

IBM Director 4.20



Systems Management Guide

IBM Director 4.20



Systems Management Guide

Note: Before using this information and the product it supports, be sure to read the general information in Appendix D, "Notices," on page 367.



Third Edition (July 2004)

© Copyright International Business Machines Corporation 2004. All rights reserved.

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

Contents

Figures	ix
Tables	xiii
About this book	xv
How this book is organized	xv
Notices that are used in this book	xvi
IBM Director documentation	xvi
IBM Director resources on the World Wide Web	xvii

Part 1. IBM Director fundamentals 1

Chapter 1. Introducing IBM Director	3
IBM Director environment	3
IBM Director components	4
IBM Director Agent features	6
IBM Director extensions	7
Licensing	11
Upgrading from previous releases of IBM Director	11
Chapter 2. Operating systems supported by IBM Director and IBM Director tasks	13
Supported operating systems supported by IBM Director components	13
Operating systems supported by IBM Director tasks	15
IBM Director task support for BladeCenter products	29
Chapter 3. Understanding IBM Director Console	31
The IBM Director Console interface	31
Scheduler	40
Message Browser	48
System Status	48
User Administration	49
Encryption Administration	50
Mass Configuration	51
Chapter 4. Managing and monitoring systems with event action plans	55
How events work in the IBM Director environment	55
Planning and designing event action plan implementations	57
Building an event action plan	59
Working with existing event action plans	72

Part 2. IBM Director Console tasks 77

Chapter 5. Active PCI Manager	79
Fault Tolerant Management Interface (FTMI)	79
Slot Manager	83
Chapter 6. Asset ID	93
Chapter 7. BladeCenter Assistant	95
Starting the BladeCenter Configuration or BladeCenter Management subtask	95
BladeCenter Configuration subtask	97

BladeCenter Management subtask	106
Deployment wizard subtask	110
Switch Management launch pad subtask	126
Chapter 8. Capacity Manager	127
Viewing and activating monitors	127
Identifying bottlenecks	128
Receiving automatic notification of a bottleneck	129
Generating a report.	131
Viewing report details	137
Saving and printing a report.	137
Viewing previously generated reports	138
Predicting future performance	139
Viewing a performance forecast graph	139
Changing settings	140
Chapter 9. CIM Browser	143
Starting the CIM Browser task	143
Viewing information in the CIM Browser	144
Setting a property value for a CIM-class instance	144
Executing a method for a CIM-class instance	144
Creating shortcuts to classes and methods	145
Chapter 10. Configure Alert Standard Format	147
Configuring Alert Standard Format	147
Configuring Secure Power Management	147
Using Secure Remote Management.	151
Chapter 11. DMI Browser	153
Starting the DMI Browser task	153
Viewing component information in the DMI Browser	153
Setting an attribute value for a DMI group	154
Creating a group-class shortcut	154
Chapter 12. Event Log	155
Viewing and changing display options	155
Changing event log settings.	157
Exporting events from the event log.	158
Chapter 13. File Transfer	159
Starting the File Transfer task	159
Transferring files between managed systems	160
Synchronizing files, directories, or drives	160
Disabling TCP session support	161
Chapter 14. Hardware Status	163
Chapter 15. Inventory	167
Viewing inventory data	167
Exporting inventory-query results to a file.	170
Viewing and editing the inventory-software dictionary	170
Chapter 16. Management Processor Assistant	175
Starting the Management Processor Assistant task	175
Communications subtask.	177
Configuration subtask	179

Management subtask	189
Chapter 17. Microsoft Cluster Browser	193
Chapter 18. Network Configuration	195
Viewing and configuring IP addresses	195
Chapter 19. Process Management	197
Viewing and working with processes, services, and device-services information	197
Creating and applying a process monitor	200
Removing process monitors.	201
Viewing process monitors	201
Creating and running process tasks	201
Issuing a command on a managed system	203
Restricting anonymous command execution.	204
Chapter 20. Rack Manager	207
Starting the Rack Manager task	207
Starting a component association	208
Canceling a component association.	208
Creating and configuring a rack	209
Adding components to an existing rack	209
Removing a rack component	210
Chapter 21. Remote Control	211
Starting a remote-control session.	211
Changing remote-control states	212
Changing the refresh rate	212
Recording a remote-control session.	213
Playing a recorded remote-control session	213
Restricting remote-control usage	213
Sending key combinations	214
Transferring the clipboard	214
Chapter 22. Remote Session	215
Chapter 23. Resource Monitors	217
Viewing available resource monitors	217
Setting a resource-monitor threshold	217
Viewing all resource-monitor thresholds	220
Recording a resource monitor	220
Viewing a graph of a resource-monitor recording	221
Exporting a resource-monitor recording	222
Monitoring the same resource on multiple groups or managed systems	222
Exporting and importing threshold tasks	222
Viewing resource-monitor data on the ticker tape	223
Chapter 24. ServeRAID Manager	225
Starting the ServeRAID Manager task	225
Viewing system or device information	226
Viewing ServeRAID alerts	226
Locating defunct disk drives.	226
Chapter 25. SNMP Browser and SNMP devices	227
Setting discovery parameters	227
Creating a new SNMP device	228

Configuring SNMP trap forwarding	228
Using the SNMP Browser	229
Chapter 26. Software Distribution	233
Understanding software distribution	233
Importing software and building software packages	234
Importing a previously created software package using Director File Package wizard (Premium Edition only)	249
Distributing a software package	250
Creating and editing software-package categories	250
Working with software packages	252
Changing software-distribution server preferences	253
Viewing details about file-distribution servers and software packages	254
Chapter 27. Software Rejuvenation	257
Starting the Software Rejuvenation task	257
Configuring a service rejuvenation	258
Scheduling a software rejuvenation	259
Editing a rejuvenation schedule	261
Deleting a rejuvenation schedule	261
Creating a schedule filter.	261
Setting rejuvenation options for all managed systems	262
Predicting resource exhaustion	263
Viewing resource utilization	265
Creating an event filter for software-rejuvenation events	265
Using keyboard shortcuts	266
Chapter 28. System Accounts	267
Adding a group	267
Deleting a user	267
Editing group membership	268
Chapter 29. System Availability.	269
Starting the System Availability task.	269
Changing the graph dates	271
Changing the settings criteria	272
Saving the system-availability report	273

Part 3. IBM Director features for accessing IBM Director components 275

Chapter 30. Working with management servers using the command-line interface (DIRCMD)	277
Installing and accessing DIRCMD	277
DIRCMD syntax	277
Chapter 31. Working with managed systems using Web-based Access (Windows only)	305
Starting Web-based Access.	305
The Web-based Access interface.	308
Viewing hardware status	309
Viewing managed-system information	310
Working with managed systems	320

Part 4. Troubleshooting and maintenance 325

Chapter 32. Solving IBM Director problems	327
Installation, upgrades, and uninstallation	327
IBM Director Server.	329
IBM Director Console	333
IBM Director Agent	337
Managed systems running Windows	338
IBM Director tasks	339
Software Distribution	342
Web-based Access	344
Systems running double-byte character set languages	345
 Chapter 33. Updating IBM Director	 347
 Chapter 34. Getting help and technical assistance	 349
Before you call	349
Using the documentation.	349
Getting help and information from the World Wide Web	350
Software service and support	350

Part 5. Appendixes	351
 Appendix A. Resource-monitor attributes.	 353
 Appendix B. Obtaining FRU data files using the GETFRU command	 359
 Appendix C. Terminology summary and abbreviation list	 361
IBM Director terminology summary	361
Abbreviations	361
 Appendix D. Notices	 367
Edition notice	367
Trademarks.	368
 Glossary	 369
 Index	 379

Figures

1. Hardware in an IBM Director environment	4
2. Software in an IBM Director environment	5
3. IBM Director Console	31
4. IBM Director Console toolbar	32
5. IBM Director Console: Group Contents pane listing a selected group.	34
6. “Dynamic Group Editor” window	35
7. “Task Based Group Editor” window	36
8. “Static Group Editor” window	37
9. “Category Editor” window.	38
10. “Group Import” window	39
11. “Scheduler” window	41
12. “New Scheduled Job” window	42
13. “Repeat” window	43
14. “New Scheduled Job” window: Tasks page	43
15. “New Scheduled Job” window: Options page	44
16. “New Scheduled Job” window: Scheduling a task that is activated by dragging it onto a managed object	46
17. “Scheduler” window: Selecting a job type in the Jobs page	47
18. “Scheduler” window: Selecting a specific job execution in the Jobs page	47
19. System Status menu	49
20. “Encryption Administration” window	50
21. “Configure Alert Standard Format: Profile Builder” window.	51
22. “Configure Alert Standard Format: Profile Builder” window, displaying a new profile	52
23. “Status” window	53
24. “Status” window: Profile Status field	53
25. “Event Action Plan Builder” window	60
26. “Simple Event Filter Builder” window: Event Type page	63
27. “Customize Action” window: Customizing an action for a ticker-tape alert	67
28. “Event Action Plan Builder” window: Event action plan with an event filter and event action assigned to it	70
29. “Customize Action” window displaying example values	71
30. Prompt when modifying an existing event action plan	73
31. “Fault Tolerant Management Interface” window	80
32. “Slot Manager” window: Slot view page	84
33. “Slot Manager” window: Tree view page	85
34. “Slot Manager” window: Table view page	86
35. Examples of slot error status	87
36. “Asset ID” window	93
37. “Management Processor Assistant” window: BladeCenter Management subtask.	96
38. “Management Processor Assistant” window: IP properties page	100
39. “Management Processor Assistant” window: Hardware page	101
40. “Management Processor Assistant” window: DNS page	102
41. “Management Processor Assistant” window: Restart service processor page	103
42. “Management Processor Assistant” window: Login profiles pane	105
43. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window	112
44. BladeCenter Deployment wizard: “Login to the BladeCenter management module” window	113
45. BladeCenter Deployment wizard: “Change the user name and password for the management module” window.	114
46. BladeCenter Deployment wizard: “Configure the management module properties” window	115
47. BladeCenter Deployment wizard: “Configure the management module protocols” window	116
48. BladeCenter Deployment wizard: “Configure the IP addresses” window	117
49. BladeCenter Deployment wizard: “Change the user name and password for switch modules” window	118

50. BladeCenter Deployment wizard: “Configure the switch module” window	119
51. BladeCenter Deployment wizard: “Deploy operating systems on the blade servers” window	120
52. BladeCenter Deployment wizard: “Configure the deployment policies” window	121
53. BladeCenter Deployment wizard: “Setup summary” window	122
54. IBM Director Console Tasks pane: BladeCenter Deployment wizard profile	123
55. “Monitor Activator” window	128
56. “Simple Event Filter Builder” window	131
57. “Report Definitions” window: Report Parameters page	132
58. “New Time Interval” window	132
59. “Report Definitions” window: Method of Generating a Report page	133
60. “Report Definitions” window: Monitor Selection page	134
61. “Report Definitions” window: Threshold Settings page	134
62. “Report Viewer” window	135
63. “Report Viewer” window: Lower-right pane displaying a performance-forecast graph.	139
64. “Settings” window: Graph page	141
65. “Settings” window: Window page	141
66. “Settings” window: Monitors page	142
67. “CIM Browser” window	143
68. “Configure Alert Standard Format” window: General page	148
69. “Configure Alert Standard Format” window: Configuration page	149
70. “Configure Alert Standard Format” window: Remote Management page	149
71. Web-based Access, saving authentication keys	150
72. “Event Log” window displaying all events for all managed systems	155
73. “Set Time Range” window	156
74. “Set Log View Count” window	156
75. “Choose the Color for Critical” window	157
76. “Server Preferences” window: Event Management page	157
77. “File Transfer” window	159
78. IBM Director Console displaying hardware-status groups.	163
79. IBM Director Console, hardware-status icons located in the bottom-right portion	163
80. “Hardware Status” window showing all hardware-status events	164
81. “Hardware Status” window showing events for a single managed system.	164
82. “Inventory Query Browser” window	168
83. “Inventory Query Builder” window	169
84. “Inventory Software Dictionary Editor” window.	171
85. “Management Processor Assistant” window: Management subtask	176
86. “Management Processor Assistant” window: IP properties page	181
87. “Management Processor Assistant” window: Hardware page	182
88. “Management Processor Assistant” window: DNS page	183
89. “Management Processor Assistant” window: Restart service processor page	184
90. “Management Processor Assistant” window: Modem settings - Hardware pane	186
91. “Management Processor Assistant” window: Modem settings - Software pane	187
92. “Network Configuration” window: IP Address page	195
93. “Process Management” window	198
94. “Process Monitors” window	200
95. “Process Task” window	202
96. “Execute Command” window	203
97. “Rack Manager” window.	207
98. “Remote Control” window	212
99. “Remote Session” window for a managed system running Windows	215
100. “Resource Monitors” window for a managed device.	218
101. “System Threshold” window for setting numeric thresholds	218
102. “System Threshold” window for setting text-string thresholds	219
103. “Resource Monitors” window, clicking Record	221
104. “Resource Monitor Recording” window	221
105. “ServeRAID Manager” window	225

106. “ServeRAID Manager” window displaying a defunct disk drive	226
107. “Select MIB to Compile” window.	230
108. “SNMP Browser” window	230
109. “SNMP Browser” window with a device tree expanded	231
110. “Add Profile” window	232
111. “Software Distribution Manager” window (Standard Edition).	235
112. “Software Distribution Manager” window (Premium Edition).	235
113. Director Update Assistant wizard	236
114. “About InstallShield” window	237
115. InstallShield Package wizard	239
116. Microsoft Windows Installer Package wizard	240
117. RPM Package wizard.	241
118. AIX InstallIP Package wizard	242
119. OS/400 Restore Library Package wizard.	243
120. OS/400 Restore Library Package wizard: “Advanced Options” window.	243
121. OS/400 Restore Licensed Program Package wizard	244
122. OS/400 Restore Object Package wizard	245
123. Custom Package Editor: “Create Custom Package” window	246
124. Custom Package Editor: “Pre-Distribution” window	247
125. Custom Package Editor: “Post-Distribution” window.	247
126. Custom Package Editor: “File Permissions” window	248
127. Custom Package Editor: “Windows NT/2000/XP/2003 Configuration” window	248
128. Director File Package wizard	249
129. “New Package Category” window	251
130. “Server Preferences” window: Software Distribution page	253
131. “Distribution Preferences” window	254
132. “File Distribution Servers Manager” window	255
133. “Software Rejuvenation” window.	257
134. “Service Rejuvenation” Window	258
135. “Repeat Schedule - Server” window	259
136. “Repeat Schedule - Service” window	260
137. “Schedule Filter” window	262
138. “Rejuvenation Options” window	262
139. Prediction Configuration wizard: “Modify Configuration Forecasting Data” window	264
140. “System Accounts” window.	267
141. “System Availability” window	270
142. “System Downtime” window	271
143. “Customization of Graph Dates” window	271
144. “Settings” window	273
145. Web-based Access	308
146. Director page in the left pane	309
147. Hardware Status pane	310
148. Information page in the left pane	311
149. Task services in the left pane	320

Tables

1. IBM Director tasks and the supported operating-system tables	16
2. Supported operating systems for the Asset ID, CIM Browser, Configure Alert Standard Format, Configure SNMP Agent, DMI Browser, and Event Log tasks	17
3. Supported operating systems for hardware alerts and the File Transfer, Hardware Status, and Inventory tasks	18
4. Supported operating systems for the Management Processor Assistant, Microsoft Cluster Browser, and Network Configuration tasks	20
5. Supported operating systems for the Power Management task	22
6. Supported operating systems for the Process Management, Remote Control, Remote Session, and Resource Monitors tasks	24
7. Supported operating systems for the ServeRAID Manager, SNMP Browser, and System Accounts tasks	25
8. Supported operating systems for the Server Plus Pack tasks	26
9. Supported operating systems for IBM Director software-distribution features	28
10. IBM Director task support for BladeCenter products	29
11. Event filters	61
12. Event Filter Builder notebook pages	64
13. Event action types	66
14. Event data substitution variables	68
15. FTMI CIM queries	83
16. FTMI CIM events	83
17. Slot Manager adapter attributes	91
18. Data types the XML file can contain	125
19. Performance-analysis icon descriptions	136
20. Resource-monitor status icons	220
21. Resource monitors for resource-exhaustion prediction	263
22. DIRCMD management commands	278
23. DIRCMD options	278
24. DIRCMD exit codes	280
25. Server-management bundle syntax	281
26. Managed-system bundle syntax	291
27. Event-management bundle syntax	292
28. Resource-monitor bundle syntax	294
29. Process-monitor bundle syntax	295
30. SNMP-device bundle syntax	296
31. Management Processor Assistant bundle syntax	300
32. BladeCenter-configuration bundle syntax	302
33. BladeCenter-chassis bundle syntax	302
34. Chassis bundle syntax	303
35. Device driver details	314
36. Installation problems	327
37. Upgrade problems	328
38. Uninstallation problems	329
39. IBM Director Server problems	329
40. IBM Director Console problems	333
41. IBM Director Agent problems	337
42. Managed systems running Windows problems	338
43. IBM Director task problems	339
44. Software Distribution problems	342
45. Web-based Access problems	344
46. Systems running double-byte character set languages problems	345
47. Resource-monitor attributes	353
48. Abbreviations used in IBM Director	361

About this book

This book provides instructions for using IBM® Director 4.20 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 documentation also provides planning and implementation information for event management.

How this book is organized

Chapter 1, “Introducing IBM Director,” on page 3, contains an overview of IBM Director, including components, features, and extensions.

Chapter 2, “Operating systems supported by IBM Director and IBM Director tasks,” on page 13, contains information about what operating systems the IBM Director 4.20 components and tasks support.

Chapter 3, “Understanding IBM Director Console,” on page 31, details the basic functionality of IBM Director Console, including group creation and management, using managed objects, and scheduling systems-management tasks.

Chapter 4, “Managing and monitoring systems with event action plans,” on page 55, contains information about how IBM Director uses events for systems management. The chapter also provides details about planning, designing, and building event action plan implementations.

Chapter 5, “Active PCI Manager,” on page 79, through Chapter 29, “System Availability,” on page 269, describe the tasks that you can perform using IBM Director Console. Each chapter in this part discusses a different task, and the chapters are arranged alphabetically by the task name.

Chapter 30, “Working with management servers using the command-line interface (DIRCMD),” on page 277, describes the tasks that you can perform using the command-line interface to IBM Director Server.

Chapter 31, “Working with managed systems using Web-based Access (Windows only),” on page 305, contains information about using Web-based Access to view real-time asset and health information on a managed system.

Chapter 32, “Solving IBM Director problems,” on page 327, lists solutions to problems that you might encounter with IBM Director.

Chapter 33, “Updating IBM Director,” on page 347, provides information about updating this version of IBM Director.

Chapter 34, “Getting help and technical assistance,” on page 349, contains information about accessing IBM Support Web sites for help and technical assistance.

Appendix A, “Resource-monitor attributes,” on page 353, details the resource-monitor attributes available when using the Resource Monitor task.

Appendix B, “Obtaining FRU data files using the GETFRU command,” on page 359, details how to obtain the field-replaceable unit (FRU) data files using the GETFRU command on managed systems.

Appendix C, “Terminology summary and abbreviation list,” on page 361, contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director documentation.

Appendix D, “Notices,” on page 367, contains product notices and trademarks.

The glossary on page 369 provides definitions for terms used in IBM Director documentation.

Notices that are used in this book

This documentation 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 documentation

The following documents are available in Portable Document Format (PDF) from the IBM Director 4.20 Web site at

<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55606>:

- *IBM Director 4.20 Installation and Configuration Guide* Third Edition, July 2004 (dir4.20_docs_install.pdf)
- *IBM Director 4.20 Systems Management Guide* Third Edition, July 2004 (dir4.20_docs_sysmgt.pdf)
- *IBM Director 4.1 Events Reference* (dir41_events.pdf)
- *IBM Director 4.20 Upward Integration Modules Installation Guide* Second Edition, July 2004 (dir4.20_docs_uim.pdf)

Note: Check this Web site regularly for new or updated IBM Director documentation.

For planning purposes, the following IBM @server[®] and xSeries[®] documents might be of interest:

- *IBM @server BladeCenter Type 8677 Planning and Installation Guide*
- *Remote Supervisor Adapter, User's Guide*

- *Remote Supervisor Adapter, Installation Guide*
- *Remote Supervisor Adapter II, User's Guide*
- *Remote Supervisor Adapter II, Installation Guide*
- *IBM Management Processor Command-Line Interface Version 2.0 User's Guide*

You can obtain these documents from the IBM Support Web site at <http://www.ibm.com/pc/support/>.

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

- *Creating a Report of the Tables in the IBM Director 4.1 Database (TIPS0185)*
- *IBM Director Security (REDP-0417-00)*
- *IBM @server BladeCenter Systems Management with IBM Director V4.1 and Remote Deployment Manager V4.1 (REDP-3776-00)*
- *Implementing Systems Management Solutions using IBM Director (SG24-6188)*
- *Integrating IBM Director with Enterprise Management Solutions (SG24-5388)*
- *Managing IBM TotalStorage NAS with IBM Director (SG24-6830)*
- *Monitoring Redundant Uninterruptible Power Supplies Using IBM Director (REDP-3827-00)*

You can download these documents from the IBM Redbooks Web site at <http://www.ibm.com/redbooks/>. You also might want to search this Web site for documents that focus on specific IBM hardware; such documents often contain systems-management material.

Note: 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 Director 4.20

<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55606>

You can download the following IBM Director 4.20 code and information from this Web page:

- CD image
- Documentation
- IBM LM78 and system management bus (SMBus) device drivers for Linux®
- Readme files
- Extensible Markup Language (XML) files for use with the Software Distribution task

Check this Web page regularly for updated readme files and documentation.

IBM Director Agent page

http://www.ibm.com/servers/eserver/xseries/systems_management/sys_migration/ibmdiragent.html

You can download the IBM Director Hardware and Software Compatibility document from this Web page. This document lists supported @server and xSeries systems, as well as all supported operating systems. It is updated every 6 to 8 weeks.

IBM @server Information Center

<http://www.ibm.com/servers/library/infocenter>

This Web page provides information about the IBM Virtualization Engine™ and IBM Director Multiplatform.

IBM ServerProven page

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

The ServerProven® Web page provides information about xSeries, BladeCenter™, and IntelliStation® hardware compatibility with IBM Director.

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**.

IBM Systems Management Software: Download/Electronic Support page

http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html

Use this Web page to download IBM systems-management software, including IBM Director. Check this Web page regularly for new IBM Director releases and updates.

IBM xSeries Systems Management page

http://www.ibm.com/pc/ww/eserver/xseries/systems_management/index.html

This Web page presents an overview of IBM systems management and IBM Director. It also contains links to Web pages for IBM Director extensions including Remote Deployment Manager, Scalable Systems Manager, Server Plus Pack, and Software Distribution (Premium Edition).

Part 1. IBM Director fundamentals

Chapter 1. Introducing IBM Director	3
Chapter 2. Operating systems supported by IBM Director and IBM Director tasks.....	13
Chapter 3. Understanding IBM Director Console.....	31
Chapter 4. Managing and monitoring systems with event action plans	55

Chapter 1. Introducing IBM Director

IBM Director is a comprehensive systems-management solution. Based on industry standards, it can be used with most Intel[®]-microprocessor-based systems and certain IBM @server iSeries[™] and pSeries[®] servers.

A powerful suite of tools and utilities, IBM Director automates many of the processes that are 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[®] software), Computer Associates, Hewlett-Packard, Microsoft[®], NetIQ, and BMC Software.

Note: There are two versions of IBM Director: IBM Director and IBM Director Multiplatform. They are based on the same code and software components (IBM Director Server, IBM Director Agent, and IBM Director Console), but the two versions are delivered differently. IBM Director comes with IBM xSeries servers and @server BladeCenter products. It also can be purchased for use on non-IBM systems. IBM Director Multiplatform is a system service that can be installed through IBM Virtualization Engine on iSeries, pSeries, and xSeries servers.

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 5000 systems.

An IBM Director environment contains the following groups of hardware:

- 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 Simple Network Management Protocol (SNMP) agents installed or embedded. Such devices are called *SNMP devices*.

Figure 1 shows the hardware in an IBM Director environment.

