server 3

## M

managed object  
understanding the concept of 12  
managed system  
definition 1  
understanding the concept of 12  
management console  
definition 2  
Management Processor Assistant (MPA) task 88  
Communications Configuration subtask 90  
Fill all function 89  
Management Processor Configuration subtask 91  
alert-forwarding profile, configuring 91  
dial-in login profiles, creating and changing 92  
modem settings, configuring 92  
network settings for the service processor,  
configuring 91  
service processor data, viewing 91

Management Processor Assistant (MPA) task  
(*continued*)  
Management Processor Configuration subtask  
(*continued*)  
service processor, restarting 91  
Server Management subtask 92  
blue light indicator, viewing 93  
component data, viewing 92  
environmental data, viewing 92  
event log, viewing 93  
hardware summary, viewing 93  
Light Path Diagnostics 93  
managed system, restarting 94  
power supply status, viewing 93  
servers, powering on and off 93  
start (boot) options, viewing and changing 94  
starting 88  
Management Processor Configuration subtask 91  
management server  
definition 1  
Memory service (Web-based Access)  
upgrade options 189  
Message Browser 36  
Microsoft Cluster Browser task 94  
starting 94  
Microsoft Management Console (MMC) 5  
Microsoft Windows Installer Package wizard 128  
monitor  
apply threshold (DIRCMD) 176  
list (DIRCMD) 175  
list thresholds (DIRCMD) 176  
Monitor services (Web-based Access)  
Event Viewer 191  
MPA Agent 5  
MPA task, see Management Processor Assistant (MPA)  
task 88

## N

native  
add systems (DIRCMD) 173  
list (DIRCMD) 173  
list systems (DIRCMD) 173  
start discovery (DIRCMD) 173  
Network  
DNS tab 198  
IP Address tab 198  
Network task (Web-based Access) 198

## P

physical platforms  
understanding the concept of 13  
Process Management task 96  
closing an application (process) 97  
device services, starting and stopping 97  
issuing a command on a managed system 100  
process monitors  
applying 98  
creating 98  
removing 99

- Process Management task *(continued)*
  - process monitors *(continued)*
    - viewing 99
  - process tasks
    - creating 100
    - running 100
  - processes, services, and device-services information
    - viewing and working with 96
  - restricting anonymous command execution 101
  - Windows services
    - starting, stopping, pausing, and resuming 97
- process monitors
  - applying 98
  - creating 98
  - removing 99
  - viewing 99
- process tasks
  - creating 100
  - running 100
- procmon
  - apply PM task (DIRCMD) 177
  - create PM task (DIRCMD) 177
  - list (DIRCMD) 176
  - list PM tasks (DIRCMD) 177
- publications xiv

## R

- Rack Manager 6
  - overview 8
- Rack Manager task 102
  - component association
    - canceling 104
    - starting 104
  - creating and configuring a rack 104
  - existing rack
    - adding components to 105
    - removing components from 105
  - starting 102
- Real Time Diagnostics 9
- Redbooks xiv
- Remote Control task 106
  - changing the refresh rate 107
  - remote-control session
    - playing a recorded 107
    - recording a 107
    - starting a 106
  - remote-control states
    - changing 107
  - restricting remote-control usage 107
  - sending key combinations 108
- Remote Deployment Manager 8
- Remote Session task 108
- Remote Supervisor Adapter 5
- Remote Supervisor Adapter II 5
- Resource Monitors task 109
  - resource monitors
    - attributes 211
    - exporting a resource-monitor recording 116
    - monitoring the same resource on multiple groups or managed systems 116

- Resource Monitors task *(continued)*
  - resource monitors *(continued)*
    - recording 113
    - status icons 113
    - viewing 109
    - viewing resource-monitor data on the ticker tape 117
  - resource-monitor recording
    - viewing a graph of 115
  - resource-monitor threshold
    - setting 110
    - viewing 113
  - threshold tasks, exporting and importing 116
- RPM Package wizard 130

## S

- Scheduler 27
  - Calendar pages, using 33
  - execution history logs, viewing 35
  - job information, viewing 34
  - job properties, viewing 35
  - scheduled job history information, viewing 35
  - scheduled jobs information, viewing 33
  - scheduling a task
    - directly 28
    - dragging a task onto a managed system 32
    - starting 28
- Serialization tab 197
- server
  - access objects (DIRCMD) 169
  - add to static group (DIRCMD) 171
  - create dynamic group (DIRCMD) 171
  - create static group (DIRCMD) 171
  - delete groups (DIRCMD) 172
  - delete objects (DIRCMD) 169
  - discover all (DIRCMD) 168
  - list (DIRCMD) 168
  - list dynamic group criteria (DIRCMD) 170
  - list group attributes (DIRCMD) 170
  - list group by attribute (DIRCMD) 170
  - list group members (DIRCMD) 170
  - list groups (DIRCMD) 169
  - list inventory values (DIRCMD) 171
  - list noninteractive tasks (DIRCMD) 172
  - list object attributes (DIRCMD) 168
  - list objects (DIRCMD) 168
  - list objects by attribute (DIRCMD) 169
  - ping objects (DIRCMD) 169
  - remove from static group (DIRCMD) 172
  - run task (DIRCMD) 172
- Server 3
  - license 3
  - supported operating systems 3
- server function 168
- Server Plus Pack 6
  - installation 7
  - purchasing 7
- server-management bundle 168
- ServeRAID Manager 5
- ServeRAID Manager task 117