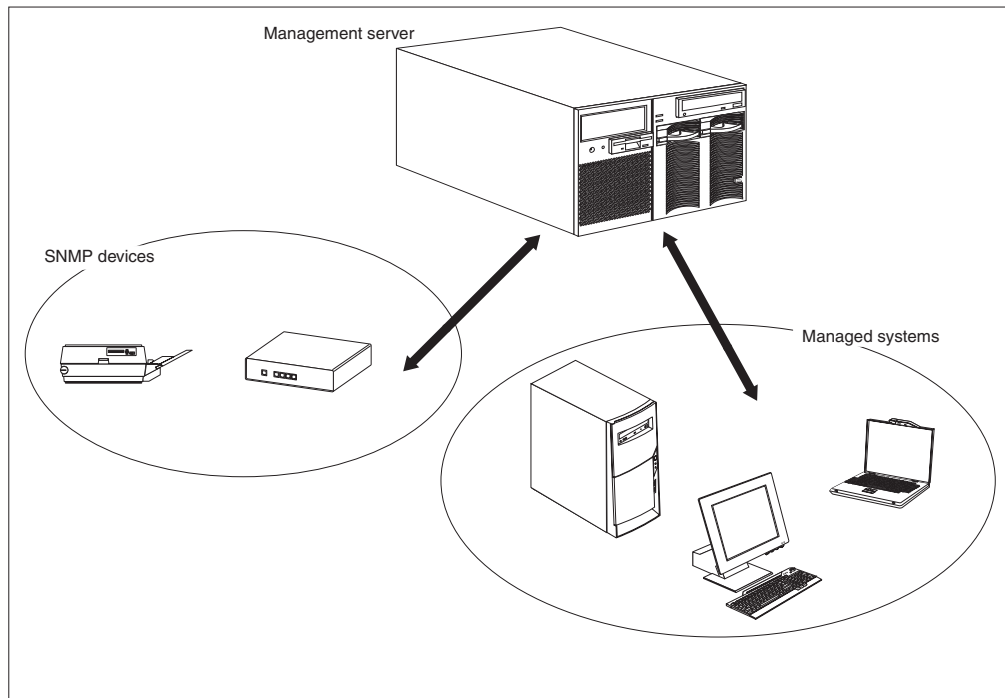


Figure 1. Hardware in an IBM Director environment

IBM Director components

The IBM Director software has three components:

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

IBM Director Server must be installed on the management server. When you install IBM Director Server on Microsoft Windows® or Linux, IBM Director Agent and IBM Director Console are installed automatically also. When you install IBM Director Server on IBM i5/OS™, IBM Director Agent is installed automatically also.

IBM Director Agent must be installed on each system that you want to manage.

IBM Director Console must be installed on each system from which a system administrator will remotely access the management server using the graphical user interface (GUI). A system on which IBM Director Console is installed is a *management console*.

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

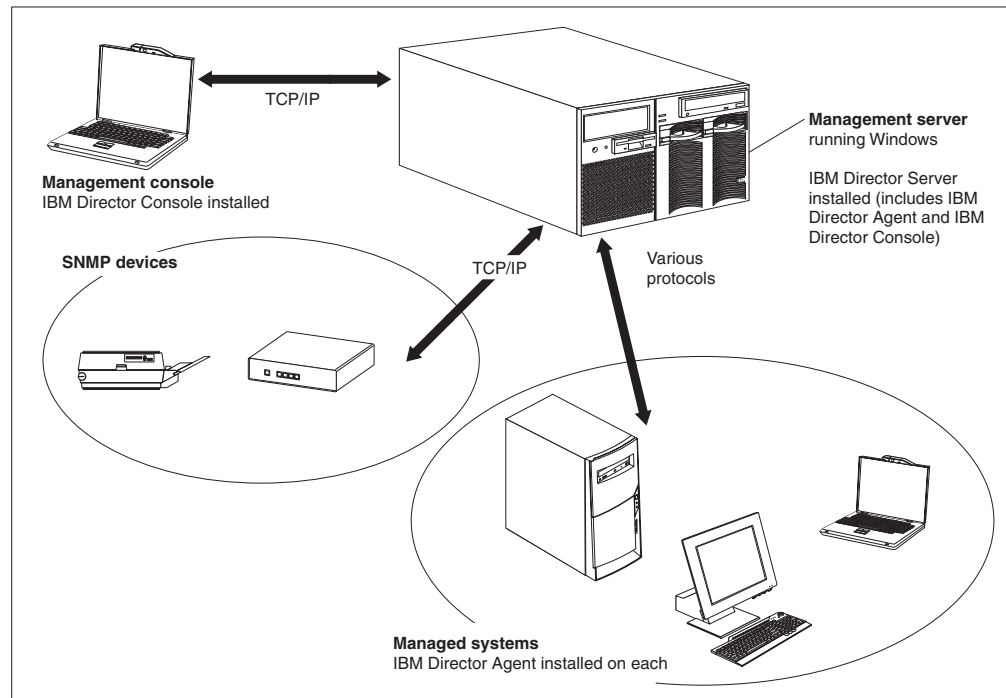


Figure 2. Software in an IBM Director environment

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.

Every IBM xSeries server and @server BladeCenter unit 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 Transmission Control Protocol/Internet Protocol (TCP/IP), Network Basic Input/Output System (NetBIOS), Internetwork Package Exchange (IPX), and Systems Network Architecture (SNA). IBM Director Server can communicate with all systems in your network that have IBM Director Agent installed.

The IBM Director Agent features vary according to the operating system on which IBM Director Agent is installed. For example, you can install Web-based Access only on Windows 32-bit operating systems.

All IBM @server Intel-compatible servers, IBM @server JS20 blade servers, IBM NetVista™ desktop computers, IBM ThinkCentre™ desktop computers, IBM PC desktop computers, IBM IntelliStation workstations, IBM ThinkPad® mobile computers, IBM TotalStorage® Network Attached Storage (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 GUI for IBM Director Server. Data is transferred between IBM Director Console and IBM Director Server through TCP/IP. Using IBM Director Console, you can conduct comprehensive systems management using either a drop-and-drag action or a single click.

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

You may 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 xSeries servers that contain a ServeRAID adapter or an integrated small computer system interface (SCSI) controller with redundant array of independent disks (RAID) capabilities. Using ServeRAID Manager, you can monitor and manage RAID arrays without taking the servers offline.

Note: ServeRAID Manager is not supported on VMware console or guest operating systems.

Management Processor Assistant Agent

Management Processor Assistant (MPA) Agent works with xSeries and @server 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)
- Intelligent Platform Management Interface (IPMI) baseboard management controller
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

You must install MPA Agent in order to use the MPA task to configure, monitor, and manage the service processors.

MPA Agent handles in-band communication between service processors and IBM Director Server. MPA Agent also provides in-band alert notification for certain managed systems running Linux and NetWare. For managed systems running

Linux, if System Health Monitoring is not supported on a server, MPA Agent handles in-band alert notification. For managed systems running NetWare, if supported by the service processor, MPA Agent handles in-band alert notification.

IBM Director Remote Control Agent

You can use IBM Director Remote Control Agent to perform remote desktop functions on managed systems. 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 supported only on Windows 32-bit and 64-bit operating systems.

Web-based Access

When you install Web-based Access on a managed system, you can access IBM Director Agent and view real-time asset and health information about the managed system from either a Web browser or the Microsoft Management Console (MMC). This feature is supported only on Windows 32-bit operating systems.

Web-based Access help files

These are the help files for the Web-based Access interface. They provide information about the managed-system data that is available when you use Web-based Access, as well as instructions for performing administrative tasks. Web-based Access is supported only on Windows 32-bit operating systems.

System Health Monitoring

System Health Monitoring provides active monitoring of critical system functions, including system temperatures, voltages, fan speeds, and power state. It produces and relays hardware alerts to the operating-system event log, IBM Director Server, and other management environments. This feature can be installed only on Windows 32-bit operating systems.

Notes:

1. For managed systems running Windows, you *must* install System Health Monitoring if you want to monitor the system hardware and send in-band alerts.
2. For managed systems running Linux, System Health Monitoring is supported on some xSeries servers. It is not an installable IBM Director Agent feature but is built into IBM Director Agent.

SNMP Access and Trap Forwarding

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

Note: For managed systems running Linux, SNMP Access and Trap Forwarding is not an installable IBM Director Agent feature but is built into IBM Director Agent.

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 Remote Deployment Manager, IBM Scalable Systems Manager, IBM Virtual Machine 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™ 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 on the *IBM Director* CD. The Server Plus Pack components for an IBM Director Agent installation are 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, which is located on the *IBM Director Server Plus Pack* CD.

The *IBM Director Server Plus Pack* CD is offered for purchase at 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, 365, 440 and 445 servers and the RXE-100 Remote Expansion Enclosure.

Using Active PCI Manager, you 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). Using FTMI, you can view network adapters that are members of fault-tolerant groups; you also can perform offline, online, failover, and eject operations on the displayed adapters. Using Slot Manager, you 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.

Capacity Manager

Using Capacity Manager, you 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, you can build a realistic, visual representation of a rack and its components. By clicking an element in the visual representation, you can access detailed information (such as system health and inventory data) for the rack component.

Software Rejuvenation

Using Software Rejuvenation, you 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; after being notified, you can take corrective action before a failure occurs.

You 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. Because Software Rejuvenation is cluster aware, you can use it to restart a node without taking the cluster offline.

System Availability

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

IBM Director Software Distribution (Premium Edition)

IBM Director Software Distribution (Premium Edition) adds functions to the IBM Director Software Distribution task. You can use the base IBM Director Software Distribution task to import IBM software and build software packages using the Update Assistant wizard. When you purchase and install IBM Director Software Distribution (Premium Edition), you can accomplish the following additional tasks:

- Import both IBM and non-IBM software and build software packages using the wizards that are designed for the following platforms: AIX®, i5/OS, Linux, and Windows
- Back up or export a software package for use on another management server
- Import a software package that was created by another management server

IBM Software Distribution (Premium Edition) is offered for purchase for an additional fee. For more information, contact your IBM marketing representative.

IBM Remote Deployment Manager

IBM Remote Deployment Manager (RDM) is a flexible and powerful tool for configuring, deploying, and retiring systems. Using RDM, you 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, because it uses industry-standard protocols to wake and discover target systems, RDM does not require an agent component.

RDM is offered for purchase for an additional fee. For more information, contact your IBM marketing representative.

IBM Scalable Systems Manager

You can use Scalable Systems Manager (SSM) for viewing, configuring, and managing static hardware partitions on supported xSeries servers. Using Scalable Systems Manager, you can perform the following tasks:

- View information about predefined scalable systems and scalable partitions that is saved in non-volatile random access memory (NVRAM)
- Configure and manage additional scalable systems and scalable partitions
- Configure RXE-100 Remote Expansion Enclosures that are attached to servers that are used in scalable partitions

Because SSM communicates with servers out-of-band through their service processor, it does not require an agent component.

You can download SSM from the IBM Support Web site.

IBM Virtual Machine Manager

IBM Virtual Machine Manager (VMM) enables the use of VMware VirtualCenter and Microsoft Virtual Server in an IBM Director environment. When VMM and these virtualization applications are installed, you can perform the following tasks from IBM Director Console:

- Correlate relationships between physical platforms and virtual components
- Report status of physical platforms and their corresponding virtual components
- Log in to the management interface of the virtualization application
- Discover virtual components
- Perform power operations on virtual machines
- Create event action plans that involve virtual objects

Additionally, for environments running VMware VirtualCenter, VMM provides the ability to move a running virtual machine between two physical hosts.

Additional IBM Director extensions

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

Cluster Systems Management

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

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

Real Time Diagnostics

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

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

Licensing

Every IBM xSeries server and @server BladeCenter unit comes with an IBM Director Server license. This license includes authorizations for the following installations:

- One installation of IBM Director Server
- 20 installations of IBM Director Agent on non-IBM systems
- Unlimited installations of IBM Director Console

Most IBM Intel-compatible systems come with a license for IBM Director Agent. For a complete list of IBM Intel-compatible systems and @server JS20 blade servers that are entitled to an IBM Director Agent license, see the *IBM Director Hardware and Software Compatibility* document. You can download this PDF file from the IBM Director Agent Web page at http://www.ibm.com/pc/ww/eserver/xseries/systems_management/nfdir/agent.html.

You can purchase additional licenses for non-IBM systems, if needed. For more information, contact your IBM marketing representative.

The license to install IBM Director Server also includes the right to install the Server Plus Pack on the management server. This allows you to use the Server Plus Pack extensions (except for Rack Manager) on the management server *only*. To install the Server Plus Pack on managed systems or Rack Manager on the management server, you must purchase additional licenses. Contact your IBM marketing representative for more information.

Upgrading from previous releases of IBM Director

If you are running one of the following versions of IBM Director on a supported operating system, you can upgrade to IBM Director 4.20:

- IBM Director 3.1
- IBM Director 3.1.1
- IBM Director 4.1
- IBM Director 4.10.2
- IBM Director 4.11
- IBM Director 4.12

Versions of IBM Director earlier than IBM Director 3.1 are not compatible with IBM Director 4.20.

IBM Director Server 4.20 can manage systems running IBM Director Agent, version 3.1 or later. This enables you to manage systems that are running operating systems that are not supported by IBM Director 4.20.

IBM Director Server and IBM Director Console must be at the same release level. If you upgrade IBM Director Server, you must upgrade IBM Director Console also.

If IBM Director Console and IBM Director Agent are installed on the same system, both software components must be at the same release level as IBM Director Server.

If the IBM SMBus device driver for Linux, version 4.1, 4.11, or 4.12, is installed on a managed system, you must uninstall the device driver and then install the IBM SMBus device driver, version 4.20.

Chapter 2. Operating systems supported by IBM Director and IBM Director tasks

This chapter provides information about what operating systems are supported by the IBM Director 4.20 components and IBM Director tasks.

Supported operating systems supported by IBM Director components

This section lists the operating systems upon which IBM Director Server, IBM Director Agent, and IBM Director Console are supported.

Consider the following restrictions concerning operating-system support:

- To install IBM Director Agent on the following operating systems, you can use either IBM Director Multiplatform or the IBM Director software that came with your BladeCenter unit:
 - AIX 5L, Version 5.2
 - Red Hat® Enterprise Linux AS, version 3.0, for IBM PowerPC® (iSeries and pSeries)
 - SUSE LINUX Enterprise Server 8 for IBM pSeries and IBM iSeries

The software for these installations also can be downloaded from the IBM Support Web site.

- To install IBM Director Agent or IBM Director Server on i5/OS (formerly OS/400®), you must use IBM Director Multiplatform, which is installed using the IBM Virtualization Engine.

For the most recent list of supported operating systems, see the *IBM Director Hardware and Software Compatibility* document. This PDF file is updated every 6 to 8 weeks. You can download it from http://www.ibm.com/servers/eserver/xseries/systems_management/sys_migration/ibmdiragent.html.

IBM Director Server

You can install IBM Director Server on the following operating systems:

- i5/OS, Version 5 Release 3
- Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 3.0, for Intel x86
- Red Hat Enterprise Linux ES, versions 2.1 and 3.0
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- Windows 2000, Advanced Server and Server Editions (Service Pack 3 required)
- Windows Server 2003, Enterprise, Standard, and Web Editions

IBM Director Agent

You can install IBM Director Agent on the following operating systems:

- AIX 5L, Version 5.2 (Recommended Maintenance Package 5.2.00-03 or later required)
- i5/OS, Version 5 Release 3
- Novell NetWare, versions 6.0 and 6.5
- Red Hat Linux Advanced Server, version 2.1 (Update 3 required)

- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 3.0, for Intel x86
- Red Hat Enterprise Linux ES and WS, versions 2.1 and 3.0
- Red Hat Enterprise Linux AS, version 3.0, for AMD64 (64-bit)
- Red Hat Enterprise Linux AS, version 3.0, for IBM PowerPC (iSeries and pSeries)
- Red Hat Enterprise Linux AS, version 3.0, for Intel Itanium (64-bit)
- SUSE LINUX Enterprise Server 8 for AMD64 (Service Pack 3 required)
- SUSE LINUX Enterprise Server 8 for IBM pSeries and IBM iSeries (Service Pack 3 required)
- SUSE LINUX Enterprise Server 8 for Itanium Processor Family (Service Pack 3 required)
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- VMware ESX Server, version 1.5.2 (Patch 3 required) with the following guest operating systems:
 - Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
 - Windows NT® 4.0 Workstation (Service Pack 6a or later required)
 - Windows NT 4.0 Server, Enterprise and Standard Editions (Service Pack 6a or later required)
 - Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 or later required)
 - Windows Server 2003, Enterprise, Standard, and Web Editions
- VMware ESX Server, version 2.0, with the following guest operating systems:
 - Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
 - Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
 - SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
 - Windows NT 4.0 Server (Service Pack 6a or later required)
 - Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 or later required)
 - Windows Server 2003, Enterprise, Standard, and Web Editions
- VMware ESX Server, version 2.0.1, with the following guest operating systems:
 - Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
 - Red Hat Enterprise Linux AS, versions 2.1 (Update 3 required)
 - Red Hat Enterprise Linux AS, version 3.0, for Intel x86
 - SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
 - Windows NT 4.0 Server (Service Pack 6a or later required)
 - Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 or later required)
 - Windows Server 2003, Enterprise, Standard, and Web Editions
- VMware ESX Server, version 2.1, with the following guest operating systems:
 - Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
 - Red Hat Enterprise Linux AS, version 3.0, for Intel x86
 - SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
 - Windows NT 4.0 Server (Service Pack 6a or later required)
 - Windows 2000, Advanced Server and Server Editions (Service Pack 3 or later required)
 - Windows XP Professional Edition (Service Pack 1 required)

- Windows Server 2003, Enterprise, Standard, and Web Editions
- Windows NT 4.0 Workstation (Service Pack 6a or later required)
- Windows NT 4.0 Server, Standard, Enterprise, and Terminal Server Editions (Service Pack 6a or later required)
- Windows NT 4.0 Server with Citrix MetaFrame (Service Pack 6a or later required)
- Windows 2000, Advanced Server, Datacenter Server, Professional, and Server Editions (Service Pack 3 or later required)
- Windows XP Professional Edition (Service Pack 1 or 1a recommended)
- Windows Server 2003, Enterprise, Datacenter, Standard, and Web Editions
- Windows Server 2003, Datacenter and Enterprise Editions, 64-bit versions

IBM Director Console

You can install IBM Director Console on the following operating systems:

- Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 3.0, for Intel x86
- Red Hat Enterprise Linux ES, versions 2.1 and 3.0
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 required)
- Windows XP Professional Edition (Service Pack 1 or 1a recommended)
- Windows Server 2003, Enterprise, Standard, and Web Editions

Operating systems supported by IBM Director tasks

Support for IBM Director tasks can vary depending on the following items:

- The managed system hardware
- The operating system that is installed on a managed system
- The service processor installed in the managed system
- The level of the device drivers that are installed on the managed system

Note: The device drivers that are available for a managed system depend on the service processor and operating system that are installed on the managed system.

For information about what hardware features are supported on IBM xSeries, BladeCenter, or IntelliStation hardware or what operating systems are supported on IBM xSeries, BladeCenter, or IntelliStation hardware, go to the IBM ServerProven Web site at <http://www.ibm.com/pc/us/compat/index.html>.

Note: IBM Director Agent for Windows NT has the following limitations in its systems-management capabilities and features:

- Read-only access when managing systems running Windows NT.
- The graphical user interface for the Network Configuration task is read-only in IBM Director Console.
- The graphical user interface for the System Accounts Configuration subtask is read-only in IBM Director Console.
- Active PCI Manager is not supported.
- Events for virtual and physical network interface cards (NIC) are discarded.

- The Network Adapter Common Information Model (CIM) provider (IBMPSG_PhysicalNetworkAdapter class) does not provide the physical slot number. Only the logical slot number can be obtained. Removable, Replaceable, and HotSwappable properties are not available.

Table 1 lists each IBM Director task and its associated supported operating-system tables.

Table 1. IBM Director tasks and the supported operating-system tables

Task	Supported operating-system table:
Active PCI Manager	Table 8 on page 26
Asset ID™	Table 2 on page 17
BladeCenter Assistant	Table 10 on page 29
Capacity Manager	Table 8 on page 26
CIM Browser	Table 2 on page 17
Configure Alert Standard Format	Table 2 on page 17
Configure SNMP Agent	Table 2 on page 17
DMI Browser	Table 2 on page 17
Event Log	Table 2 on page 17
File Transfer	Table 3 on page 18
Hardware alerts	Table 3 on page 18
Hardware Status	Table 3 on page 18
Inventory (hardware and software)	Table 3 on page 18
Management Processor Assistant	Table 4 on page 20
Microsoft Cluster Browser	Table 4 on page 20
Network Configuration	Table 4 on page 20
Power Management	Table 5 on page 22
Process Management	Table 6 on page 24
Rack Manager	Table 8 on page 26
Remote Control	Table 6 on page 24
Remote Session	Table 6 on page 24
Resource Monitors	Table 6 on page 24
ServeRAID Manager	Table 7 on page 25
SNMP Browser	Table 7 on page 25
Software Distribution	Table 9 on page 28
Software Rejuvenation	Table 8 on page 26
System Accounts	Table 7 on page 25
System Availability	Table 8 on page 26
Update Assistant	Table 9 on page 28

Table 2. Supported operating systems for the Asset ID, CIM Browser, Configure Alert Standard Format, Configure SNMP Agent, DMI Browser, and Event Log tasks

Operating system	Asset ID ¹	CIM Browser	Configure Alert Standard Format ¹	Configure SNMP Agent ¹	DMI Browser ²	Event Log	
Microsoft Windows							
Windows NT 4.0	<ul style="list-style-type: none"> • Workstation • Server Standard Edition • Server Enterprise Edition • Server Terminal Server Edition • Server With Citrix MetaFrame 	Yes	Yes	Yes	Yes	Yes	
Windows 2000	<ul style="list-style-type: none"> • Professional Edition • Server Edition • Advanced Server Edition • Datacenter Server Edition 	Yes	Yes	Yes	Yes	Yes	
Windows XP	Professional Edition	Yes	Yes	Yes	Yes	Yes	
Windows Server 2003	<ul style="list-style-type: none"> • Standard Edition • Enterprise Edition • Web Edition • Datacenter Edition 	Yes	Yes	Yes	Yes	Yes	
	<ul style="list-style-type: none"> • For 64-bit Itanium systems • Enterprise Edition • Datacenter Edition 	No	No	No	No	Yes	
Linux							
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	<ul style="list-style-type: none"> • AS • ES • WS 	Yes	Yes	Yes	Yes	No	Yes
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	<ul style="list-style-type: none"> • Intel Itanium • AMD64 • IBM PowerPC (iSeries and pSeries) 	No	No	No	No	No	Yes
SUSE LINUX Enterprise Server 8	For x86	Yes	Yes	No	Yes	No	Yes
	<ul style="list-style-type: none"> • AMD64 • IBM pSeries and iSeries • Itanium Processor Family 	No	No	No	No	No	Yes
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	Console	Yes	Yes	No	No	No	Yes
	Guest operating systems	Yes	Yes	No	Windows only	Windows only	Yes
Other							
NetWare, versions 6.0 and 6.5		No	No	No	No	No	Yes
AIX 5L, Version 5.2		No	No	No	No	No	Yes
i5/OS, Version 5 Release 3 ¹		No	No	No	No	No	Yes
<p>1. If IBM Director Server is installed on a server running i5/OS, this task is not available.</p> <p>2. To use the DMI Browser task, the Desktop Management Interface (DMI) Service Layer must be installed.</p>							

The hardware on which the operating system is running determines what hardware alerts you can receive. The managed system must have a supported service processor in order to receive MPA events. Alerts can be MPA- or CIM-based events, and there is a subset of events that are both MPA and CIM-based. Also, if the managed system hardware has system-health support, system-health events are provided through CIM-based events.

Table 3. Supported operating systems for hardware alerts and the File Transfer, Hardware Status, and Inventory tasks

Operating system		File Transfer	Hardware alerts	Hardware Status ⁷	Inventory	
					Hardware	Software
Microsoft Windows						
Windows NT 4.0	<ul style="list-style-type: none"> • Workstation • Server Standard Edition • Server Enterprise Edition • Server Terminal Server Edition • Server With Citrix MetaFrame 	Yes	Yes ²	Yes ²	Yes	Yes
Windows 2000	<ul style="list-style-type: none"> • Professional Edition • Server Edition • Advanced Server Edition • Datacenter Server Edition 	Yes	Yes ²	Yes ²	Yes	Yes
Windows XP	Professional Edition	Yes	Yes ²	Yes ²	Yes	Yes
Windows Server 2003	<ul style="list-style-type: none"> • Standard Edition • Enterprise Edition • Web Edition • Datacenter Edition 	Yes	Yes ²	Yes ²	Yes	Yes
	For 64-bit Itanium systems <ul style="list-style-type: none"> • Enterprise Edition • Datacenter Edition 	Yes	Yes ³	Yes ³	Yes ⁸	Yes
Linux						
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	<ul style="list-style-type: none"> • AS • ES • WS 	Yes	Yes ⁴	Yes ⁴	Yes	Yes
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	Intel Itanium	Yes	Yes ³	Yes ³	Yes ⁸	Yes
	AMD64	Yes	Yes ⁴	Yes ⁴	Yes ⁸	Yes
	IBM PowerPC (iSeries and pSeries)	Yes	Yes ⁵	Yes ⁵	Yes	Yes
SUSE LINUX Enterprise Server 8	For x86	Yes	Yes ⁴	Yes ⁴	Yes	Yes
	AMD64	Yes	Yes ⁴	Yes ⁴	Yes ⁸	Yes
	IBM pSeries and iSeries	Yes	Yes ⁵	Yes ⁵	Yes ⁸	Yes
	Itanium Processor Family	Yes	Yes ³	Yes ³	Yes ⁸	Yes
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	Console	Yes	Yes ⁴	Yes ⁴	Yes	Yes
	Guest operating systems	Yes ¹	Not applicable	Not applicable	Yes	Yes
Other						
NetWare, versions 6.0 and 6.5		Yes	Yes ⁶	Yes ⁶	Yes ⁸	No

Table 3. Supported operating systems for hardware alerts and the File Transfer, Hardware Status, and Inventory tasks (continued)

Operating system	File Transfer	Hardware alerts	Hardware Status ⁷	Inventory	
				Hardware	Software
AIX 5L, Version 5.2	Yes	Yes ⁵	Yes ⁵	Yes ⁸	Yes
i5/OS, Version 5 Release 3	Yes	No	No	Yes	Yes

1. File systems that are displayed for the guest operating system are limited to file systems within its virtual disk.
2. Out-of-band generated by a service processor or in-band generated by CIM only.
3. Out-of-band only, generated by a service processor.
4. Out-of-band generated by a service processor or in-band generated by CIM (CIM support is system specific) only.
5. (BladeCenter JS20 only) Out-of-band only, generated by a service processor.
6. In band; out-of-band generated by service processor.
7. Supported (although the support might be limited) whenever in-band or out-of-band alerts generated by a service processor or in-band alerts generated by CIM are supported on a server.
8. CIM-based support is not available.

Support for Management Processor Assistant is available when a supported service processor is installed in a server. In-band support for Management Processor Assistant depends on whether a service processor device driver is available for the operating system running on the managed system. For more information about managing service processors, and in-band and out-of-band communication, see the *IBM Director 4.20 Installation and Configuration Guide*.

Table 4. Supported operating systems for the Management Processor Assistant, Microsoft Cluster Browser, and Network Configuration tasks

Operating system		Management Processor Assistant		Microsoft Cluster Browser	Network Configuration ³
		In-band support	Out-of-band support		
Microsoft Windows					
Windows NT 4.0	<ul style="list-style-type: none"> • Workstation • Server Standard Edition • Server Enterprise Edition • Server Terminal Server Edition • Server With Citrix MetaFrame 	Yes	Yes	Yes	Yes ⁴
Windows 2000	<ul style="list-style-type: none"> • Professional Edition • Server Edition • Advanced Server Edition • Datacenter Server Edition 	Yes	Yes	Yes	Yes
Windows XP	Professional Edition	No	Yes	Yes	Yes
Windows Server 2003	<ul style="list-style-type: none"> • Standard Edition • Enterprise Edition • Web Edition • Datacenter Edition 	Yes	Yes	Yes	Yes
	For 64-bit Itanium systems	No	Yes	No	No
Linux					
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	<ul style="list-style-type: none"> • AS • ES • WS 	Yes	Yes	No	Yes
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	Intel Itanium	No	Yes	No	No
	AMD64	Yes	Yes	No	No
	IBM PowerPC (iSeries and pSeries)	No	Yes	No	No
SUSE LINUX Enterprise Server 8	For x86	Yes ¹	Yes	No	Yes
	For AMD64	Yes	Yes	No	No
	For IBM pSeries and iSeries	No	Yes	No	No
	For Itanium Processor Family	No	Yes	No	No

Table 4. Supported operating systems for the Management Processor Assistant, Microsoft Cluster Browser, and Network Configuration tasks (continued)

Operating system		Management Processor Assistant		Microsoft Cluster Browser	Network Configuration ³
		In-band support	Out-of-band support		
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	Console	Yes ²	Yes	No	Yes
	Guest operating systems	Not applicable	Not applicable	No	Yes
Other					
NetWare, versions 6.0 and 6.5		Yes ²	Yes	No	No
AIX 5L, Version 5.2		No	Yes	No	No
i5/OS, Version 5 Release 3 ³		No	No	No	No
<ol style="list-style-type: none"> 1. In-band only, on servers that have either Remote Supervisor Adapter and Remote Supervisor Adapter II device drivers for this operating system. 2. Support depends on service processor device driver availability. 3. If IBM Director Server is installed on a server running i5/OS, the Network Configuration task is not available. 4. The graphical user interface for the Network Configuration task is read-only in IBM Director Console. 					

Power Management support is provided by a combination of IBM Director Agent, Management Processor Assistant, and Alert Standard Format (ASF). Support for each Power Management subtask can vary depending on the managed system hardware and hardware options, and the operating system.

Table 5. Supported operating systems for the Power Management task

Operating system		Power Management subtasks					
		Power On	Restart	Restart Now	Power Off	Power Off Shutdown	Shutdown
Microsoft Windows							
Windows NT 4.0	<ul style="list-style-type: none"> • Workstation • Server Standard Edition • Server Enterprise Edition • Server Terminal Server Edition • Server With Citrix MetaFrame 	Yes ^{1, 2}	Yes ^{4, 5}	Yes ^{1, 3}	Yes ¹	Yes ⁵	Yes ⁴
Windows 2000	<ul style="list-style-type: none"> • Professional Edition • Server Edition • Advanced Server Edition • Datacenter Server Edition 	Yes ^{1, 2, 3}	Yes ^{4, 5}	Yes ^{1, 3}	Yes ^{1, 3}	Yes ^{4, 5}	No
Windows XP	Professional Edition	Yes ^{1, 2, 3}	Yes ^{4, 5}	Yes ^{1, 3}	Yes ^{1, 3}	Yes ^{4, 5}	No
Windows Server 2003	<ul style="list-style-type: none"> • Standard Edition • Enterprise Edition • Web Edition • Datacenter Edition 	Yes ^{1, 2, 3}	Yes ^{4, 5}	Yes ^{1, 3}	Yes ^{1, 3}	Yes ^{4, 5}	No
	For 64-bit Itanium systems <ul style="list-style-type: none"> • Enterprise Edition • Datacenter Edition 	Yes ^{1, 2}	Yes ⁴	Yes ^{1, 3}	Yes ¹	Yes ⁴	No
Linux							
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	<ul style="list-style-type: none"> • AS • ES • WS 	Yes ^{1, 2}	Yes ^{4, 5}	Yes ¹	Yes ¹	Yes ¹	No
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	<ul style="list-style-type: none"> • Intel Itanium • AMD64 	Yes ^{1, 2}	Yes ⁴	Yes ¹	Yes ¹	Yes ¹	No
	IBM PowerPC (iSeries)	Yes ²	Yes ²	Yes ⁶	Yes ⁶	Yes ¹	No
	IBM PowerPC (pSeries)	Yes ⁶	Yes ^{4, 6}	Yes ⁶	Yes ⁶	Yes ⁶	No
SUSE LINUX Enterprise Server 8	For x86	Yes ^{1, 2}	Yes ^{4, 5}	Yes ¹	Yes ¹	Yes ¹	No
	For AMD64	Yes ^{1, 2}	Yes ⁴	Yes ¹	Yes ¹	Yes ¹	No
	For IBM pSeries	Yes ⁶	Yes ^{4, 6}	Yes ⁶	Yes ⁶	Yes ⁶	No
	For IBM iSeries	Yes ⁶	Yes ²	Yes ⁶	Yes ⁶	No	No
	For Itanium Processor Family	Yes ^{1, 2}	Yes ⁴	Yes ¹	Yes ¹	No	No
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	Console	Yes ^{1, 2}	Yes ^{4, 5}	Yes ¹	Yes ¹	Yes ¹	No
	Guest operating systems	No	Yes ⁴	No	Yes ⁴	Windows only ⁴	No
Other							
NetWare, versions 6.0 and 6.5		Yes ^{1, 2}	Yes ^{4, 5}	Yes ¹	Yes ¹	Yes ¹	Yes ⁴
AIX 5L, Version 5.2		Yes ⁶	Yes ^{4, 6}	Yes ⁶	Yes ⁴	Yes ⁶	No

Table 5. Supported operating systems for the Power Management task (continued)

Operating system	Power Management subtasks					
	Power On	Restart	Restart Now	Power Off	Power Off Shutdown	Shutdown
i5/OS, Version 5 Release 3	No	No	No	No	No	No
<ol style="list-style-type: none"> 1. Support provided by Management Processor Assistant when a supported service processor is installed in the managed system. 2. Support provided by IBM Director Agent when the Wake on LAN[®] feature is available in the managed system. 3. Support provided by ASF 2.0 when an ASF 2.0-capable NIC is installed in the managed system. 4. Support provided by IBM Director Agent. 5. Support provided by Management Processor Assistant when a supported service processor and the MPA Agent is installed on the managed system. 6. (BladeCenter JS20 only) Support provided by Management Processor Assistant. 						

Table 6. Supported operating systems for the Process Management, Remote Control, Remote Session, and Resource Monitors tasks

Operating system		Process Management	Remote Control	Remote Session ¹	Resource Monitors
Microsoft Windows					
Windows NT 4.0	<ul style="list-style-type: none"> • Workstation • Server Standard Edition • Server Enterprise Edition • Server Terminal Server Edition • Server With Citrix MetaFrame 	Yes	Yes	Yes	Yes
Windows 2000	<ul style="list-style-type: none"> • Professional Edition • Server Edition • Advanced Server Edition • Datacenter Server Edition 	Yes	Yes	Yes	Yes
Windows XP	Professional Edition	Yes	Yes	Yes	Yes
Windows Server 2003	<ul style="list-style-type: none"> • Standard Edition • Enterprise Edition • Web Edition • Datacenter Edition • For 64-bit Itanium systems, Enterprise Edition • For 64-bit Itanium systems, Datacenter Edition 	Yes	Yes	Yes	Yes
Linux					
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	<ul style="list-style-type: none"> • AS • ES • WS 	Yes	No	Yes	Yes
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	<ul style="list-style-type: none"> • Intel Itanium • AMD64 	Yes	No	Yes	Yes
	IBM PowerPC (iSeries and pSeries)	Yes	No	Yes	Yes
SUSE LINUX Enterprise Server 8	<ul style="list-style-type: none"> • For x86 • AMD64 • IBM pSeries and iSeries • Itanium Processor Family 	Yes	No	Yes	Yes
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	Console	Yes	No	Yes	Yes
	Guest operating systems	Yes	Windows only	Yes	Yes
Other					
NetWare, versions 6.0 and 6.5		Yes	No	Yes	Yes
AIX 5L, Version 5.2		Yes	No	Yes	Yes
i5/OS, Version 5 Release 3		Yes	No	Yes	Yes
1. The Remote Session task works on any SNMP device that has either Secure Shell (SSH) or Telnet server installed and running. Also, the root user must not be locked out.					

Table 7. Supported operating systems for the ServeRAID Manager, SNMP Browser, and System Accounts tasks

Operating system		ServeRAID Manager ¹	SNMP Browser ²	System Accounts ¹
Microsoft Windows				
Windows NT 4.0	<ul style="list-style-type: none"> • Workstation • Server Standard Edition • Server Enterprise Edition • Server Terminal Server Edition • Server With Citrix MetaFrame 	Yes	Yes	Yes ³
Windows 2000, Professional Edition	<ul style="list-style-type: none"> • Professional Edition • Server Edition • Advanced Server Edition • Datacenter Server Edition 	Yes	Yes	Yes
Windows XP	Professional Edition	Yes	Yes	Yes
Windows Server 2003	<ul style="list-style-type: none"> • Standard Edition • Enterprise Edition • Web Edition • Datacenter Edition • For 64-bit Itanium systems, Enterprise Edition • For 64-bit Itanium systems, Datacenter Edition 	Yes	Yes	Yes
Linux				
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	<ul style="list-style-type: none"> • AS • ES • WS 	Yes	Yes	Yes
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	Intel Itanium	Yes	Yes	No
	AMD64	Yes	Yes	No
	IBM PowerPC (iSeries and pSeries)	No	Yes	No
SUSE LINUX Enterprise Server 8	For x86	Yes	Yes	No
	AMD64	Yes	Yes	No
	IBM pSeries and iSeries	No	Yes	No
	Itanium Processor Family	Yes	Yes	No
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	Console	No	Yes	Yes
	Guest operating system	No	Yes	Yes
Other				
NetWare, versions 6.0 and 6.5		Yes	Yes	No
AIX 5L, Version 5.2		No	Yes	No
i5/OS, Version 5 Release 3 ¹		No	Yes	No
<ol style="list-style-type: none"> 1. If IBM Director Server is installed on a server running i5/OS, this task is not available. 2. To use the SNMP Browser task, the operating system SNMP agent must be installed. 3. The graphical user interface for the System Accounts Configuration subtask is read-only in IBM Director Console. 				

Server Plus Pack tasks

Table 8 lists the operating systems supported by the Server Plus Pack tasks. When reviewing Table 8, consider the following limitations:

- These tasks are specifically designed for use on xSeries and Netfinity servers.
- If IBM Director Server is installed on a server running i5/OS, the Server Plus Pack tasks are not available.
- Active PCI Manager support depends not only on the operating system, but also on the managed system hardware. See “Active PCI Manager” on page 8 for information about support.

Table 8. Supported operating systems for the Server Plus Pack tasks

Operating system		Active PCI Manager	Capacity Manager	Rack Manager	Software Rejuvenation	System Availability
Microsoft Windows						
Windows NT 4.0	Workstation	No	No	Yes	No	No
	• Server Standard Edition • Server Enterprise Edition	No	Yes	Yes	Yes	Yes
	• Server Terminal Server Edition • Server With Citrix MetaFrame	No	No	Yes	No	No
Windows 2000	Professional Edition	No	No	Yes	No	No
	• Server Edition • Advanced Server Edition • Datacenter Server Edition	Yes	Yes	Yes	Yes	Yes
Windows XP	Professional Edition	No	No	Yes	No	No
Windows Server 2003	• Standard Edition • Enterprise Edition • Web Edition	Slot Manager only	Yes	Yes	Yes	Yes
	Datacenter Edition	Slot Manager only	Yes	Yes	Yes	Yes
	For 64-bit Itanium systems • Enterprise Edition • Datacenter Edition	No	No	Yes	No	No
Linux						
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	• AS • ES	No	Yes	Yes	Yes	Yes
	WS	No	No	Yes	No	No
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	• Intel Itanium • AMD64 • IBM PowerPC (iSeries and pSeries)	No	No	No	No	No

Table 8. Supported operating systems for the Server Plus Pack tasks (continued)

Operating system		Active PCI Manager	Capacity Manager	Rack Manager	Software Rejuvenation	System Availability
SUSE LINUX Enterprise Server 8	For x86	Slot Manager only	Yes	Yes	Yes	Yes
	AMD64	No	No	No	No	No
	IBM pSeries and iSeries	No	No	Yes	No	No
	Itanium Processor Family	No	No	No	No	No
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	Console	No	Yes	No	No	Yes
	Guest operating systems	No	Yes	No	Yes	Yes
Other						
NetWare, versions 6.0 and 6.5		No	Yes	Yes	No	No
AIX 5L, Version 5.2		No	No	No	No	No
i5/OS, Version 5 Release 3		No	No	No	No	No

Software-distribution features

Table 9 lists the operating-system support for the software-distribution features.

Table 9. Supported operating systems for IBM Director software-distribution features

Operating system		Software Distribution		Update Assistant
		Standard Edition	Premium Edition	
Microsoft Windows				
Windows NT 4.0	<ul style="list-style-type: none"> • Workstation • Server Standard Edition • Server Enterprise Edition • Server Terminal Server Edition • Server With Citrix MetaFrame 	Yes	Yes	Yes
Windows 2000	<ul style="list-style-type: none"> • Professional Edition • Server Edition • Advanced Server Edition • Datacenter Server Edition 	Yes	Yes	Yes
Windows XP	Professional Edition	Yes	Yes	Yes
Windows Server 2003	<ul style="list-style-type: none"> • Standard Edition • Enterprise Edition • Web Edition • Datacenter Edition • For 64-bit Itanium systems, Enterprise Edition • For 64-bit Itanium systems, Datacenter Edition 	Yes	Yes	Yes
Linux				
Red Hat Enterprise Linux, versions 2.1 and 3.0, for 32-bit systems	<ul style="list-style-type: none"> • AS • ES • WS 	Yes	Yes	Yes
Red Hat Enterprise Linux AS, version 3.0, for 64-bit systems	<ul style="list-style-type: none"> • Intel Itanium • AMD64 • IBM PowerPC (iSeries and pSeries) 	Yes	Yes	Yes
SUSE LINUX Enterprise Server 8	<ul style="list-style-type: none"> • For x86 • AMD64 • IBM pSeries and iSeries • Itanium Processor Family 	Yes	Yes	Yes
VMware ESX Server, versions 1.5.2, 2.0, 2.0.1, and 2.1	<ul style="list-style-type: none"> • Console • Guest operating systems 	Yes	Yes	Yes
Other				
NetWare, versions 6.0 and 6.5		No	No	No
AIX 5L, Version 5.2		Yes	Yes	Yes
i5/OS, Version 5 Release 3		Yes	Yes	No

IBM Director task support for BladeCenter products

A BladeCenter unit consists of a chassis, one or two management modules, one or more switches (up to four total), and one or more blade servers (depending on the model, up to 14 total).

The chassis is the physical enclosure that contains the blade servers. The chassis has one or two management modules that contain 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 to be a managed device. When you view 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 object. However, after you install IBM Director Agent on the blade server, it is a managed object, and the features and functions that you can use on the blade server are comparable to those that you can use on any managed object. For information about IBM Director Console, physical platforms and managed objects, see Chapter 3, “Understanding IBM Director Console,” on page 31.

IBM Director tasks that you can use on your BladeCenter unit can vary, depending on the features and options that you have installed. See Table 10 for a list of IBM Director tasks and information about whether you can use a task on the chassis, switch, or a blade server without IBM Director Agent installed. Unless otherwise noted in this documentation, a task behaves the same for blade servers as for any managed system.

Notes:

1. When IBM Director Agent is installed on a blade server, the supported tasks depend on the operating system that is installed on the blade server. See “Operating systems supported by IBM Director tasks” on page 15 for information.
2. If IBM Director Server is installed on a server running i5/OS, the BladeCenter Assistant task is not available.

Table 10. IBM Director task support for BladeCenter products

Task	Chassis	Switch	Blade server without IBM Director Agent installed
BladeCenter Configuration	Yes	No	Yes
BladeCenter Management	Yes	No	Yes
BladeCenter Deployment wizard	Yes	No	No
Switch Management launch pad	No	Yes	No
Blue indicator light	Yes	No	Yes
Event action plans	Yes	Yes	Yes
Hardware Status	Yes	No	Yes ¹
Inventory	Yes	Yes	Yes
Power Management	No	No	Yes

Table 10. IBM Director task support for BladeCenter products (continued)

Task	Chassis	Switch	Blade server without IBM Director Agent installed
Rack Manager	Yes	Yes	No
Remote Session	No	Yes	No
Remote Monitors	No	Yes	No
SNMP devices (Browser)	No	Yes	Yes ²
<p>1. Inventory of the chassis, switch, and blade servers can be obtained through the management module. Blade server inventory that is collected through the management module is a subset of the total inventory that is available if IBM Director Agent is installed on the blade server.</p> <p>2. To use the SNMP Browser task, the operating system SNMP agent must be installed on the server blade.</p>			

Chapter 3. 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 provides information about how to use IBM Director Console to accomplish these activities, and how to use IBM Director tasks that are used on other tasks, such as Scheduler.

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 objects included in the group selected in the Groups pane.
- The Tasks pane lists IBM Director tasks that are available.

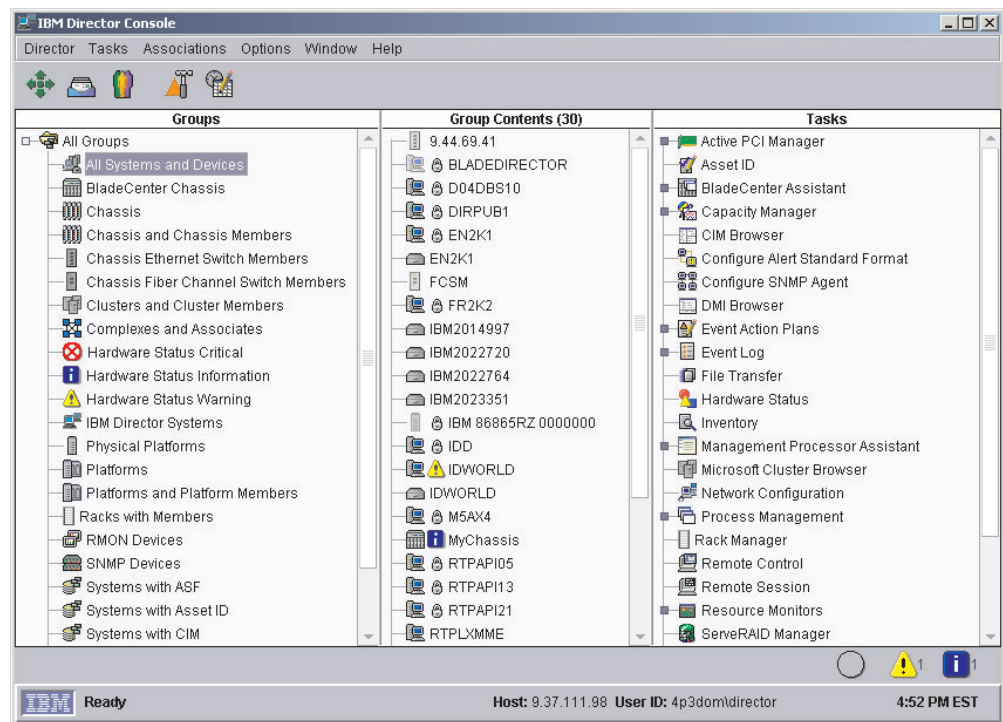


Figure 3. IBM Director Console

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

A padlock icon beside a managed object indicates that the object is secured by a server and inventory information about the object cannot be collected. To request access to the object, right-click the managed object and click **Request Access**. By providing a valid user name that has local administrative rights to that managed object 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 same method.

Notes:

1. (ISMP systems only) You cannot log in to an ISMP directly, as it lacks a userid and password. Instead, connect out-of-band to an ISMP installed on an ASM interconnect network through a Remote Supervisor Adapter or Remote Supervisor Adapter II serving as the ASM gateway.
2. (ASM processor systems only) Use the Management Processor Assistant to configure an out-of-band path to the ASM processor system, then change the userid and password to request access the physical platform using IBM Director Console.

You can right-click a managed object in the Group Contents pane to see what actions you can perform on the object. For example, you can delete the object, perform a presence check on the object, or **View Inventory** of the object.

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

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

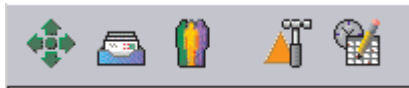


Figure 4. IBM Director Console toolbar

From left to right, the icons represent:

- Discover All Systems (see the *IBM Director 4.20 Installation and Configuration Guide*)
- Message Browser (see “Message Browser” on page 48)
- User Administration (see “User Administration” on page 49)
- Event Action Plan Builder (see Chapter 4, “Managing and monitoring systems with event action plans,” on page 55)
- Scheduler (see “Scheduler” on page 40)

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 ways:

- Dragging a task onto a managed object (or a managed group, in some cases)
- Dragging a managed object (or a managed group, in some cases) onto a task
- Right-clicking a managed object (or managed group, in some cases)

Throughout this documentation, only dragging a task onto a managed object or group is explained as the method of starting tasks, although you can use any of the three methods.