- ServerProven Web site 2
  - Service Packs xv
  - service processors
    - alert notification (in-band) 5
    - in-band communication 5
    - management 5
  - setting 119
  - Shutdown task (Web-based Access) 200
  - simple event filter 22
  - Slot Manager 7
  - Slot Manager, see Active PCI Manager task 45
  - SNMP Browser task 120
    - attribute value
      - setting 121
  - SNMP device
    - create (DIRCMD) 178
    - definition 1
    - discover (DIRCMD) 178
    - Get Bulk request (DIRCMD) 179
    - Get Next request (DIRCMD) 178
    - Get request (DIRCMD) 178
    - Inform request (DIRCMD) 179
    - list all (DIRCMD) 178
    - list function set (DIRCMD) 178
    - perform an SNMP walk (DIRCMD) 180
    - send SNMPv1 trap (DIRCMD) 180
    - send SNMPv2 trap (DIRCMD) 180
    - Set request (DIRCMD) 179
  - SNMP devices 118
    - compiling a MIB file 120
    - creating 119
    - discovery parameters 119
  - SNMP task (Web-based Access) 199
  - Software Distribution Premium Edition
    - overview 8
  - Software Distribution task 121
    - file-distribution servers, viewing details about 137
    - Premium Edition 122
    - redirected distribution 122
    - software packages
      - Custom Package Editor, using to import and build 131
      - Director File Package wizard, using to import 133
      - Director Update Assistant, using to import and build 123
      - distributing 133
      - InstallShield Package wizard, using to import and build 125
      - Microsoft Windows Installer Package wizard, using to import and build 128
      - RPM Package wizard, using to import and build 130
      - viewing details about 137
      - working with 135
    - software-distribution server preferences, changing 136
    - software-package categories
      - creating 134
      - editing 135
    - Standard Edition 122
  - Software Distribution task (*continued*)
    - understanding software distribution 122
  - software packages
    - distributing 133
    - editing 135
    - exporting 136
    - restricting access to 136
    - viewing contents of 135
    - viewing creation and distribution status 136
    - viewing details about 137
    - viewing software-distribution history 136
  - Software Rejuvenation 6
    - overview 8
  - Software Rejuvenation task 138
    - keyboard shortcuts 146
    - Prediction Configuration wizard, starting 143
    - rejuvenation options, setting 143
    - rejuvenation schedule
      - deleting 142
      - editing 141
      - resource utilization, viewing 145
      - schedule filter, creating 142
      - scheduling a software rejuvenation 140
      - service rejuvenation, configuring 139
      - software-rejuvenation events, creating an event filter for 145
      - starting 139
  - solving IBM Director problems 201
  - static groups 16
  - support, customer xv
  - Switch Management LaunchPad subtask 60
  - System Accounts task 146
  - System Availability 7
    - overview 8
  - System Availability task 147
    - graph dates, changing 149
    - settings criteria, changing 149
    - starting 147
    - system-availability report, saving 150
  - System Health
    - LAN Leash 193
    - low disk space 193
    - processor removed 193
    - temperature out of specification 193
    - voltage out of specification 193
  - System Health Monitoring 5
  - System tab 197
  - System Updates 200
  - system variables 23
    - changing 25
    - viewing 25
- ## T
- Task Based Group Editor 15
  - tasks
    - Asset ID
      - System tab 197
  - tasks (Web-based Access)
    - Asset ID
      - Asset tab 197



tasks (Web-based Access) *(continued)*

Asset ID *(continued)*  
  Serialization tab 197  
  User tab 197  
  Warranty tab 198

Network  
  DNS tab 198  
  IP Address tab 198

  Shutdown task 200  
  System Update 200

tasks menu (Web-based Access)

  Web Links 200

terminology

  extensions 6  
  managed system 1  
  management console 2  
  management server 1  
  SNMP device 1

threshold event filter 22

tools (Web-based Access)

  Shutdown task 200

trademarks 224

troubleshooting 201

Web-based Access *(continued)*

  Ports service 190  
  Process page 190  
  Services page 190  
  starting using a Web browser 181  
  starting using MMC 183  
  System Health 192  
    LAN Leash 193  
    low disk space 193  
    processor removed 193  
    temperature out of specification 193  
    voltage out of specification 193

  Tasks menu 195

Web-based Access help files 5

WINS tab 198

## U

upward integration 1  
User Administration 36  
User tab 197

## V

viewing 93  
viewing and changing 59

## W

Warranty tab 198  
Web Links  
  System Updates 200  
Web Links (Web-based Access) 200  
Web site  
  IBM ServerProven 2  
Web-based Access 5, 181  
  Asset ID 196  
  Basic System service 187, 188  
  configuration tasks  
    Asset ID 196  
  DNS tab 198  
  Drives Service  
    physical drives 188, 189  
  Event Viewer 191  
  Information tab 186  
  Memory service 189  
  Monitor services 191  
  Multimedia service 189  
  Operating System service 189  
    Drivers tab 190  
    Process tab 190  
    Services tab 190  
  Physical Drives tab 188, 189







Part Number: 01R0538

Printed in U.S.A.

SC01-R053-80



(1P) P/N: 01R0538