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

- From the menu bar
- From the toolbar

Note: When IBM Director Console is processing a task, the hourglass is displayed for that window and you cannot use the mouse to work with the window. Although it might be possible to work with the window using key strokes, do *not* do so.

Managed systems and managed objects

One key to using IBM Director is understanding the concept of managed systems, managed devices, and managed objects. Each term refers to different types of hardware.

- A *managed system* has IBM Director Agent installed.
- A *managed device* is an SNMP device such as a network device, printer, desktop computer, or server that has an SNMP agent installed or embedded.
- A *managed object* can refer to a managed system or device, or a Windows cluster, BladeCenter chassis, management processor, multi-node server (scalable system), scalable partition, static partition, physical platform, remote input/output (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 one or more physical platforms representing the xSeries server or servers 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 also can be created when:

- A deployable system is discovered through an RDM scan
- You right-click any blank space in the Group Contents pane to create the physical platform manually
- IBM Director Server determines that a physical platform does not exist already 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 Internet Protocol (IP) access to a Remote Supervisor Adapter service processor. It will query the Remote Supervisor Adapter or Remote Supervisor Adapter II service processor for the topology of its associated ASM interconnect 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.

Note: To delete a physical platform from IBM Director Console, you also must delete any associated managed system or systems.

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 objects and devices.

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

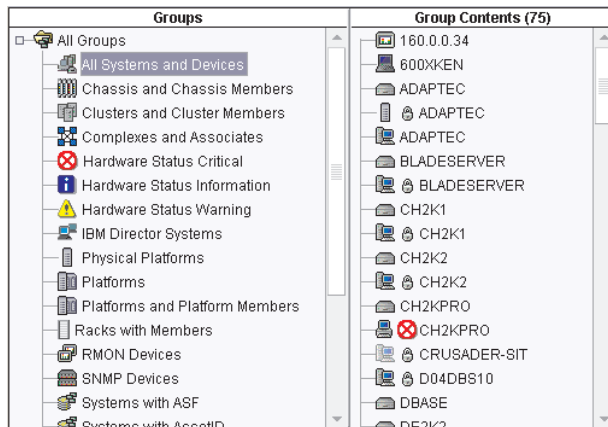


Figure 5. IBM Director Console: Group Contents pane listing a selected group

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

Note: (i5/OS only) The following groups do not appear in the Groups pane when using a management server that is running i5/OS:

- Systems with ASF
- Systems with ASF Secure Remote Management
- Systems with Asset ID
- Systems with SNMP Agent
- Racks with Members

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 36.

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 objects must match. IBM Director automatically adds or removes managed objects 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.

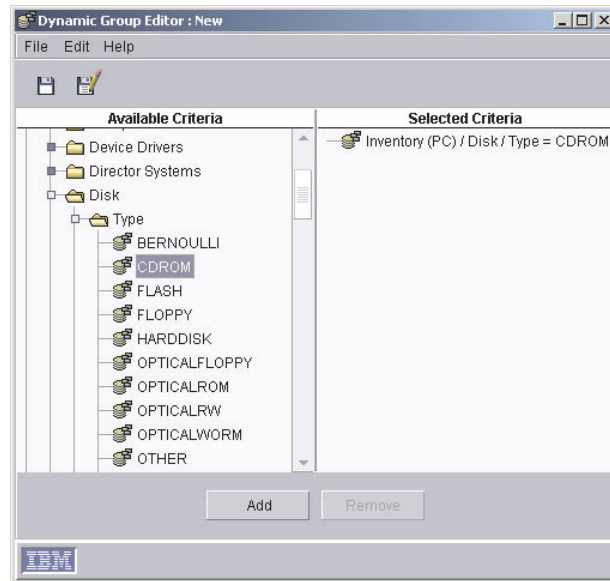


Figure 6. “Dynamic Group Editor” window

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 the equal sign (=). 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.

Note: The group name is case-sensitive.

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.

Notes:

1. You cannot use a wild card (*.*) to create a dynamic group.
2. To create a dynamic group for criteria that is not present in the IBM Director Server database, you must use DIRCMD. For more information, see “Installing and accessing DIRCMD” on page 277.

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 objects is enabled. This type of dynamic group saves you time because you can drag a task directly onto all managed objects 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.

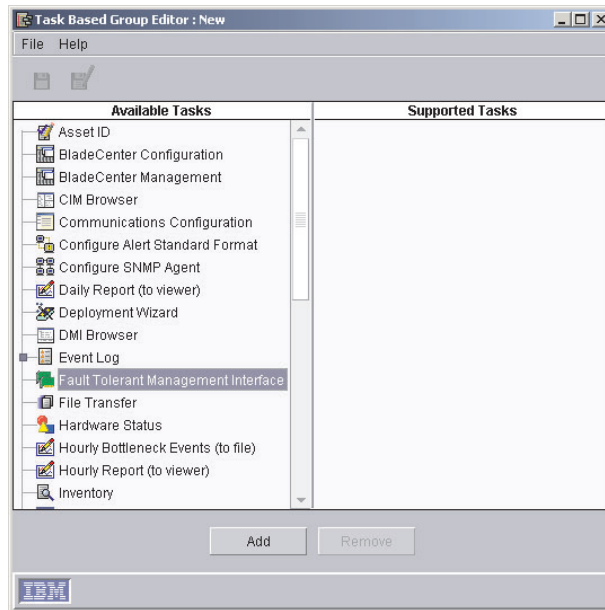


Figure 7. “Task Based Group Editor” window

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.

Note: The group name is case-sensitive.

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 objects 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” window opens in the bottom half of the Groups pane.

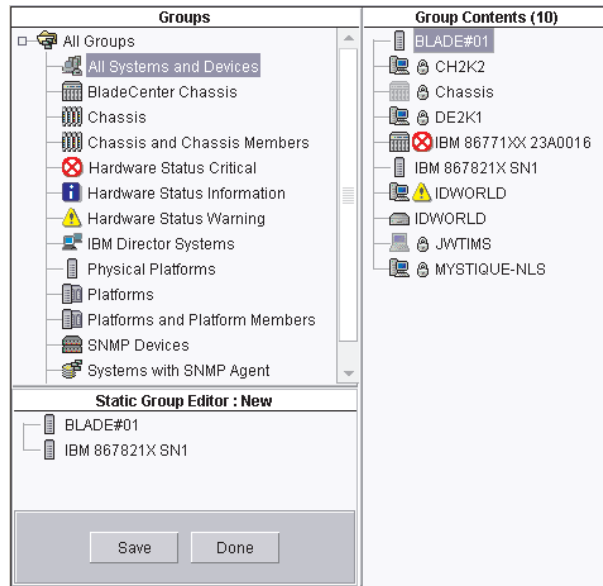


Figure 8. “Static Group Editor” window

2. Drag the managed systems that you want to add to the new static group onto the “Static Group Editor” window. The selected managed objects are added to the group.
3. When you are finished adding managed objects, 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.

Note: The group name is case-sensitive.

5. Click **OK**. The group is displayed under **All Groups** in the Groups pane.
6. Click **Done** to close the “Static Group Editor” window.

Using the Category Editor: Use the Category Editor to organize large numbers of groups by creating group categories. Group categories that are created with the Category Editor are static, although the groups that are 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” window opens in the bottom half of the Groups pane.

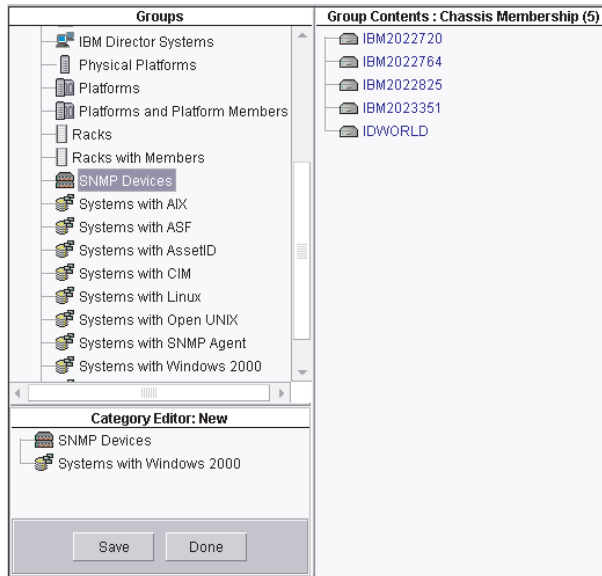


Figure 9. “Category Editor” window

2. Drag the groups that 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. This is the group name that will be listed in the Groups pane.

Note: The group name is case-sensitive.

5. Click **OK**. The new group category is displayed in the Groups pane.
6. Click **Done** to close the “Category Editor” window. The group is displayed under **All Groups** in the Groups pane.

Group export and import

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 that you want to export from the groups that are 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 that 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 that 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.

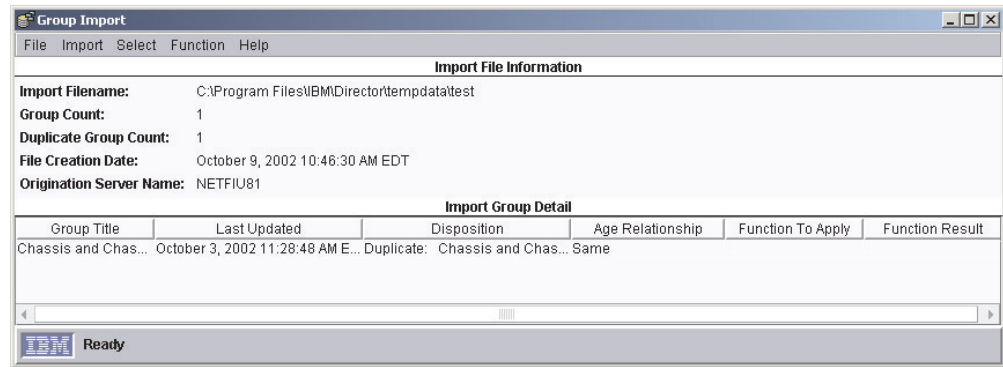


Figure 10. “Group Import” window

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 according to 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 associations are available:

- None
- Object Type
- TCP/IP Addresses
- TCP/IP Host Names
- IPX Network IDs
- Domains/Workgroups
- Chassis Membership
- Cluster Membership
- Physical Platform—Remote I/O Enclosures
- Platform Membership
- Rack Membership
- Scalable Partitions Membership
- Scalable Systems Membership
- TCP/IP Routers/DNS
- Status
- SNMP System Object ID

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 alphabetically in blue type.

You also can display additional information about the managed objects that are displayed in the Group Contents pane by selecting options from the bottom half of the **Associations** menu. For example, you can view the managed objects that have event action plans applied to them. If a managed object has an event action plan applied to it, the managed object 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 options are available:

Software Packages

Shows which packages, if any, have been delivered to a managed object using the Software Distribution task.

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

Activations

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

Resource Monitors

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

Event Action Plans

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

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 allow saving changes to an existing job; you must always save changes to an existing job as a new job.

Starting Scheduler

You can start Scheduler in either of two ways:

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

To schedule a task using the second technique, see “Dragging a task onto a managed object or group” on page 45.

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.

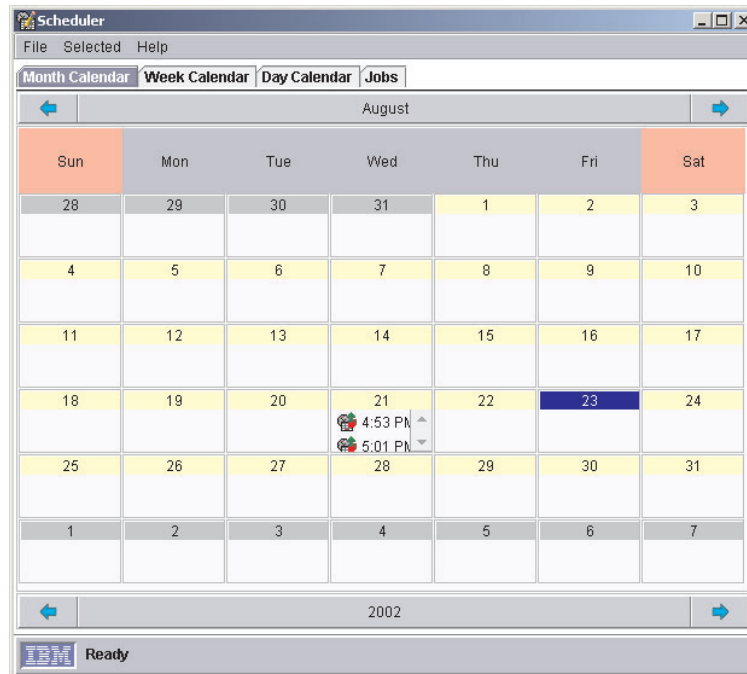


Figure 11. “Scheduler” window

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

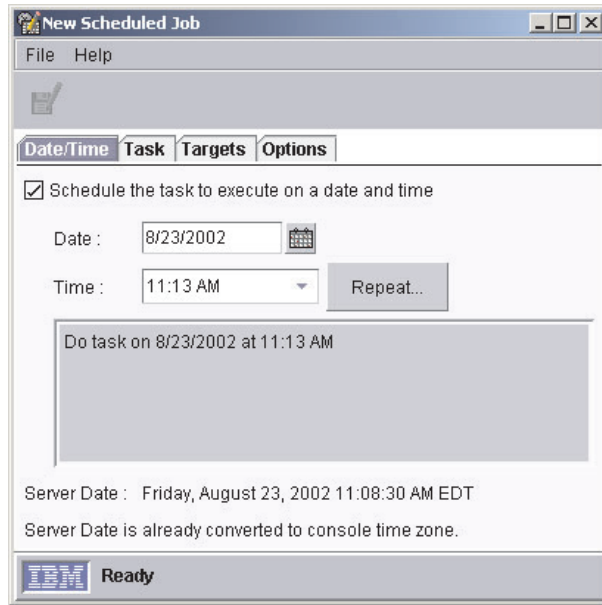


Figure 12. “New Scheduled Job” window

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.

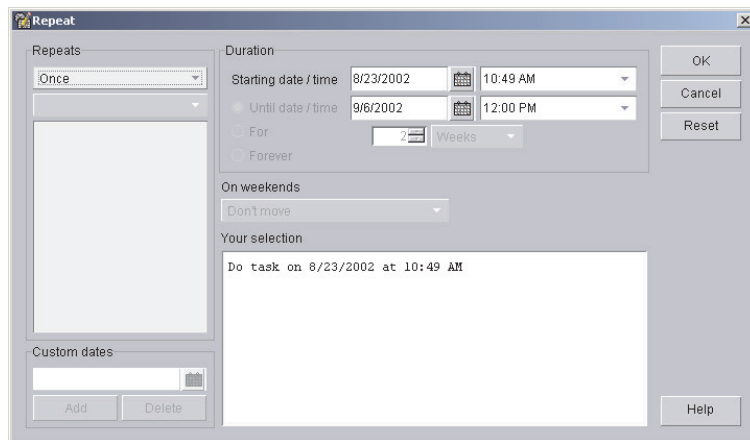


Figure 13. "Repeat" window

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 that 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.

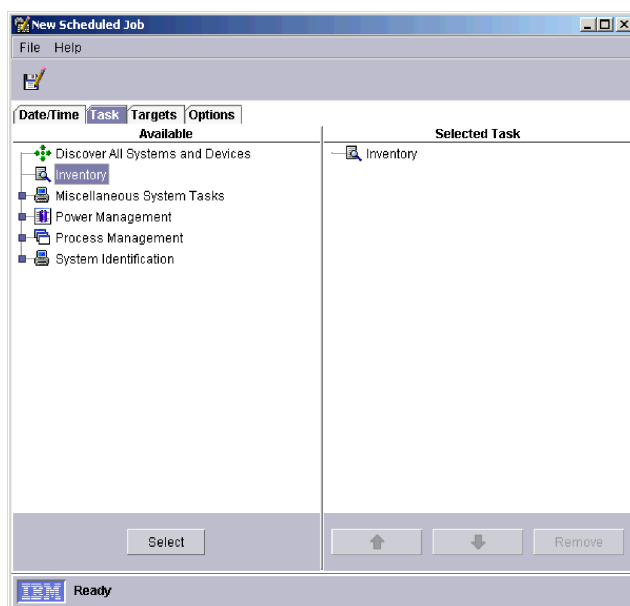


Figure 14. "New Scheduled Job" window: Tasks page

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 objects as the target, click **Specify a list of systems as targets**. In the Available pane, double-click a managed object. The managed object is added to the Selected Group pane. Repeat this procedure 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**

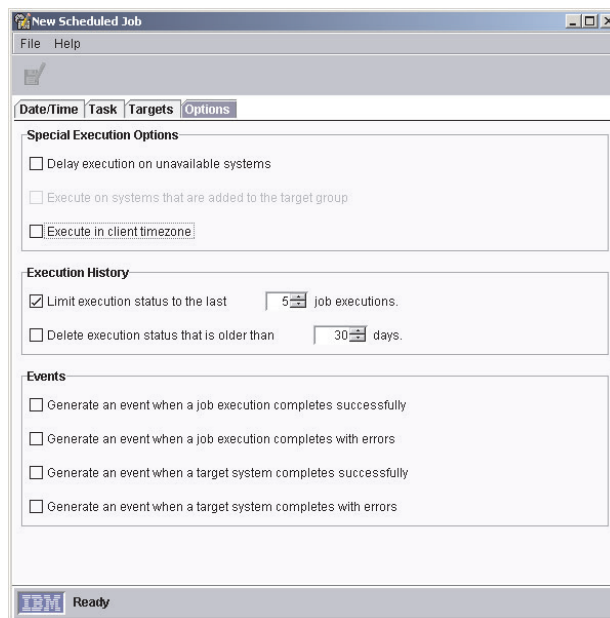


Figure 15. “New Scheduled Job” window: Options page

The following three special execution options are available:

Delay execution on unavailable systems

If you select this check box, targeted managed objects 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 object was offline at the time of job execution and comes online at a later time, the task will be executed on that managed object as soon as it comes back online.

If you do not select this check box and a targeted object 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 objects that are added to the target group are detected, and the scheduled job is activated on the managed objects 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 objects.

The one-time job stays active in Scheduler to run on any new managed object that might be added to the managed group in the future.

Execute in client time zone

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

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

In the **Execution History** group box, you can limit the number of job executions that are 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 managed objects or on individual target managed objects. For example, if a target object does not respond, the target object is completed 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 object or group

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

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

1. Drag a noninteractive task (certain tasks that you perform using Capacity Manager, Resource Monitors, and Process Management tasks, for example, support scheduling this way) onto a managed object or group. You are prompted to select whether to perform the task immediately or to schedule it.
2. Click **Schedule**. The “New Scheduled Job” window opens.

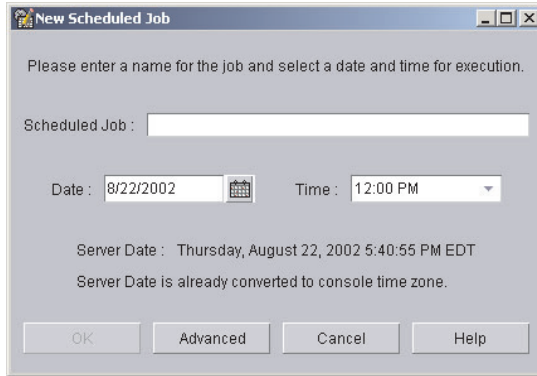


Figure 16. “New Scheduled Job” window: Scheduling a task that is activated by dragging it onto a managed object

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 that 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 42 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 11 on page 41).

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. 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. When you click a scheduled job type in the left pane, 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, is displayed in the right pane (see Figure 17).

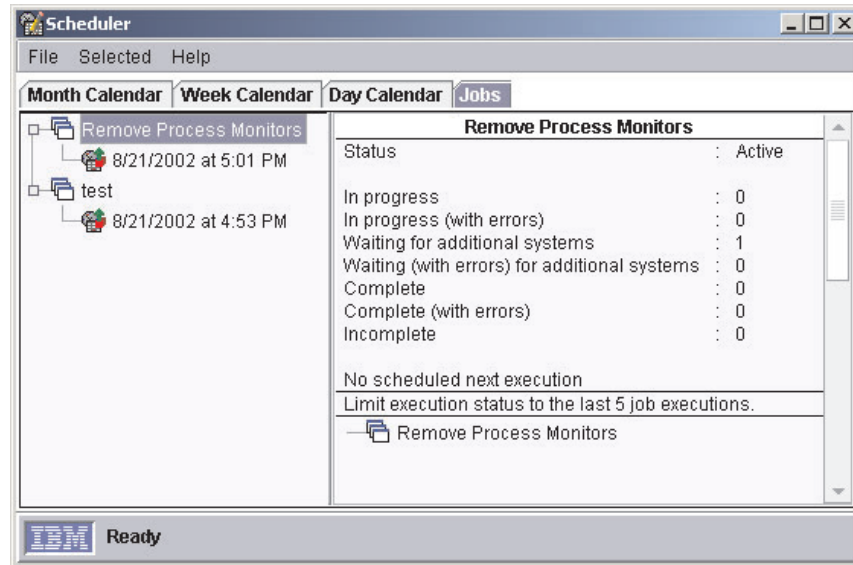


Figure 17. “Scheduler” window: Selecting a job type in the Jobs page

When you click a specific execution of a scheduled job in the left pane, information about that job execution is displayed in the right pane. The information that is displayed is identical to the information in the “Execution History” window (see Figure 18).

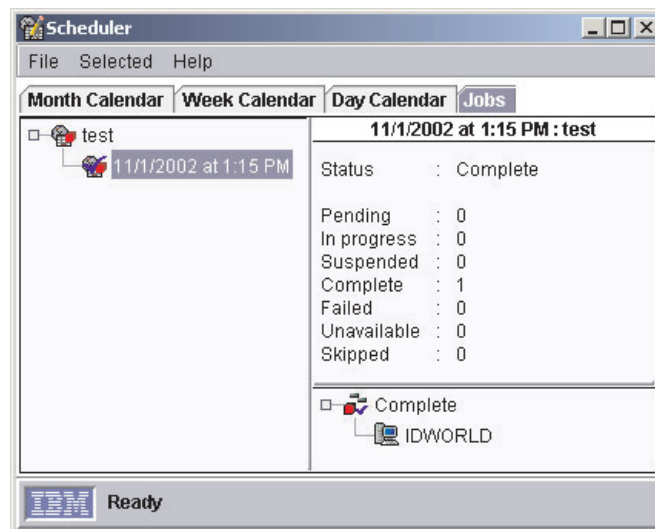


Figure 18. “Scheduler” window: Selecting a specific job execution in the Jobs page

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 allow 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 objects. Target objects are grouped together according to the status of each target for an execution and are displayed in the bottom pane of the window.

Viewing execution history logs

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

Message Browser

You can use the Message Browser to view events (alerts) that are 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 Chapter 4, “Managing and monitoring systems with event action plans,” on page 55 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 223 for more information.)

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

System Status

You can set or clear system status for the following items:

- Disk
- System
- Application
- Operating System
- Network
- User
- Security

You can set an Error, Warning, or Information level status flag for any of these items. You also can clear an existing system status flag shown on a managed object. Setting a system status flag only labels the managed object, and does not cause any other task to run.

Complete the following steps to set a system status flag on a managed object:

1. In the Groups pane, click **All Systems and Devices**. The Group Contents pane displays the managed objects.
2. Right-click a managed object in the Group Contents pane and click **System Status**. The System Status menu is displayed.

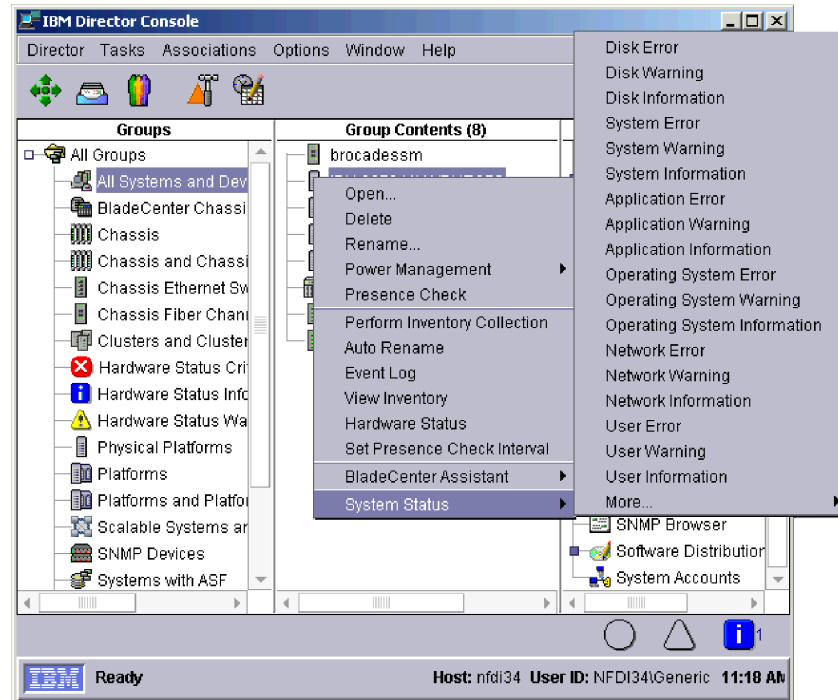


Figure 19. System Status menu

3. Click **Disk Information**. The menu closes and a Disk Information icon is displayed next to the managed object icon.

Complete the following steps to clear a system status flag on a managed object:

1. In the Groups pane, click **All Systems and Devices**. The Group Contents pane displays the managed objects.
2. Right-click the managed object in the Group Contents pane that you added the Disk Information system status to, and click **System Status**. The System Status menu is displayed as shown in Figure 19.
3. Click **Disk Information**. The menu closes and the Disk Information icon is removed from the managed object.

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 4.20 Installation and Configuration Guide*.

Note: If you want to authorize a new IBM Director Console user, you must use the tools that are 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 the 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.

Note: These defaults only affect members of the Diradmin group. These defaults do not limit the attributes of members of the Dirsuper group.

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 the 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 20. “Encryption Administration” window

These settings apply to communication between IBM Director Server and its managed objects. For information about secure communication settings between IBM Director Server and IBM Director Console or DIRCMD, see the *IBM Director 4.20 Installation and Configuration Guide*.

Note: You also must configure encryption in IBM Director Agent on the managed system.

Mass Configuration

You can use Mass Configuration to run a single task on a group of managed objects. Using mass-configuration profiles, you can quickly configure a group of managed objects. You can use Mass Configuration with the following tasks:

- Configure Alert Standard Format
- Asset ID
- Network Configuration
- Configure SNMP Agent

Creating a profile

To use Mass Configuration, you must create a profile. The following procedure uses the Configure Alert Standard Format task as an example. Complete the following steps to create a profile:

1. In IBM Director Console Tasks pane, right-click the **Configure Alert Standard Format** task and click **Profile Builder**. The “Configure Alert Standard Format: Profile Builder” window opens.

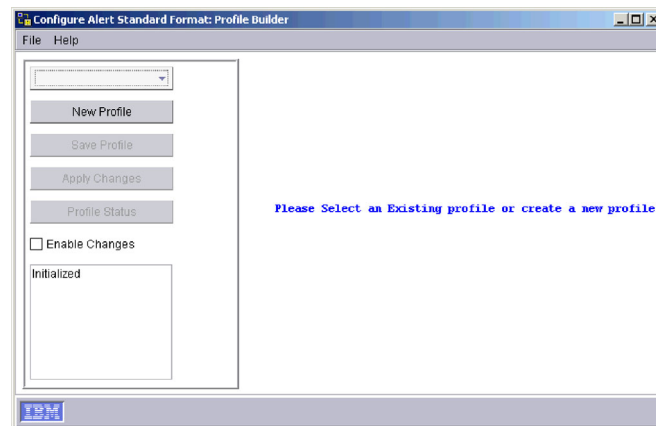


Figure 21. “Configure Alert Standard Format: Profile Builder” window

2. Click **New Profile**. The “Input” window opens.
3. Type the new profile name in the field and click **OK**. The new profile name displays in the field in the upper left of the “Configure Alert Standard Format: Profile Builder” window.

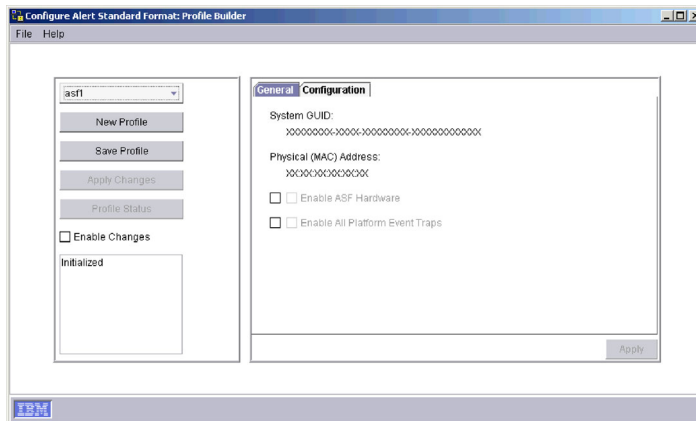


Figure 22. “Configure Alert Standard Format: Profile Builder” window, displaying a new profile

4. In the right pane of the “Profile Builder” window, edit the information as applicable. See Chapter 10, “Configure Alert Standard Format,” on page 147 for more information.
5. (Optional) Select the **Enable Changes** check box to allow other administrators to edit this profile.
6. Click **Save Profile**, then **Yes**, to save the profile.
7. Click **File** → **Close** to close the “Profile Builder” window.

Applying a profile to a group

Profiles are saved in the IBM Director Console Tasks pane underneath the task they are associated with. You can apply a profile to an individual managed object or a group.

Complete the following steps to apply a profile to a managed object or a group:

1. Expand the **Configure Alert Standard Format** task to display the task profiles.
2. Drag a profile onto a managed object or a group. The “Status” window opens and displays the status of applying the profile to each managed object in the group.
3. Click **Close** to close the “Status” window.

Managing profiles

You can edit groups associated with a profile or delete the profile using the “Profile Manager” window.

Complete the following steps to manage profiles for a task:

1. Expand the **Configure Alert Standard Format** task to display the task profiles.
2. Right-click a profile and click **Profile Manager**. The “Status” window opens.

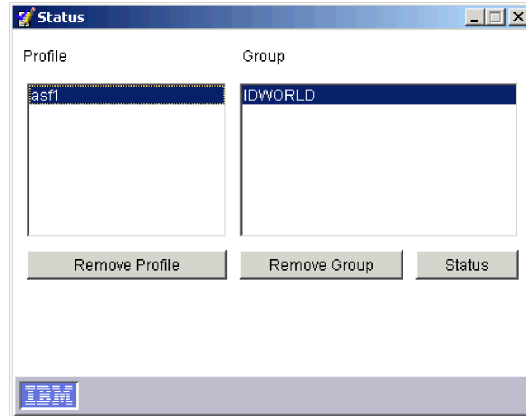


Figure 23. “Status” window

3. To remove a profile, click the profile in the **Profile** field; then, click **Remove Profile**.
4. To remove a group from the profile, click the profile in the **Profile** list and click the group in the **Group** list; then, click **Remove Group**.
5. To view the status of the profile, click **Status**. The **Profile Status** field is displayed.



Figure 24. “Status” window: Profile Status field

6. Click **Close** to close the Profile Status field and return to the “Status” window.
7. Click **X** in the right of the window bar to close the “Status” window.

Chapter 4. Managing and monitoring systems with event action plans

This chapter provides information about events and event action plans, how to plan, design, and build event action plan implementations, and how to work with existing event action plans.

You can use event action plans to specify actions that occur as a result of events that are generated by a managed object. (For more information about managed objects, see “Managed systems and managed objects” on page 33.) An event action plan is composed of two types of components:

- One or more event filters, which specify event types and any related parameters
- One or more event actions, which occur in response to filtered events

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

By creating event action plans and applying them to specific managed objects, 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 object and change a managed-object variable when a specific event occurs. You can use process-monitor events and resource-monitor events to build an event action plan. For more information, see “Viewing and working with processes, services, and device-services information” on page 197 and “Viewing available resource monitors” on page 217.

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 that you can easily identify what a specific plan does. For more tips for creating event action plans, see “Planning and designing event action plan implementations” on page 57. Also, for more information about events, event types, and extended attributes, see the *IBM Director 4.1 Events Reference*.

Note: When you first start IBM Director, the Event Action Plan wizard starts. You can use this wizard to create an event action plan also. See the *IBM Director 4.20 Installation and Configuration Guide* for more information.

How events work in the IBM Director environment

An *event* is an occurrence of a predefined condition relating to a specific managed object. There are two types of events: alert and resolution. An *alert* is the occurrence of a problem relating to a managed object. A *resolution* is the occurrence of a correction or solution to a problem.

Note: In the IBM Director product, there are tasks and features that use the word *alert* in place of the word *event*. Also, some tasks use the word *notification* instead of event.

Sources that can generate events include, but are not limited to, the following programs and protocols:

- IBM Director Agent
- Microsoft Windows event log

- Windows Management Instrumentation (WMI)
- SNMP through out-of-band communication
- Alert standard format (ASF) Platform Event Traps (PET) through out-of-band communication
- Intelligent Platform Management Interface (IPMI) Platform Event Traps (PET) through out-of-band communication
- IBM service processors through out-of-band communication

You can use these events when working with managed objects. To monitor one or more events, you must create an event filter that contains an event type from one of these sources, use the event filter as part of an event action plan, and then apply the event action plan to a managed object. Events from the Windows event log are displayed in the Windows event log tree in the Event Type Filter Builder. Events from WMI are displayed in the Common Information Model (CIM) tree.

Monitoring operating-system specific events in the IBM Director environment

If you want to monitor certain Windows- or i5/OS-specific events in the IBM Director environment, you must create an event action plan in order for IBM Director to process the events. Managed objects running Windows or i5/OS can generate the following events:

Windows-specific event types	i5/OS-specific event types
<ul style="list-style-type: none"> • Windows event log • (Optional) A subset of the following CIM events: <ul style="list-style-type: none"> – Windows event log – Windows services – Windows registry • (Optional) DMI 	Msgq

Even though these events are generated by their respective operating systems (or an optional layer that is installed on the operating system), IBM Director does not process these events unless you create an event action plan to do so. When you install IBM Director, it has one predefined active event action plan: Log All Events. However, this event action plan does *not* log these Windows- or i5/OS-specific events. You must create an event action plan with a simple event filter that contains the event types for one or more of these events. Then, you must apply this event action plan to the managed object running Windows or i5/OS.

When IBM Director Agent starts on a managed object running Windows, the `twgescli.exe` program starts, too. This program listens for IBM Director Server to send a message to IBM Director Agent that an event action plan has been applied to that managed object. If the event action plan includes a simple event filter that contains the event types for any of the Windows-specific events, IBM Director appropriates these events for its own use. This is called *event subscription*. The `twgescli.exe` program subscribes to the event types that are specified in the event action plan and translates the Windows-specific events into an IBM Director event type. Then, the program forwards the events to the management server from which the event action plan was applied.

When IBM Director Agent starts on a managed object running i5/OS, the process is the same with comparable code to `twgescli.exe` that is included in the IBM Director Agent for i5/OS.

Processing an event in the IBM Director environment

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

IBM Director completes the following steps to determine which event actions to execute:

1. The managed object generates an event and forwards the event to all the management servers that have discovered the managed object (except for some events, such as those that are 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 event and determines which managed object generated the event and which group or groups the managed object belongs to.
3. IBM Director Server determines whether any event action plans are applied to the managed object or to any of the groups of which the managed object 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

To plan and design an event action plan, you must determine what the goal of the event action plan is. Consider which managed objects you intend to target with the event action plan. You can target all managed objects, a subgroup of managed objects, or a specific managed object.

You can structure event filters and event actions in different ways. This section presents 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 that are presented.

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

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

- What do you want to monitor on most or all of the managed objects of the same type as a whole? This answer determines the grouping and event filters for your event action plans.
- How will you group your managed objects as smaller groups, according to the additional events you want to monitor? The smaller groups are usually based on the following criteria:
 - Managed-object manufacturer, for vendor-specific events
 - Function of the managed object, for services and resources specific to that function
- What type of managed objects are you monitoring?
- What is the function of the managed object?

- What are the key monitors for the managed object?
- Are there other managed objects for which you want to use the same monitors?

Grouping managed objects

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

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

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

By manufacturer

Each managed-object manufacturer has its own event action plans. Many organizations have managed objects 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 object.

By function

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

By resources

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

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

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 objects or only certain software running on these managed objects.

A structure based on managed-object function

Servers performing different functions must be managed differently.

A structure based on the type of event

Some structures based on the type of event 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, you can structure your event action plans and event filters according to the 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 that you can use to determine whether to include an event with other events:

- All managed objects that are targeted for the filter are able to generate all events that are included in the filter. If the managed object does not generate the event for which the filter is defined, the filter will not be effective on that managed object.
- The event actions that will be used to respond to the event are the same for all targeted objects.
- The other event filter options besides the event type are common for all targeted objects. 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 are not generated by all managed objects. In such instances, you can apply the event action plan to those managed objects, but it will have no effect. For example, if an event filter is based on a ServeRAID event and that event action plan is applied to managed objects 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 you can reduce the number of event action plans you have to build and maintain.

All currently available event types are displayed in the tree on the Event Type page in the “Event Filter Builder” window. The currently installed tasks and extensions publish their events in the Event Type tree when IBM Director Server or IBM Director Agent starts.

Note: Whether the events are published when IBM Director Server or IBM Director Agent starts depends on the tasks or extensions and how they are implemented.

If you add an extension to your IBM Director installation, the extension might publish its events either when it is added to the installation or when the extension sends its first event. If the extension publishes when it sends its first event, *only* that event is published.

Building an event action plan

Building an event action plan consists of the following steps:

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

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

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

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. For more information, see “Planning and designing event action plan implementations” on page 57.

Creating a new event action plan

Complete the following steps to create a new event action plan:

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

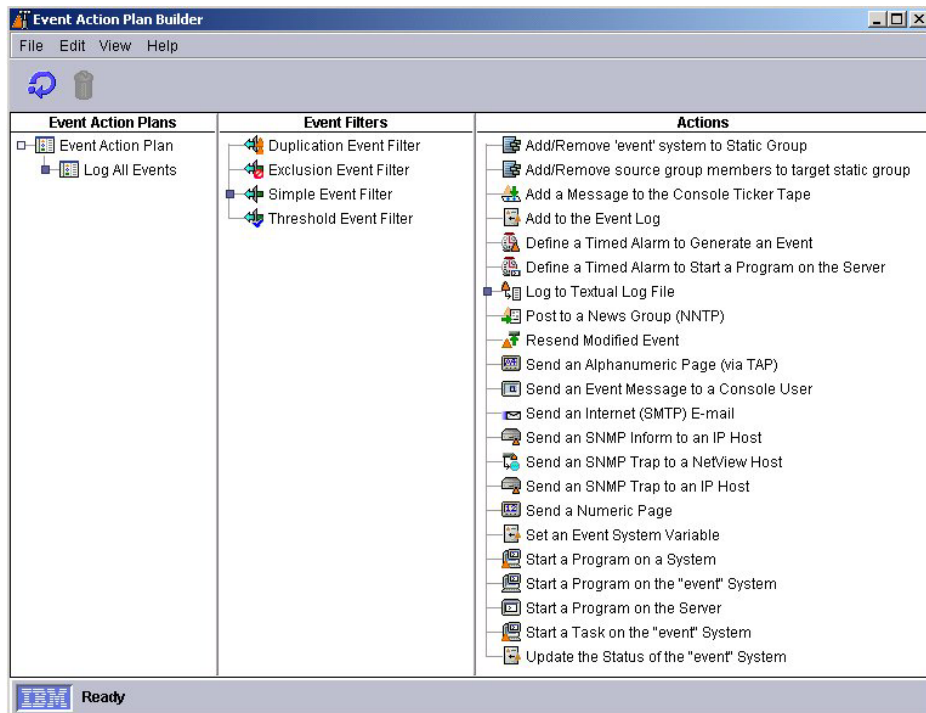


Figure 25. “Event Action Plan Builder” window

The “Event Action Plan Builder” window contains three panes:

Event Action Plans pane

Lists event action plans. One default event action plan, Log All Events, is included with IBM Director. For more information about Log All Events, see “Monitoring operating-system specific events in the IBM Director environment” on page 56. 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 that are displayed under the applicable filter types. Expanding the **Simple Event Filter** tree

displays, in addition to any customized simple event filters that were created, the preconfigured event type filters. For more information, see “Creating event filters.”

Actions pane

Lists event action types, with customized actions that are displayed under the event action types. For more information, see “Customizing event actions” on page 66.

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. Continue to “Creating event filters.”

Creating event filters

An event filter processes only the events that are specified by the filter and ignores all other events. For information about structuring event filters, see “Structuring event filters” on page 59. In the “Event Action Plan Builder” window, the Event Filters pane displays the event filters that are listed in Table 11.

Table 11. Event filters

Event filter	Description
Simple Event	<p>Simple event filters are general-purpose filters; most event filters are this type. When you expand this tree, any customized simple event filters that you have created are displayed. Also, the following predefined, read-only event filters are displayed:</p> <ul style="list-style-type: none"> • 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 <p>Some of these predefined filters use the severity of events to determine which events they will allow to pass through; other filters 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 object, except for Windows-specific and i5/OS-specific events. For more information about these events, see “Monitoring operating-system specific events in the IBM Director environment” on page 56. Using one of these preconfigured event filters ensures that the correct event type or event severity is preselected.</p> <p>If you want to see what events are included in a predefined event filter, double-click that predefined event filter in the Event Filters pane. The “Simple Event Filter Builder” window opens, and the Event Filter Builder notebook is displayed. Select the applicable notebook page to view the selected event filters. For example, click the Severity tab to view the selections for the Critical Event filter. You cannot change predefined event filters; they are read-only. However, you can make changes and click File → Save As to save the modified event filter with another name.</p>

Table 11. Event filters (continued)

Event filter	Description
Duplication Event	<p>Duplication event filters ignore duplicate events, in addition to the options that are available in the simple event filters.</p> <p>To use this filter, you must specify the number of times (Count) that the same event is ignored during a specified time range (Interval). Then, this filter processes the first event that meets the criteria that are defined for this filter. Only the first event triggers the event actions that are associated with this event filter. For the associated event actions to be triggered again, one of the following conditions must be met:</p> <ul style="list-style-type: none"> • The value that is specified in the Count field must be exceeded. • The time range that is specified in the Interval field must elapse. • The value that is specified in the Count field must be exceeded by 1 (Count+1) within the time range that is specified in the Interval field. <p>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 that 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 exceeded during the specified interval.</p>
Exclusion Event	<p>Exclusion event filters exclude certain event types, in addition to the simple event filter options. Using this filter, you define the criteria of the events to exclude.</p>
Threshold Event	<p>A threshold event filter processes an event after it occurs a specified number of times within a specified interval, in addition to the simple event filter options.</p> <p>An event that meets the criteria that are defined in this filter triggers associated actions only after an event meets the criteria for the number of times that are 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.</p> <p>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.</p>

Complete the following steps to create the event filters:

1. In the Event Filters pane, double-click an event filter type. The applicable “Event Filter Builder” window opens and the Event Filter Builder notebook is displayed.

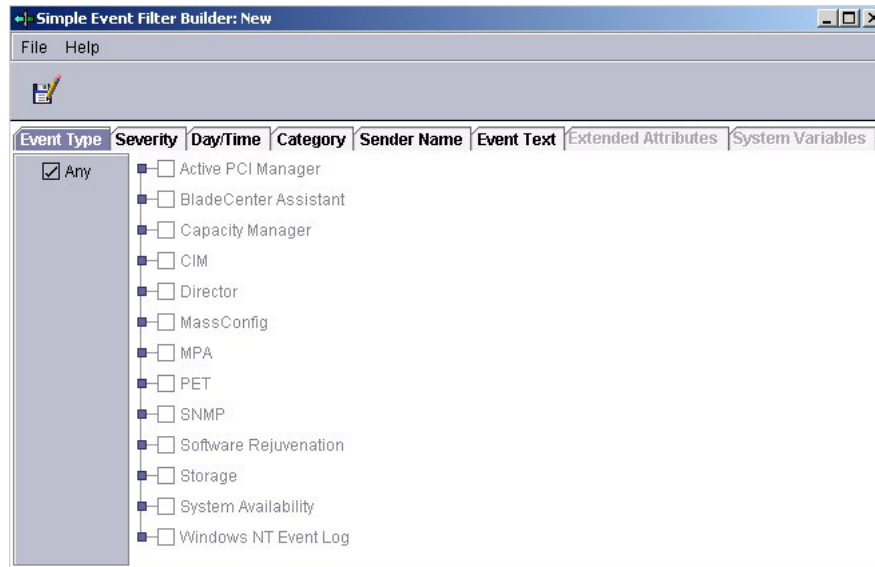


Figure 26. “Simple Event Filter Builder” window: Event Type page

Note: 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.

2. Complete the applicable fields for the event filter that you want to create.

Note: By default, the **Any** check box is selected for all filtering categories, indicating that no filtering criteria apply. For more information about the **Any** check box, see Table 12 on page 64.

Depending on the event filter type that you selected, the “Event Filter Builder” window contains some or all of the pages that are listed in Table 12 on page 64.

Table 12. Event Filter Builder notebook pages

Page	Description
Event Type	<p>Use the Event Type page to specify the source or sources of the events that are to be processed. This tree is created dynamically; entries are added by tasks and as new alerts are received. Entries in the tree can be expanded to display suboption events.</p> <p>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.</p> <p>By default, the Any check box is selected, meaning that none of the events that are listed are filtered, except for Windows-specific and i5/OS-specific events. For more information about these events, see “Monitoring operating-system specific events in the IBM Director environment” on page 56. 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 key.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. When you select a root option in the Event Type tree, all suboption events are selected as well. For example, when you select MPA in the “Simple Event Filter Builder” window, all Component, Deployment, Environmental, and Platform suboption events are selected also. <p>If additional event types are published after you create the event filter, the newly available event types are included in your event filter only if the new event types are suboption events of an event type that you selected. However, if you want to include a newly published event type that is not a suboption event, you must update the event filter by selecting the new event type. For more information about event publishing, see “Structuring event filters” on page 59.</p> 2. The event types for BladeCenter events are displayed under MPA, except for BladeCenter Deployment wizard-specific events, which are displayed under BladeCenter Assistant.
Severity	<p>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.</p> <p>When you select more than one severity, they are joined together using logical OR. The source of the event determines what severity the event is. Generally, the severity levels have the following meanings:</p> <p>Fatal The event caused a failure and must be resolved before the program or component is restarted.</p> <p>Critical The event might cause a failure and must be resolved immediately.</p> <p>Minor The event is not likely to cause immediate program failure but should be resolved.</p> <p>Warning The event is not necessarily problematic but might warrant investigation.</p> <p>Harmless The event is for information only. Most events of this severity do not indicate potential problems. However, offline events are categorized as harmless, and these events <i>can</i> indicate potential problems.</p> <p>Unknown The application that generated the event did not assign a severity level.</p>

Table 12. Event Filter Builder notebook pages (continued)

Page	Description
Day/Time	<p>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.</p> <p>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.</p> <p>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 object 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.</p>
Category	<p>Use the Category page to specify an event filter according to the status of an event (alert or resolution of a problem). However, not all events have resolutions.</p>
Sender Name	<p>Use the Sender Name page to specify the managed object to which the event filter will apply. Events that are generated by all other managed objects will be ignored. By default, the Any check box is selected, indicating that events from all managed objects (including IBM Director Server) are processed by the event filter.</p> <p>Initially, only IBM Director Server is shown in the list. As other managed objects generate events, such as when a threshold is exceeded, this list is added to dynamically. If you anticipate that other managed objects will generate events, you also can type managed-object names into the field and click Add to add them.</p>
Extended Attributes	<p>Use the Extended Attributes page to specify additional event-filter criteria using additional keywords and keyword values that you can associate with some categories of events, such as SNMP. This page is available only when you clear the Any check box on the Event Type page and select certain entries from that page.</p> <p>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.</p> <p>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, below the Sender Name category.</p>
System Variables	<p>Use the System Variables page to further qualify the filtering criteria by specifying a system variable. This page is available only if there are one or more system variables. A system variable consists of a user-defined pairing of a keyword and value that are known only to the local management server. See “Viewing and changing system variables” on page 73 for more information.</p> <p>Note: These user-defined system variables are not associated with the system variables of the Windows operating system.</p>
Event Text	<p>Use the Event Text page to specify event message text to associate with the event.</p>

3. Click **File** → **Save As**. The “Save Event Filter” window opens.
4. Type a name for the filter. When you are naming an event filter, the name should indicate the type of events for which the filter is targeted and 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 unrecoverable storage events that occur on a weekend should be named to reflect that.
5. Click **OK** to save the filter. The new filter is displayed in the Event Filters pane under the applicable filter type.
6. (Optional) Create additional event filters for use in a single event action plan. Repeat step 1 on page 62 through step 5.
7. In the Event Filters pane, drag the event filter onto the event action plan (in the Event Action Plans pane) that you created in “Creating a new event action plan” on page 60. The event filter is displayed under the event action plan.
8. If you have created additional event filters that you want to use in this event action plan, repeat step 7.
9. When the event filter is completed, go to “Customizing event actions.”

Customizing event actions

You must customize an event action to specify which action or actions that you want IBM Director to take as a result of the occurrence of an event. The Actions pane displays the predefined event action types that are listed in Table 13. With the exception of **Add to Event Log**, each event action type must be customized.

Table 13. Event action types

Event action type	Description
Add/Remove “event” system to Static Group	Adds a managed object to or removes a managed object from a specified static group when the managed object logs a specific event.
Add/Remove source group members to target static group	Adds all specified managed objects in a source group to a target group or removes all specified managed objects 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 IBM Director 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 Network News Transfer Protocol (NNTP).
Resend Modified Event	Creates or changes an event action that modifies and resends an original event.
Send an Alphanumeric Page (via TAP)	(Windows only) 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.

Table 13. Event action types (continued)

Event action type	Description
Send an Internet (SMTP) E-mail	Sends a Simple Mail Transfer Protocol (SMTP) e-mail message.
Send an SNMP Inform to an IP host	Sends an SNMP inform request to a specified IP host.
Send an SNMP Trap to a NetView Host	Generates an SNMP trap and sends it to a specified NetView® host using a TCP/IP connection to the host. If delivery of the SNMP trap fails, a message is posted in the history log of the managed object.
Send an SNMP Trap to an IP Host	Generates an SNMPv1 or SNMPv2c trap and sends it to a specified IP address or host name.
Send a Numeric Page	(Windows only) 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 objects on which IBM Director Agent is installed.
Start a Program on the “event” System	Starts a program on the managed object 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 object that generated the event.
Update the Status of the “event” System	When the selected resource status generates an event, causes a status indicator beside the icon of the managed object that is associated with the resource to be set or cleared according to your specification.

Complete the following steps to customize an event action:

1. In the Actions pane, double-click an event action type. The “Customize Action” window opens. The example that is shown in Figure 27 uses the Add a Message to the Console Ticker Tape event action type.

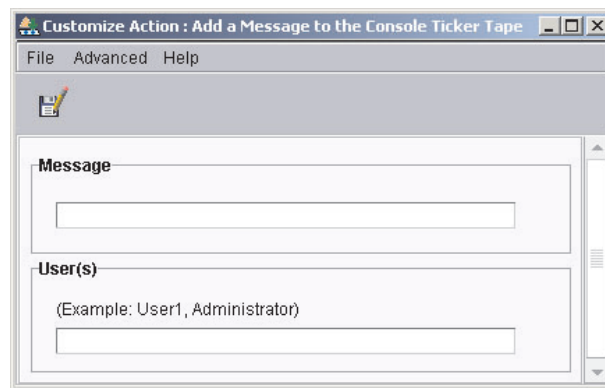


Figure 27. “Customize Action” window: Customizing an action for a ticker-tape alert

2. Complete the fields for the action type. For some event action types, 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. Table 14 describes the available event data substitution variables.

Table 14. 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 they are supplied by the event.
&type	Provides the event-type criteria that are used to trigger the event. For example, the event that is generated when a managed object goes offline is of type <code>Director.Topology.Offline</code> . 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 object 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 object from which the event was sent. This variable returns null if the name is unavailable.
&group	Provides the group to which the target object belongs and is being monitored. This variable returns null if the group is unavailable.
&category	Provides the category of the event, either Alert or Resolution. For example, if the managed object goes offline, the category is Alert. If the managed object goes online, the category is Resolution.
&pgmtype	Provides a dotted representation of the event type using internal type strings.
×tamp	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 object that is associated with the event.
&prop: <i>filename</i> # <i>propname</i>	Provides the value of the property string <i>propname</i> from property file <i>filename</i> (relative to <code>IBM\Director\classes</code>).
&sysvar: <i>varname</i>	Provides the event system variable <i>varname</i> . This variable returns null if a value is unavailable.
&slotid: <i>slot-id</i>	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, or cyclic redundancy check (CRC), of the event data (good event-specific unique ID).

Table 14. Event data substitution variables (continued)

Variable	Description
&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 that has a localized label that matches otherstring. A <i>detail slot</i> is a record in an event detail. For example, an event has one event detail that has an ID of key1 and a value of value1. You can use the substitution variable &slotid:key1 to obtain the value value1. You also can use &key1 to obtain the value value1. In the description above, otherstring is a placeholder for the user-defined event detail ID. However, if the passed ID is not found, “Not applicable” is returned.

3. Click **File** → **Save As**. The “Save Event Action” window opens.
4. Type a name for the event action. An event action name 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, begin the event action name with Pager; if the event action involves sending a message to a phone, begin the event action name with Phone. Using such a naming convention ensures that entries are grouped conveniently in the “Event Action Plan Builder” window.
5. Click **OK** to save the event action. The new action is displayed in the Actions pane under the applicable action type.
6. (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 event action, the ticker tape displays the message in 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, and then click **Test**. The event action occurs.

Note: You can verify the test result by following the steps described in “Enabling and viewing an event action history” on page 73.

7. (Optional) Customize additional event actions for use in a single event action plan. Repeat step 1 on page 67 through step 6.
8. 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. See the Event Action Plan pane in Figure 28 on page 70 for an example of an event action plan with an event filter and event action assigned to it.

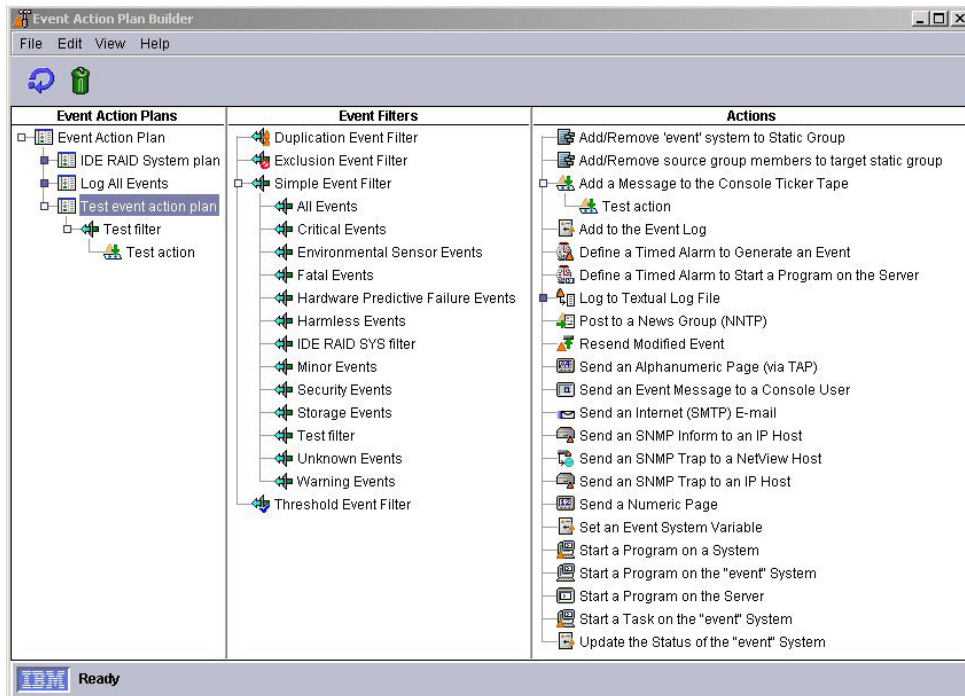


Figure 28. “Event Action Plan Builder” window: Event action plan with an event filter and event action assigned to it

9. If you have created additional event actions that you want to use in this event action plan, repeat step 8 on page 69.
10. Click **File** → **Close** to close the Event Action Plan Builder.
11. To activate the event action plan, go to “Activating the event action plan” on page 72.

For examples of customizing event action types to create event actions, see the following sections:

- Creating an e-mail notification event action (see page 70)
- Creating a pop-up message notification event action (see page 71)

Example: Creating an e-mail notification event action

In this example, an event action is customized to send an e-mail notification. Typically, this is the first type of event action that IBM Director administrators set up. This event action is flexible; 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 29 on page 71 for example values.

Note: When the Body text is generated by the event action, the Body text contains not only the text that you specify, but all the event-generated text. Many pager and phone services that support Simple Mail Transfer Protocol (SMTP) messages limit the number of characters that can be sent in a message. The resulting message might be split into multiple

messages or truncated. For this reason, keep the text of the message brief.

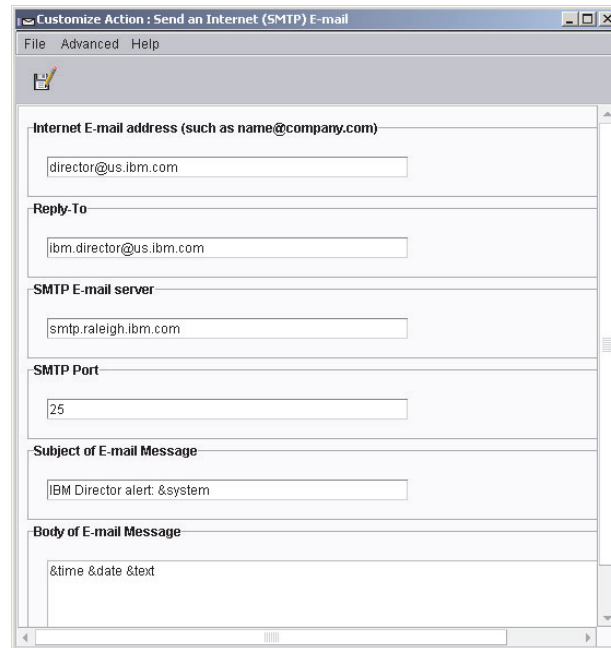


Figure 29. “Customize Action” window displaying example values

3. Click **File** → **Save As** to save the event action. The “Save Event Action” window opens.
4. Type a name for the event action. In this example, the name `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 that 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.

Example: Creating a pop-up message notification event action

In this example, an event action type is customized to use 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 object currently running the management console. However, because you cannot always be sure that the person who needs to receive the message will be using a managed object running IBM Director Console, you can use the `NET SEND` command to send a pop-up message.

Complete the following steps to configure a `NET SEND` command to send a pop-up message to a managed object named `C3PO`.

Note: This procedure requires that the Microsoft Windows Messenger service be running.

1. Determine the IP address or host name of the Windows 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 C3P0 "IBM Director: &system generated a &severity &category"`
where
 - `cmd /c` indicates to the Windows operating system on the management server to close the window automatically when the command is completed.
 - `C3P0` is the Windows 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 object that generated the event. See Table 14 on page 68 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, because `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, the name `Net send popup to C3P0` 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.

Activating the event action plan

Complete the following steps to associate the event filter and event actions to the event action plan and then activate it:

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

Working with existing event action plans

This section provides the following information about how to work with existing event action plans:

- Modifying an event action plan
- Viewing and changing system variables
- Enabling and viewing an event action history
- Viewing associations
- Restricting an event action plan
- Exporting and importing event action plans

Modifying an event action plan

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

If you modify an event filter or an event action that is 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 that is used in an existing event action plan, the following warning is displayed.

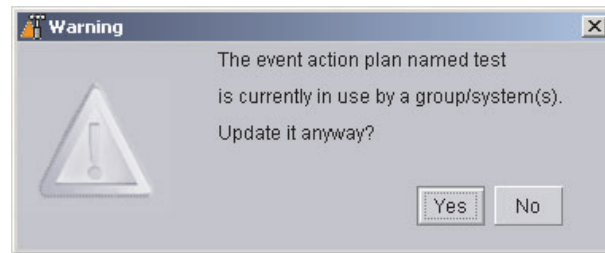


Figure 30. Prompt when modifying an existing event action plan

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

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 elapses 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 refer to system-variable names and values wherever event data substitution is allowed. See “System Variables” in Table 12 on page 64 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 objects and groups. In IBM Director Console, click **Associations** → **Event Action Plans**. If a managed object or group has an event action plan assigned to it, you can expand

the managed object or group and expand the **Event Action Plan** folder to view the specific event action plans that are applied to the managed object or group.

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

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 that are applied to the group.

Restricting event action plans

You can restrict whether an event action plan applies both to events that are received by all managed objects in a group and to events that are received by one or more managed objects in the group, or just to the events that are received by all managed objects in the group. If an event action plan is restricted, all managed objects 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 object or group that has the event action plan that 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 export and import 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 management server.

Import and export event action plans in archive format for two reasons:

- To move event action plans from one management server to another
- To back up event action plans on a management server

HTML Creates a detailed listing of the selected event action plans, including their filters and actions, in an HyperText Markup Language (HTML) format.

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

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 that 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 select, the applicable window opens (for example, if you select **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 management 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 that you transferred in step 1.
5. Click **OK** to begin the import process. The “Import Action Plan” window opens, displaying the event action plan that is to be imported.
6. Click **Import** to complete the import process. If the event action plan was previously assigned to managed objects or groups, you can preserve those assignments during the import process.

Part 2. IBM Director Console tasks

Chapter 5. Active PCI Manager	79
Chapter 6. Asset ID	93
Chapter 7. BladeCenter Assistant	95
Chapter 8. Capacity Manager	127
Chapter 9. CIM Browser	143
Chapter 10. Configure Alert Standard Format	147
Chapter 11. DMI Browser	153
Chapter 12. Event Log	155
Chapter 13. File Transfer	159
Chapter 14. Hardware Status	163
Chapter 15. Inventory	167
Chapter 16. Management Processor Assistant	175
Chapter 17. Microsoft Cluster Browser	193
Chapter 18. Network Configuration	195
Chapter 19. Process Management	197
Chapter 20. Rack Manager	207
Chapter 21. Remote Control	211
Chapter 22. Remote Session	215
Chapter 23. Resource Monitors	217
Chapter 24. ServeRAID Manager	225
Chapter 25. SNMP Browser and SNMP devices	227
Chapter 26. Software Distribution	233
Chapter 27. Software Rejuvenation	257
Chapter 28. System Accounts	267
Chapter 29. System Availability	269

Chapter 5. 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, and failover 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. As of the date of this document, FTMI is implemented according to CIM version 2.3.

Note: FTMI works only with certain network adapters and IBM xSeries servers; it does not work with all network adapters and IBM servers that are supported by IBM Director. For detailed support information, see the *IBM Director 4.20 Installation and Configuration Guide*.

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 type of 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 adapter teaming or load balancing (adaptive, bidirectional, or transmit). The collective, single adapter is also sometimes referred to as a virtual adapter or virtual network interface card (NIC).

Spare group

In this type of group, only one adapter in the group is online at any time. The remaining adapters in the group are turned 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 or failover teaming.

Starting the FTMI subtask

To start the FTMI 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.

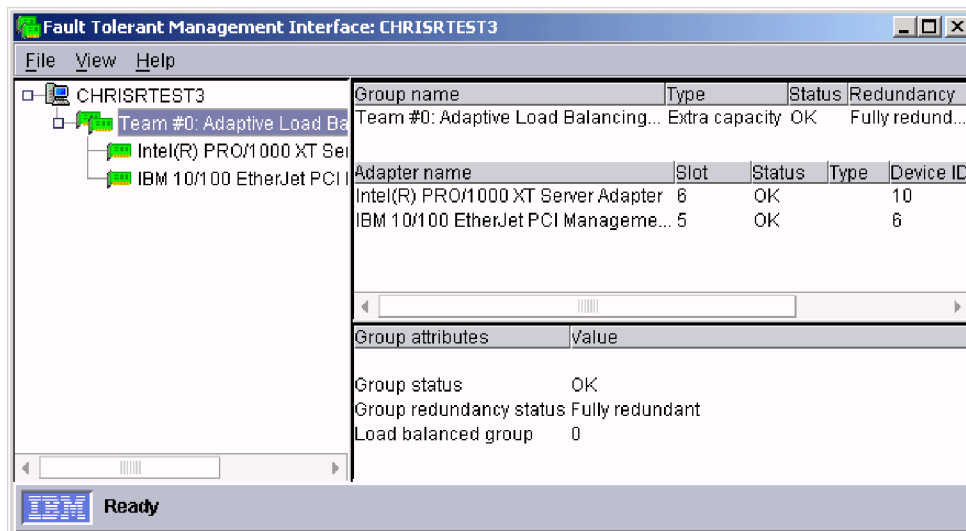


Figure 31. “Fault Tolerant Management Interface” window

In the “Fault Tolerant Management Interface” window, the left pane displays a tree structure of the fault-tolerant groups and fault-tolerant adapters that are defined for the managed system. The icon for each fault-tolerant group or adapter indicates whether the adapter is online or offline, 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 that is selected, multiple tables of information might be displayed.

FTMI updates the icons and table information whenever offline, online, or failover operations occur for an adapter. Additionally, you can refresh the window 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 Fault Tolerant Management Interface window. Click an adapter icon to display its properties in the right side 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 first table in the upper-right pane displays the name of the group, its type, status, redundancy, and the number of adapters in the group. The second table displays a list of fault-tolerant adapters that are contained in the group. Each adapter row displays the adapter name, slot number, status, type, and device ID.

The table in the lower-right pane displays additional attributes about the fault-tolerant group. It displays the status of the group, its redundancy status, and whether the group is load balanced. For an extra-capacity group, 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, and failover operations for an adapter, 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 update can take several seconds.

Additionally, you can use FTMI CIM queries and the “Event Filter Builder” window to create IBM Director alerts that are used in event action plans to notify you whenever an adapter goes offline. For details, see “FTMI CIM queries” on page 82.

After an adapter has gone offline, you can replace the adapter by ejecting it and installing a new one in its place. In this scenario, you 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 update can take several seconds.

Additionally, you can use FTMI CIM queries and the “Event Filter Builder” window to create IBM Director alerts that are used in an event action plan to notify you 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 that 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 update can take several seconds.

Additionally, you can use FTMI CIM queries and the “Event Filter Builder” window to create IBM Director alerts that are used in an event action plan to notify you 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.

FTMI CIM queries and CIM events

FTMI comes with a set of CIM queries and CIM events that you can use to create event filters in the “Event Filter Builder” window. For more information about using the Event Filter Builder and event action plans, see Chapter 4, “Managing and monitoring systems with event action plans,” on page 55.

FTMI CIM queries

The FTMI CIM queries are in the “Event Filter Builder” window under the **CIM** option and the **Fault Tolerant Management Interface Queries** suboption.

FTMI CIM queries that are used in an event filter are invoked every 60 seconds to determine whether an event should be reported. For this reason, the FTMI CIM queries affect performance, and you should carefully consider the events that you want to monitor automatically.

Table 15 lists the FTMI CIM queries for fault-tolerant adapters and fault-tolerant groups.

Table 15. 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.

FTMI CIM events

The FTMI CIM events are in the “Event Filter Builder” window under the **CIM** option and the **Fault Tolerant Management Interface Events** suboption. FTMI CIM events occur every time the associated event occurs. FTMI CIM events exist so that FTMI can properly update the interface as required. However, you can create event filters that use FTMI CIM events if you want.

Table 16 lists the FTMI CIM events.

Table 16. FTMI CIM events

FTMI CIM event	Occurs when
FTMI Instance Modification	A CIM provider notifies FTMI that the status of an adapter or group has changed.
FTMI Refresh	FTMI updates the graphical user interface to reflect a change to an adapter or group.

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 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 88.
- An Add Card wizard that determines the most suitable slot in which to insert a new adapter. For details, see “Adding adapters” on page 90.

Note: Slot Manager works only with certain IBM xSeries servers; it does not work with all IBM servers that are supported by IBM Director. For detailed support information, see the *IBM Director 4.20 Installation and Configuration Guide*.

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

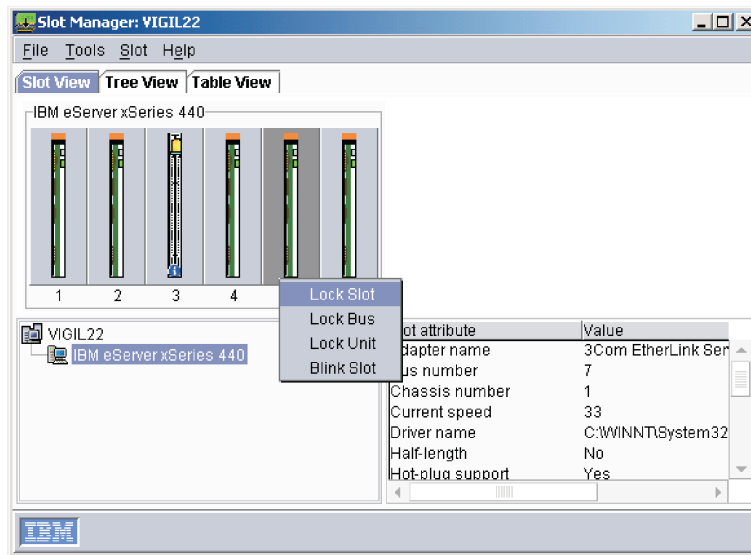


Figure 32. “Slot Manager” window: Slot view page

The “Slot Manager” window displays information about how the PCI and PCI-X adapters are connected in the system chassis and in any 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 that you want to see.

Note: The “Slot Manager” window does not display information about built-in PCI adapters or 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 megahertz (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 in the managed system (see Figure 32). 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.

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 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.

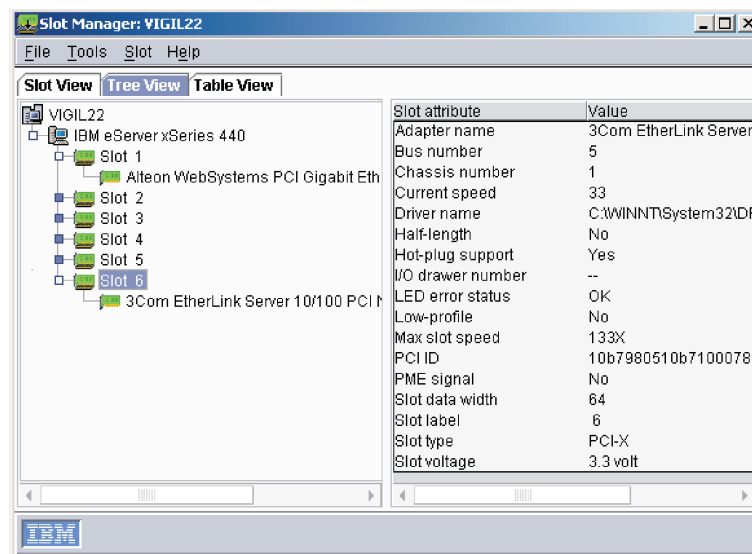


Figure 33. “Slot Manager” window: Tree view page

The right pane shows the attributes for the item (system chassis, I/O expansion drawer, slot, or adapter, but not managed system) that is 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 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.

Chassis	I/O drawer	Slot label	Slot speed	Slot max sp...	Slot type	Hot-plug slot	Adap
1	--	1	66	66X	PCI-X	Yes	Alteon V
1	--	2	66	66X	PCI-X	Yes	Ethern
1	--	3	33	100X	PCI-X	Yes	3Com E
1	--	4	33	100X	PCI-X	Yes	3Com E
1	--	5	33	133X	PCI-X	Yes	3Com E
1	--	6	33	133X	PCI-X	Yes	3Com E

Figure 34. “Slot Manager” window: Table view page

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. Slot Manager does not retain any changes that you make to the sort order after you exit the program or use the Refresh function.

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 there is a better slot location 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.

Slot error status

When the Attention light-emitting diode (LED) is flashing for a slot, you can use the Slot Manager to determine the cause of the error. Slot Manager reports the error status of a slot in the following 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 displays 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 light the Attention LED for several hardware problems, but Slot Manager cannot turn it off.

A slot can have any of the following error statuses:

- 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 .

Figure 35 shows examples of the slot icons in the Slot view and Tree view that indicate an error status.

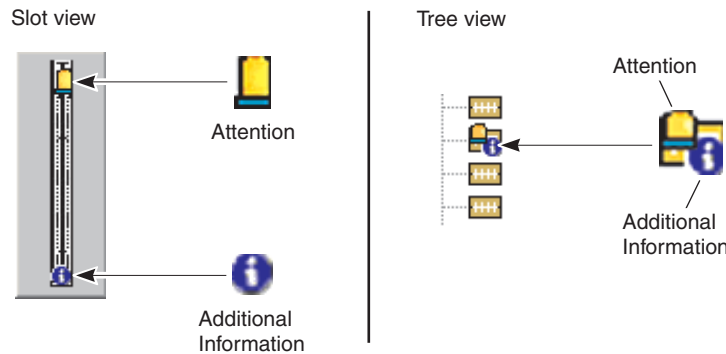


Figure 35. Examples of slot error status

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 (or slots) or bus is not included in the solution. To lock a slot, in the Tree or Slot view, right-click the slot that you want to lock; then, click **Lock slot**. To lock a bus, in the Tree or Slot view, right-click the bus that 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 that 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 that is 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 flash the Attention LED that is 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 applicable. The 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 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 the Attention LED 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 that are 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.

However, if the PCI optimization routine cannot find a solution that places adapters in buses running at the same speed and mode, the routine relaxes the mode rules. When this happens, the Analyze function looks for a solution that can improve the system PCI optimization, even though it will not be optimal.

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 and 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 87 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, make sure 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 following sections describe the performance issues that the PCI optimization routine can detect.

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 that is being analyzed:

- The adapters that are installed on any bus segment are not capable of operating at the same speed.
- A bus is exceeding the number of adapters that 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 that is being analyzed:

- A 32-bit wide bus contains a 64-bit PCI-X adapter.
- All adapters that are 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 adapters 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.

Important: (Managed systems running SUSE Linux Enterprise Server 8 only)
Advanced Configuration and Power Interface (ACPI) hot-plug operations are not supported. You must turn off these managed systems before you move an adapter to another slot.

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 at. The system must be turned off when you move the adapter so that the bus speed is reset correctly 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. Before using the Add Card wizard, you might want to run the Analyze function and correct any noted performance issues.

To start the Add Card wizard, click **Tools** → **Add Card wizard** from any view (Slot, Tree, or Table).

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 that 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 those issues. For details, see “Analyzing PCI performance” on page 88.

Notes:

1. Slot Manager cannot validate the information that is gathered by the Add Card wizard against the adapter until the adapter is installed in the system. If you provide the wrong adapter information in the wizard, the adapter might not work correctly 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, make sure that the affected slot is locked in Slot Manager so that it is not considered by the Analyze function.

Choosing an adapter and the slot characteristics

Use the first window of the Add Card wizard to designate the type of adapter that you plan to use. The left pane provides a list of adapters that are known to Slot Manager. You can either click the name of the adapter that you plan to use or, if it is not listed, click **Adapter Not Listed**. The right pane provides the values that the wizard will use for the selected adapter.

In the bottom portion of this window, there are two check boxes that are used to refine the slot selection search. Select the **Suggest only slots with hot-plug support** check box to make the wizard return only those slots that support hot-plug operations.

Note: Although a slot supports hot-plug operations, in some cases it is still necessary to restart the system to resolve bus-speed mismatch errors. This scenario occurs when the speed of the hot-added adapter is slower than that which the bus is operating at. In this case, although the slot supports hot-plug operations, you must restart the system so that the adapter runs at the same speed as the bus.

Select the **Suggest only slots that will not require a restart** check box to further limit the slot selection to only those hot-plug slots that will not require a system restart after the adapter has been inserted.

If you select a listed adapter, you can click **Next** to begin the analysis. If you select **Adapter Not Listed** and then click **Next**, Slot Manager displays a second window where you can provide details about the adapter that you plan to use.

Manually defining adapter attributes

When the adapter that you plan to use is not listed in the first window of the Add Card wizard, use the “Adapter Attributes” window to define the adapter attributes. The right portion of this window contains several fields where you define adapter attributes.

Table 17 describes the selections that you can make.

Table 17. Slot Manager adapter attributes

Attribute name	Description
Maximum speed	Select the speed of the adapter, either PCI 33 MHz , PCI 66 MHz , PCI-X 66 MHz , or PCI-X 133 MHz . If you have not selected a speed, the wizard automatically selects PCI 33 MHz .
Bus width	Select 32-bit bus width or 64-bit bus width as applicable. The default value varies according to the adapter keying that is selected.
Voltage	Select 3.3V (3.3-volt), 5V (5 volt), or Dual as applicable. The default value varies according to the adapter keying that is selected.
PME signal required, Low-profile, Half-length	Select either Yes or No as applicable for the adapter. The default for these fields is No .

If you click **Adapter keying** in the New adapter type pane, you can click through a display of valid adapter key types. Adapter keying refers to the notches in the edge connector at the bottom of the adapter. These notches determine the voltage support and data bus width of the adapter. Make sure that the displayed graphic matches the key layout of the new adapter.

Note: Some chassis fit only low-profile adapters. Conversely, low-profile adapters fit only in certain chassis. The Add Card wizard will detect a low-profile slot or adapter and give suggestions accordingly.

The supported managed systems might not support all the combinations of adapter characteristics that can be created from the “Adapter Attributes” window. The wizard cannot find a solution for an unsupported combination (for example, a 5-volt adapter in a system that supports only 3.3-volt adapters).

After you have made your selections in the second window of the wizard, click **Begin** to start analysis of the system.

Filtering for Slot Manager events

You can create an event filter in the “Event Filter Builder” window 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 Manager** tree, and then expand the **Slot events** tree to display four events that are specific to Slot Manager:

Adapter 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.

Adapter eject complete

A user has requested that the operating system eject an adapter. The eject operation unloads the device driver from the adapter and turns off its slot in preparation for removing the adapter while the system is turned on.

Power fault

The adapter has a power fault.

Surprise removal of an adapter

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

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

Chapter 6. Asset ID

You can use the Asset ID task to view lease, warranty, user, and system information, including serial numbers. You also can 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 electrically erasable programmable read-only memory (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 a local file named `asset.dat`, in the `Director\data` directory, to maintain much of the information that is 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 36. “Asset ID” window

The following pages are available:

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.

Note: You can apply the Asset ID task to a group of managed systems using Mass Configuration. For more information, see “Mass Configuration” on page 51.

Chapter 7. BladeCenter Assistant

Use the BladeCenter Assistant task to manage your BladeCenter units. Within the BladeCenter Assistant, there are four subtasks:

- BladeCenter Configuration
- BladeCenter Management
- BladeCenter Deployment wizard
- Switch Management launch pad

Note: Additional subtasks might be displayed if you have installed supported vendor software.

Use the first two subtasks for BladeCenter unit configuration and management. 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 Switch Management launch pad subtask is used to start vendor software to manage your switches.

Notes:

1. The BladeCenter Assistant Management and Configuration subtasks target the physical platform objects for the blade servers. For more information about physical platforms, see Chapter 3, “Understanding IBM Director Console,” on page 31.
2. If you log into the BladeCenter chassis with a read-only account, you have only read-only access to the management module.

Starting the BladeCenter Configuration or BladeCenter Management subtask

Complete the following steps to start a BladeCenter Assistant subtask:

1. In the IBM Director Console Tasks pane, expand the **BladeCenter Assistant** task.
2. Drag the applicable subtask onto one or more managed object icons that you want to manage to open the “Management Processor Assistant” window. If IBM Director is unable to establish a connection with one or more objects, the Servers pane is displayed in the “Management Processor Assistant” window.

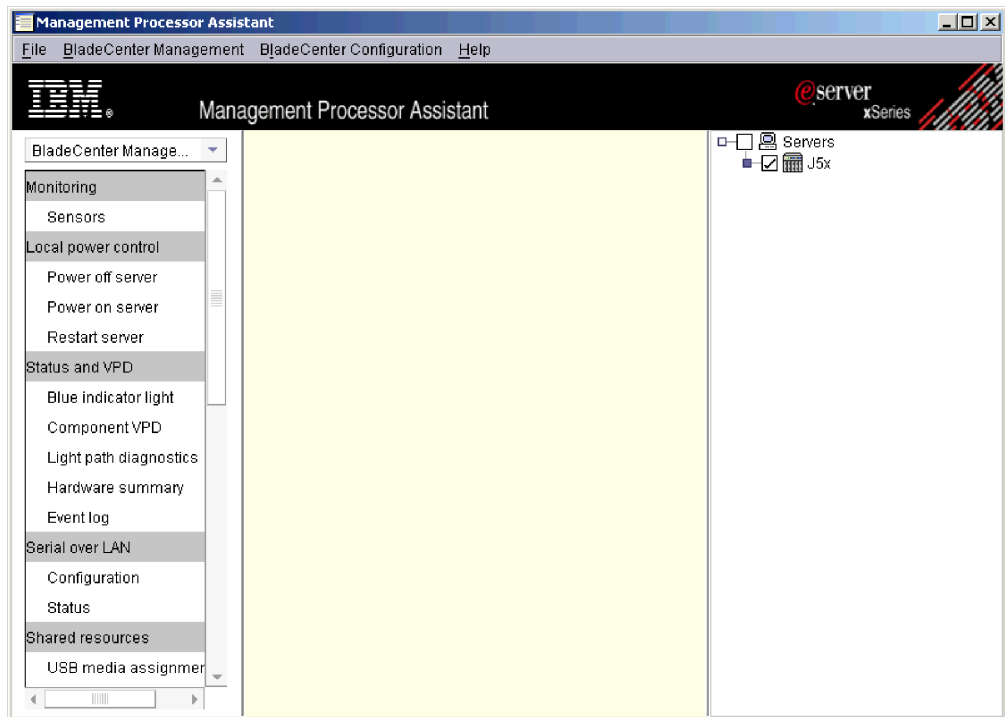


Figure 37. “Management Processor Assistant” window: BladeCenter Management subtask

The left pane contains menu options for the subtask that you selected.

When you select a menu option, the rows of information that are applicable to the selected options are displayed.

After you start the BladeCenter Configuration or BladeCenter Management subtask, use the menus and commands within the window to view, configure, and manage the BladeCenter unit.

Changing subtasks

To change to another BladeCenter Assistant subtask, click the list in the upper-left pane. The menu options for the subtask that you selected are displayed.

Selecting servers to work with

To display a hierarchical tree of BladeCenter chassis and servers that you can work with, click **File → Show/Hide server tree**. The right pane is subdivided, and the BladeCenter chassis and servers that you selected when starting the BladeCenter Assistant task are displayed in the right subpane.

If BladeCenter Assistant is unable to establish communications with the service processor for a selected system, a message is displayed that tells you to right-click the server in the Server tree pane and click **Communication**. The Communication Configuration pane opens, and you can provide the applicable parameters. If you do not do this, you will not be able to connect to that system, and the system will be unavailable in the Server tree pane.

To select the BladeCenter chassis and servers that you want to work with, expand the **Servers** icon in the Server tree pane. Select the check box for each server or BladeCenter chassis that you want to work with.

Configuring multiple servers at once

Use the Repeat option to configure many servers at once by copying the values from the row of one system to other selected systems. If the copied values are not applicable to one of the selected systems, then they are not applied to that system.

Complete the following steps to copy the values from one row to all other entries in a table:

1. In the Server tree pane, select the BladeCenter chassis or servers that you want to work with.
2. In the left pane, click a task to display the information that you want to configure.
3. In the middle pane, select an existing row that contains values that you want to copy to the other rows that are displayed.
4. Click **Repeat**. A confirmation window is displayed.
5. Click **OK**. You must click **Apply** to execute or save the changes.

Saving changes

After you add or modify information in the “Management Processor Assistant” window, you must click **Apply** to execute or save the changes. Depending on the subtask, the Apply option updates the information that is stored in IBM Director Server, modifies the configuration information on a service processor, or runs a management action.

Sorting information

To sort the information that is displayed, click on the column heading that you want to use as the sort criterion. To reverse the sort order, click the column heading again.

BladeCenter Configuration subtask

Use the BladeCenter Configuration subtask to view and configure BladeCenter chassis and blade server information.

Viewing service processor data

Use the BladeCenter Configuration subtask to view vital product data (VPD) for a service processor or microcontroller, such as firmware type, file name, and blade server name. Complete the following steps to view service processor data for a blade server:

1. Click **BladeCenter Configuration** → **Service processor configuration** → **Service Processor VPD**. The management-module information is displayed.
2. To view the Microcontroller VPD page, click the **Microcontroller VPD** tab. The ISMP firmware levels are displayed.

Configuring remote-alert settings

You can configure the information that is sent in critical, system, warning, and other alert messages. Complete the following steps to configure an alert:

1. Click **BladeCenter Configuration** → **Remote-alert settings** → **General-alert settings**. The General-alert settings pane is displayed.
2. Click the tab of the alert that you want to configure.
3. Select the alert to enable or disable the alert.
4. Click **Apply**.

Adding or modifying an alert-forwarding profile

The BladeCenter Configuration subtask provides access to alert-forwarding profiles that automatically send alerts to the systems that you specify. Alert forwarding ensures that alerts are sent to the applicable resources, even if a managed system experiences a catastrophic failure, such as an operating-system failure. You can create up to 12 alert-forwarding profiles for a BladeCenter unit.

An alert-forwarding profile is created automatically for a BladeCenter chassis the first time that the BladeCenter chassis is discovered by the management server. The management server uses the highest available entry number (typically, 12) to create the profile. The profile is configured to send the alerts to an IP address that is owned by the management server using the IBM Director Comprehensive alert-notification method. If the management server fails to assign an alert profile, an IBM Director event will be generated to warn you.

Note: A profile that is created by the management server might fail to send alerts to the applicable location if the management server owns multiple IP addresses. Make sure that the IP address that is used for the alert profile is:

- The IP address assigned to the service processor for the management server.
- Reachable from the service processor.

Complete the following steps to add or modify an alert-forwarding profile:

1. Click **BladeCenter Configuration** → **Remote-alert settings** → **Alert-forwarding profiles**. The Alert-forwarding profiles pane is displayed.
2. Click an existing profile, and then click **Add an entry**. A new record is displayed. By default, the **Chassis** and **Entry number** fields are filled in automatically with the selected chassis name and the number of the next profile record in the list.
3. Complete the alert-forwarding profile fields:
 - a. From the **Status** list, select **Enabled** to turn on the selected profile, **Disabled** to turn off the selected profile, or **Unused** to delete the selected profile.
 - b. In the **Description** field, type a brief description to help identify the selected profile.
 - c. From the **Connection type** list, select the delivery method that you want to use for the selected profile.

IBM Director Comprehensive

Receive all alerts that are generated by the management module regardless of whether the type of alert is enabled. You also must specify an IP address if you select this notification method.

SNMP over LAN

You must configure SNMP for this notification method to work properly.

E-mail over LAN

You must configure SMTP for this notification method to work properly.

- d. In the **IP address or host name** field, type the IP address or host name of the system that you want to receive the alerts. For you to edit this field, the connection type must be set to IBM Director Comprehensive or E-mail over local area network (LAN).

Note: If you provide a host name, make sure the service processor is configured to use Domain Name Systems (DNS).

- e. In the **E-mail address** field, type the e-mail address of the e-mail account that you want to receive the alerts. For you to edit this field, the connection type must be set to E-mail over LAN.
 - f. Select the **Critical events only** check box to forward only critical events.
4. Click **Apply** to save the changes.

Deleting an alert-forwarding profile

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

1. Click **BladeCenter Configuration** → **Remote-alert settings** → **Alert-forwarding profiles**. The Alert-forwarding profiles pane is displayed.
2. Click the alert-forwarding profile that you want to delete.
3. From the **Status** list, select **Unused**.
4. Click **Apply** to save the changes.

Configuring network settings for the service processor

From the Network settings pane you can restart selected service processors or view or modify the following settings for selected managed systems:

- IP properties
- Hardware
- Dynamic Host Configuration Protocol (DHCP)
- DNS
- Restart service processor

Note: When you change the network settings for a management module, IBM Director automatically selects the **Restart service processor** check box on the “Restart service processor” page. When you click **Apply**, you are asked whether you want to restart the selected service processors. If you click **Yes**, all selected service processors are restarted immediately. If you click **No**, the changes are still applied to the service processor; however, they do not take effect until the service processor is restarted.

Complete the following steps to configure network settings:

1. Click **BladeCenter Configuration** → **Network settings** → **Network interfaces**. The Network interfaces pane is displayed.
2. To configure the IP properties, click the **IP properties** tab. The IP properties page is displayed.

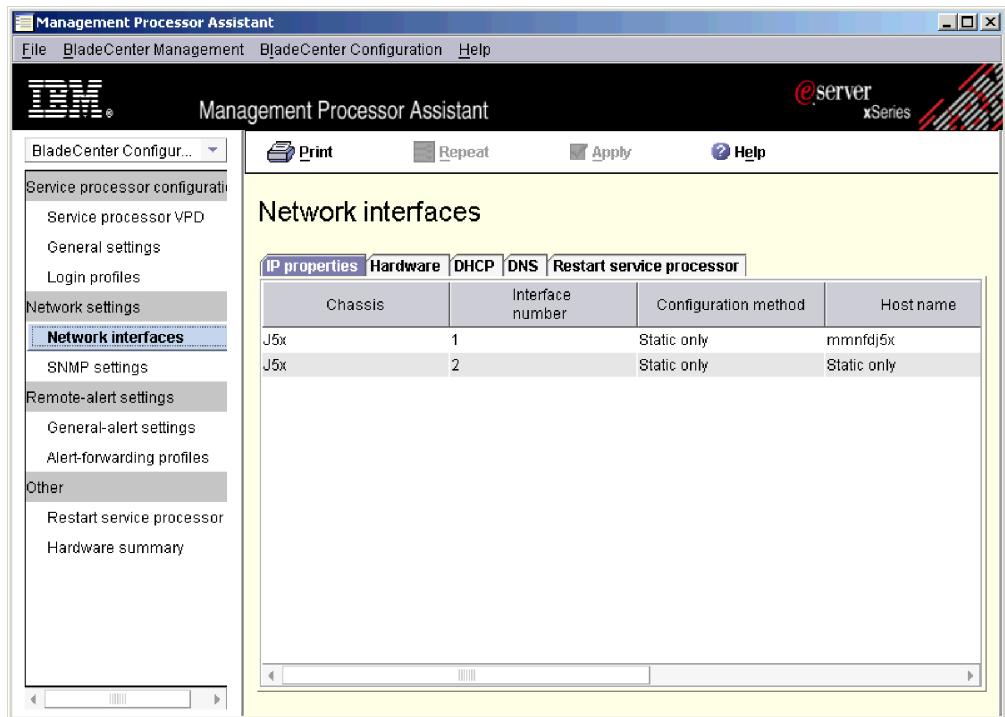


Figure 38. “Management Processor Assistant” window: IP properties page

3. Modify the applicable fields:
 - a. From the **Configuration method** list, select a configuration method. Select **Static only** to use the current configuration values. Select **DHCP, then Static** to use the static IP address when the DHCP server does not respond. Select **DHCP only** to automatically obtain an IP address from the DHCP server.

Note: If you enable DHCP, you must have an accessible, active, and configured DHCP server on your network. The configuration settings that are assigned by a DHCP server override all static IP settings that you have provided.
 - b. In the **Host name** field, type the host name of the service processor. The host name can be a maximum of 63 characters long. If the host name that you type conflicts with the IP address and DHCP is selected as the configuration type, the DHCP server assigns the appropriate IP address to the host name.
 - c. In the **IP address** field, type the IP address of the service processor.
 - d. In the **Subnet mask** field, type the subnet mask that is used by the service processor.
 - e. In the **Gateway** field, type the gateway address that is used by the service processor.
4. To configure the hardware-network settings, click the **Hardware** tab. The Hardware page is displayed.

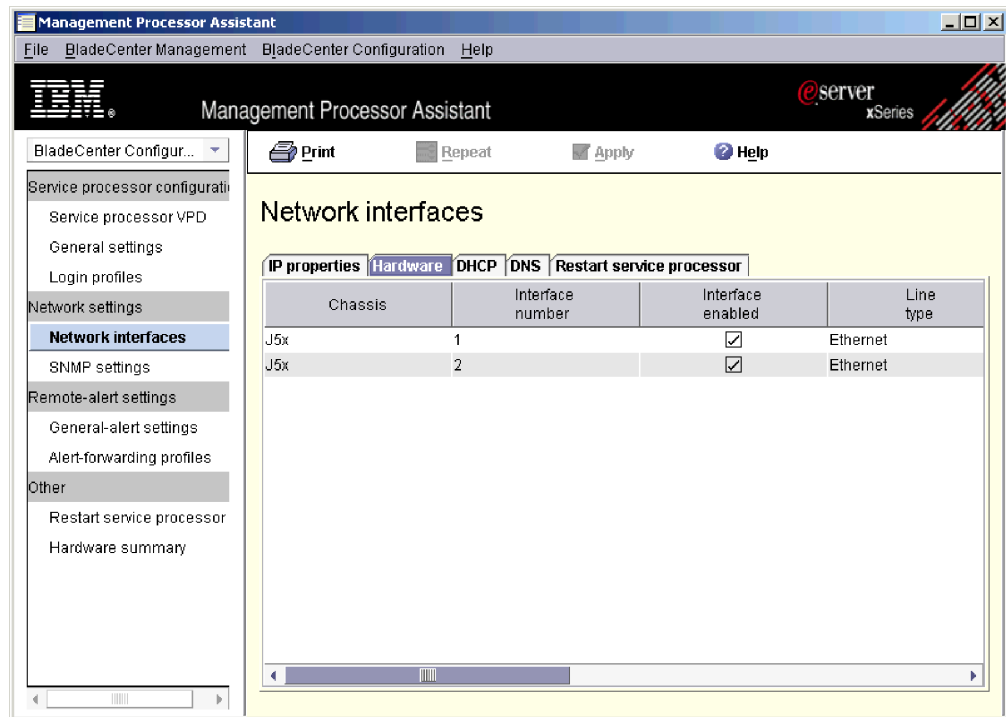


Figure 39. “Management Processor Assistant” window: Hardware page

5. Modify the applicable fields:
 - a. From the **Data rate** list, select the data-transfer rate for the service processor. Make sure that your selection corresponds to the capabilities of your network. To automatically detect the data-transfer rate, select **Auto**.
 - b. From the **Duplex** list, select the type of communication channel that is used in your network. The network interface can be full duplex only.
 - c. In the **MTU size** field, type the maximum transmission unit (MTU) size. The MTU value that you type indicates the maximum packet size (in bytes) for your network. For Ethernet, the MTU range is 60-1500.
 - d. In the **Administrator assigned MAC address** field, type a physical address for the service processor. If you specify an address, this locally administered address will override the burned-in media access control (MAC) address. The address must be in the form of xx xx xx xx xx xx (six hexadecimal digits separated by blanks).
6. To configure DNS, click the **DNS** tab. The DNS page is displayed.

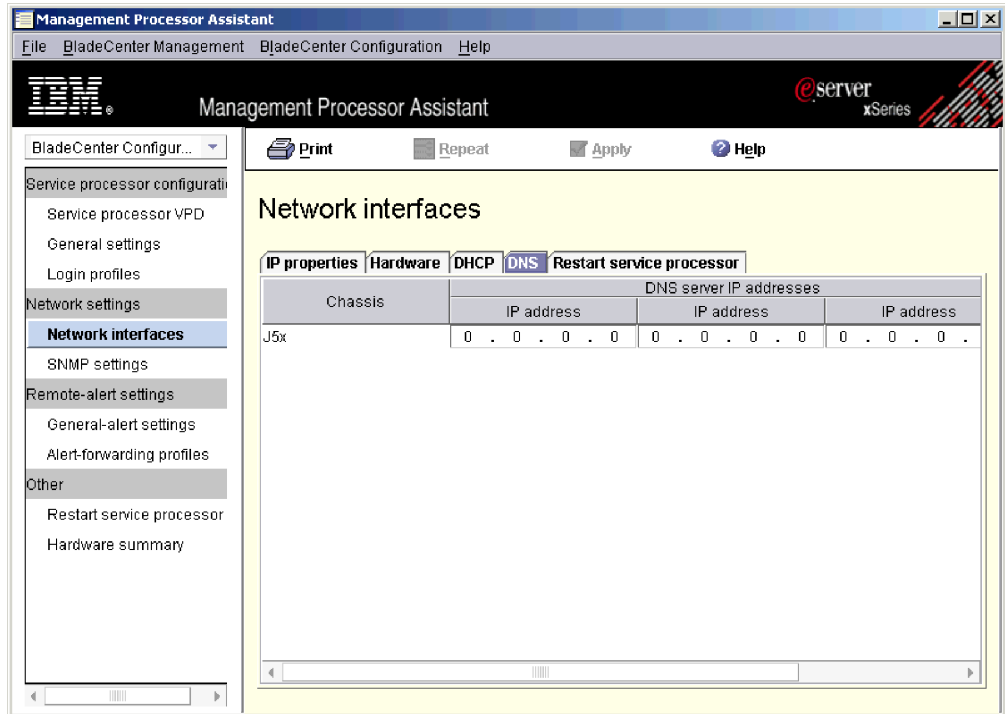


Figure 40. “Management Processor Assistant” window: DNS page

7. Modify the applicable fields:
 - a. In the **IP address** fields, type the IP addresses of the DNS servers that are on your network. You can specify a maximum of three DNS servers.
 - b. Select the **Enable DNS lookup** check box to use a DNS server on your network to translate host names into IP addresses.
8. To restart a service processor, click the **Restart service processor** tab. The Restart service processor page is displayed.

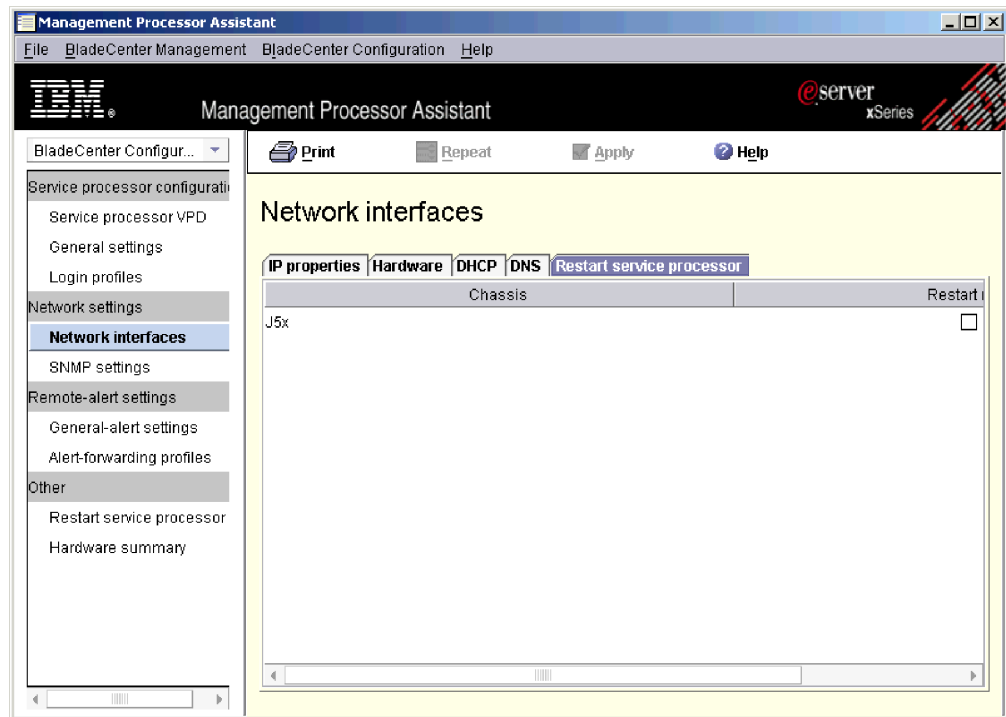


Figure 41. “Management Processor Assistant” window: Restart service processor page

9. Modify the appropriate fields:
 - a. Click the service processor that you want to restart.
 - b. Select the **Restart now** check box to restart the service processor after you apply your changes.
 - c. Select the **Allow failover** check box to allow failover when the service processor restarts.
10. Click **Apply** to save the changes.

Configuring SNMP settings

Complete the following steps to configure SNMP settings:

1. Click **BladeCenter Configuration** → **Network settings** → **SNMP settings**. The SNMP settings pane is displayed.
2. Select the server that you want to configure.
3. Modify the applicable fields:
 - a. In the **Contact** field, type the contact information for the server contact. For example, you might include the person’s name and phone number.
 - b. In the **Location** field, type a location for the server.
 - c. Select the **Agent enabled** check box to enable the SNMP agent. This check box must be selected for alerts to be sent.
 - d. Select the **Traps disabled** check box to disable SNMP traps. This check box must be cleared for alerts to be sent.
4. Configure a community:
 - a. Select the applicable server.
 - b. In the **Community name** field, type the name of the community.
 - c. In the **Host name** field, type a valid host name for the community.
5. Click **Apply**.

Restarting a service processor

After you modify the network settings for a service processor, restart the service processor to have the network settings take effect.

Complete the following steps to restart a service processor:

1. Click **BladeCenter Configuration** → **Other** → **Restart service processor**. The Restart service processor pane is displayed.
2. Select the **Restart now** check box to restart the service processor after you apply your changes.
3. Select the **Allow failover** check box to allow failover when the service processor restarts.
4. Click **Apply**.

Creating and changing login profiles

You can use login profiles to control access to your management module. When you perform a task that requires you to access the management module (for example, BladeCenter Configuration or BladeCenter Management), the saved user ID and password are used to verify access. By default, the BladeCenter unit is configured with a login profile that allows remote access. The default login profile has a user ID of USERID and a password of PASSWORD, where the 0 in the password is a zero. You can create a maximum of 12 login profiles for a supported management module.

Note: Some managed objects do not support login profiles.

Complete the following steps to create or change a login profile:

1. Click **BladeCenter Configuration** → **Server processor configuration** → **Login profiles**. The Login profiles pane is displayed.

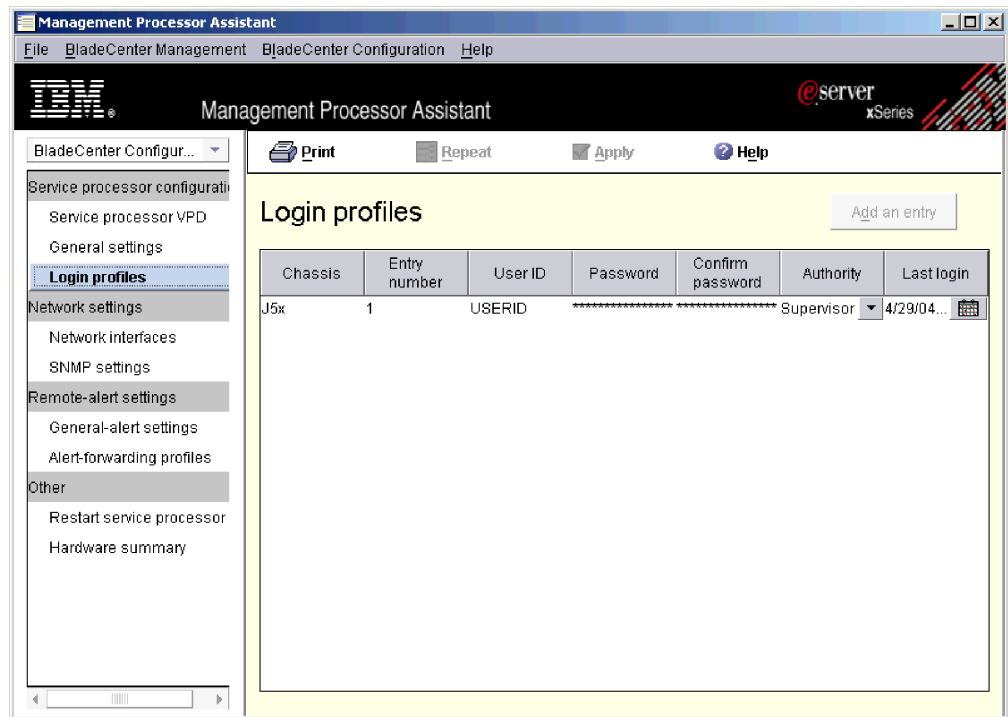


Figure 42. “Management Processor Assistant” window: Login profiles pane

2. Click an existing profile from the Login profiles pane.
3. Click **Add an entry**. A new record is displayed. The **Entry number** field is filled in automatically using the lowest entry number available. You can click the **Entry number** field to select from a list of available entry numbers.

Note: Use the Repeat option to configure multiple servers at once to use the same user ID and password.

4. Create or modify the login profile.

Note: Both the **User ID** and **Password** fields are case sensitive.

- a. In the **User ID** field, type the user ID for the new login profile.
- b. In the **Password** field, type the password for the new login profile. The password must be five to 12 characters long, contain no spaces, and have at least one alphabetic character and one numeric character.
- c. In the **Confirm password** field, retype the password for the new login.
- d. From the **Authority** list, select the level of access for the new profile. A sublist is displayed.

Supervisor

Enables the user to view and modify all supported fields and actions in the interface.

Read only

Enables the user to view data only. The user cannot make changes to information, perform file transfers, or turn on or turn off any managed objects.

Custom

Enables the user to have read-only access or supervisor access to specific functions that you explicitly select from a sublist.

- e. If needed, from the sublist, select the applicable access levels; then, click **Done**. Select an access-level check box to provide read/write access for that function. Clear an access-level check box to provide read-only access to that function.

User account management

Enables the user to add, modify, or delete user IDs and change global login settings.

Remote console access

Enables the user to access the remote server.

Remote console and virtual media access

Enables the user to access the remote server console and to modify the virtual media functions for that remote server.

Remote server and power/restart access

Enables the user to access the remote server console and to modify the power-on and restart functions for the remote server.

Ability to clear event tags

Enables the user to clear the event logs.

Adapter configuration - Basic

Enables the user to modify the basic configuration parameters for the system, such as system settings and alerts.

Adapter configuration - Networking and security

Enables the user to modify the configuration parameters relating to network interfaces, network protocols, and serial ports.

Adapter configuration - Advanced

Enables the user to modify basic configuration parameters and the configuration parameters relating to the network interfaces. Also enables the user access to the following advanced configuration settings and functions: firmware upgrades, restore adapter factory-default settings, modify and restore or reset adapter configuration from a configuration file, and restart or reset the adapter.

5. To delete a user profile, click the user profile that you want to delete, and delete the information that is displayed in the **User ID** field.

Notes:

- a. A management module must have at least one profile with supervisor authority. If there is only one profile with supervisor authority, you cannot delete the profile or change the access level.
 - b. You cannot delete a profile if you are currently logged on to the system with that profile.
6. Click **Apply**.

BladeCenter Management subtask

You can use the BladeCenter Management subtask to view BladeCenter chassis, blade server, and switch information; turn on and turn off servers; restart a managed system, view and change keyboard, video, and mouse (KVM) policy and assignment; view and change Universal Serial Bus (USB) policy and assignment; and much more.

Viewing sensor data

You can view environmental data, such as temperature, voltage, fan speeds and power supply, that is recorded by sensors in a server.

To view sensor data, click **BladeCenter Management** → **Monitoring** → **Sensors**. The data is displayed.

Viewing component data

You can view vital product data about the supported managed objects, which includes chassis, power supplies, blade servers, expansion cards, and adapters.

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

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, such as the event severity.

To view the event log that is 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) for supported management objects.

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

Viewing light path diagnostics

You can view the light path diagnostics LEDs 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 that you want.

Note: To view light path diagnostics for a blade server, you must select the chassis as well as the blade server.

Viewing and changing 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 state of the blue-indicator light on a blade server:

1. Click **BladeCenter Management** → **Status and VPD** → **Blue-indicator light**. The blue-indicator-light information is displayed.
2. In the table, click the row for the server that you want to work with.
3. From the **State** list, select a light-indicator option. The options are **On**, **Off**, and **Flashing**.
4. Click **Apply**.

Turning blade servers on and off

You can turn on and turn off a blade server remotely. Complete the following steps to turn off a blade server:

1. Click **BladeCenter Management** → **Local power control** → **Power off server**.
2. To turn off the blade server immediately, select the **Power off immediately** check box.
3. Click **Apply**.

Complete the following steps to turn on a blade server:

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

Restarting a blade server

Complete the following steps to restart a blade server:

1. Click **BladeCenter Management** → **Local 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 KVM select button for each server in a BladeCenter chassis. If you disable the KVM select button, you cannot press the KVM select button on the hardware to access the keyboard, video, and mouse on the chassis.

Complete the following steps to enable or disable this button:

1. Click **BladeCenter Management** → **Policy** → **KVM**. The selected servers are displayed.
2. Select the applicable **Local control enabled** check box for the server that you want to enable the KVM select button for, or clear the check box to disable the KVM select button for the server.
3. Click **Apply**.

Viewing and changing KVM assignment

You can view which blade-server bay currently 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** field, click the blade server that you want to own the KVM from the list.
3. If you do not want the KVM media to be assigned to a specific blade server, select the **Park** check box.
4. Click **Apply**.

Viewing and changing USB policy

You can enable or disable the USB select button for each server in a BladeCenter chassis. If you disable the USB select button, you cannot press the USB select button on the hardware to access the USB devices on the chassis.

Complete the following steps to enable or disable the USB select button:

1. Click **BladeCenter Management** → **Policy** → **Local USB control**.
2. Select the applicable **Local control enabled** check box for the server that you want to enable the USB select button for, or clear the check box to disable the USB select button for the server.
3. Click **Apply**.

Viewing and changing USB media assignment

You can view which blade-server bay owns 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** field, click the blade server that you want to own the USB media from the list.
3. If you do not want the USB media assigned to any blade server, in the **Park** field, select the check box.
4. 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** → **Local power control**.
2. Select the applicable **Local control enables** 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 startup (boot) options

You can view and change the startup (boot) sequence for blade servers. Up to four devices can be defined as boot devices. The device that is listed in the **First** field of the boot order will attempt to startup the blade server first. If the first device fails, the second device is tried, and so on, until all specified devices have been tried.

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

1. Click **BladeCenter Management** → **Shared resources** → **Blade server boot options**.
2. Select a device in the applicable **Boot order** field.
3. Click **Apply**.

Viewing and configuring I/O-module settings

Switch modules and pass-thru modules are the two types of I/O modules that are supported on BladeCenter chassis. These I/O modules provide communication between the BladeCenter servers and the external network. You can use BladeCenter Assistant to view or configure some of the supported settings for switch modules and pass-thru modules that are installed in the I/O-module bays of a BladeCenter chassis.

To view and configure I/O-module settings, click **BladeCenter Management** → **I/O modules** → **I/O module management**.

Viewing I/O-module vital product data

You can view the I/O-module vital product data, such as the build level of the I/O-module hardware, manufacture date, FRU number, and firmware levels for each of the modules on the chassis. To view this information, click **BladeCenter Management** → **I/O module** → **I/O module VPD**.

Configuring I/O-module IP settings

You can change information about the current IP settings only for I/O modules that support the applicable changes.

Complete the following steps to configure the IP settings of an I/O module:

1. Click **BladeCenter Management** → **I/O module** → **I/O module IP Configuration**.
2. In the **Host IP address** field, type the host address for the I/O module.
3. In the **Subnet mask** field, type the IP address for the subnet mask.
4. In the **Gateway** field, type the IP address for the network gateway.
5. In the **Configuration method** field, select the applicable configuration method for the I/O module.
6. Click **Apply pending**; then, click **Apply**

Note: If you click **Apply** only, the configuration settings are saved but not activated.

Deployment wizard subtask

You can use the BladeCenter Deployment wizard to create a profile that contains BladeCenter chassis configuration information.

You can run the wizard online (targeted against one or more BladeCenter chassis) or offline. When you run the wizard online, you are prompted to configure only those switch modules that are present in the chassis. When you run the wizard offline, you are prompted to configure all the currently supported switch modules. After you run the wizard and create the profile, you can apply it to one or more BladeCenter chassis. If the profile contains configuration information that it is not applicable to a specific BladeCenter chassis, the information is ignored.

You also can use the BladeCenter Deployment wizard to generate an XML file that contains BladeCenter chassis configuration information. You then can use DIRCMD, the IBM Director command-line interface, to create a profile from the XML file. You also can use DIRCMD to apply the profile to one or more BladeCenter chassis. For more information about DIRCMD, see Chapter 30, “Working with management servers using the command-line interface (DIRCMD),” on page 277.

Understanding BladeCenter Deployment wizard profiles

You can use the BladeCenter Deployment wizard to create reusable profiles that you can apply to BladeCenter chassis. A profile can contain the following configuration information:

- User names and passwords for the management module and switch modules
- IP addresses for the management module and switch modules
- Network protocol configuration information for the management module and switch modules
- Deployment policies
- Whether or not detect-and-deploy is enabled for the chassis or switch modules

Chassis detect-and-deploy profiles

You can designate one profile to automatically configure new BladeCenter chassis when they are added to the IBM Director environment. This is the *chassis detect-and-deploy profile*. IBM Director automatically applies the chassis detect-and-deploy profile when it discovers a new BladeCenter chassis or if you create a new BladeCenter chassis managed object.

If you enable a chassis detect-and-deploy policy, be careful when deleting and manually recreating chassis managed objects for previously configured BladeCenter chassis. If you delete and manually recreate a BladeCenter chassis managed object, IBM Director automatically applies the chassis detect-and-deploy profile to that chassis.

Profiles that include deployment policies

A profile can include deployment policies, if Remote Deployment Manager (RDM) is installed on your management server. A *deployment policy* associates a specific bay in the BladeCenter chassis with an RDM noninteractive task, for example, installing an operating system.

When a profile that includes deployment policies is applied to a BladeCenter chassis, the RDM noninteractive tasks are run on the blade servers in the bays that are assigned deployment policies. The blade servers must be turned off; IBM Director will not shut down or restart (reboot) blade servers that are running.

After you configure a BladeCenter chassis using a profile that contains deployment policies, IBM Director applies the deployment policy whenever a new blade server is inserted in the BladeCenter chassis. IBM Director automatically sets the blade server boot sequence to the local hard disk drive followed by the network. If an operating system is already installed, the blade server starts (boots) from the hard disk drive, and IBM Director does not run the RDM task. However, if the blade server starts (boots) from the network, IBM Director initiates the deployment policy and runs the RDM task.

Note: If the BladeCenter chassis contains an IBM HS20 SCSI Storage Expansion unit, IBM Director does not apply the deployment policy when both the following conditions apply:

- The blade server that is used with the storage expansion unit is set to start (boot) from the SCSI hard disk drive.
- You hot-swap the SCSI hard disk drive in the storage expansion unit.

To ensure that the deployment policy is applied to the new SCSI hard disk drive, after hot-swapping the SCSI hard disk drive, remove and reinsert the blade server.

Creating and applying a BladeCenter Deployment wizard profile

Note: You must have a pool of static IP addresses to assign to the management module and switch module configuration ports. To configure one BladeCenter chassis, you must have a minimum of two static IP addresses for the management module and one static IP address for each switch module. The IP addresses must be on the same subnet as the management server.

Complete the following steps to create a BladeCenter Deployment wizard profile:

1. In the IBM Director Console Tasks pane, expand the **BladeCenter Assistant** task.

2. Complete one of the following steps:

If you are running the wizard online	Drag the Deployment Wizard task onto the BladeCenter chassis that you want to configure.
If you are running the wizard offline	Double-click the Deployment Wizard task.

The BladeCenter Deployment wizard starts and the “Welcome to the BladeCenter Deployment wizard” window opens.

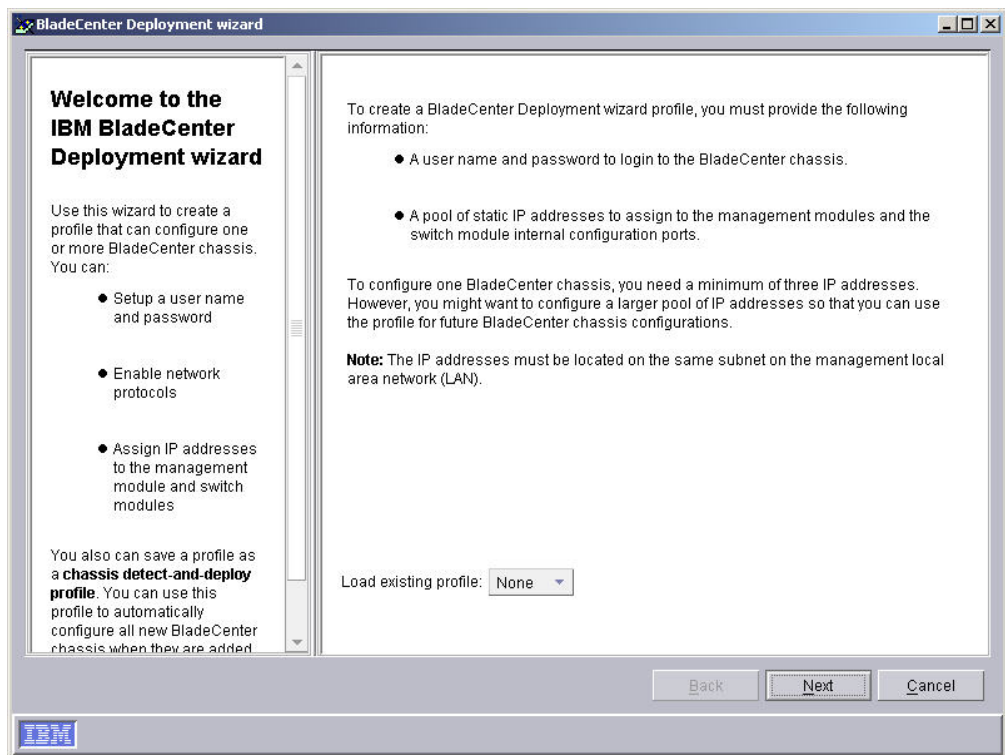


Figure 43. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window

3. Click **Next**. If you are already logged in to the management module or if you are running the wizard offline, the “Change the user name and password for the management module” window opens. Go to step 6 on page 114. If you are running the wizard against a locked BladeCenter chassis, the “Login to the BladeCenter management module” window opens.

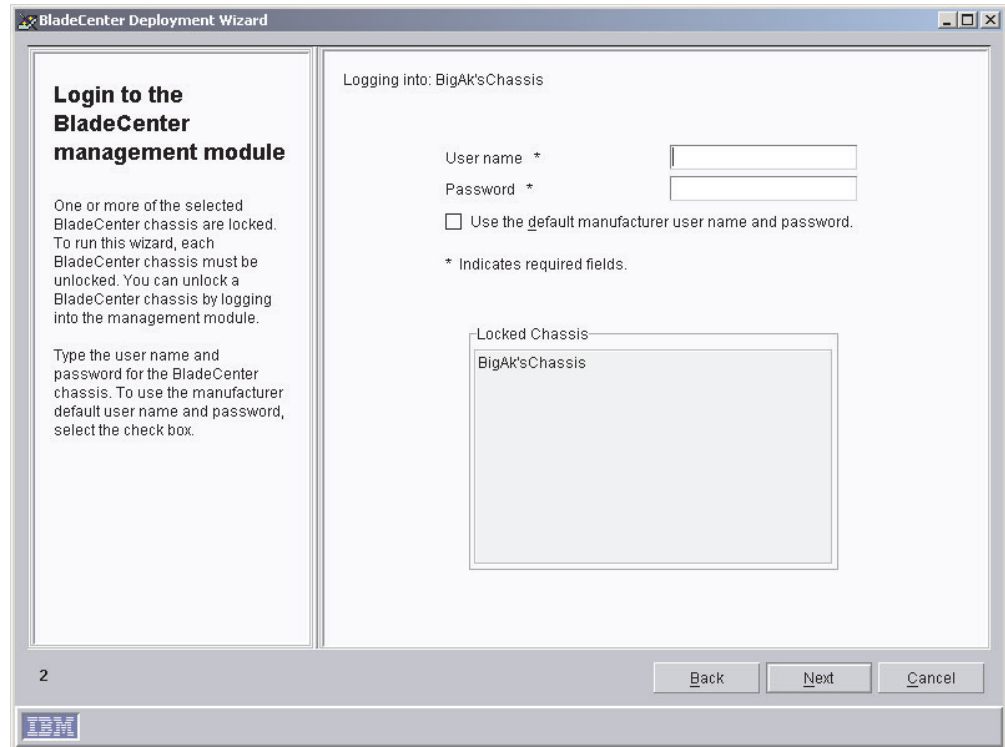


Figure 44. BladeCenter Deployment wizard: “Login to the BladeCenter management module” window

4. Log in to the BladeCenter management module:
 - a. In the **User name** field, type a valid user name for the management module.
 - b. In the **Password** field, type the password that is associated with the user name that you typed in step 4a.To use the default user account and password, select the **Use the factory-default user name and password** check box.
5. Click **Next**. The “Change the user name and password for the management module” window opens.

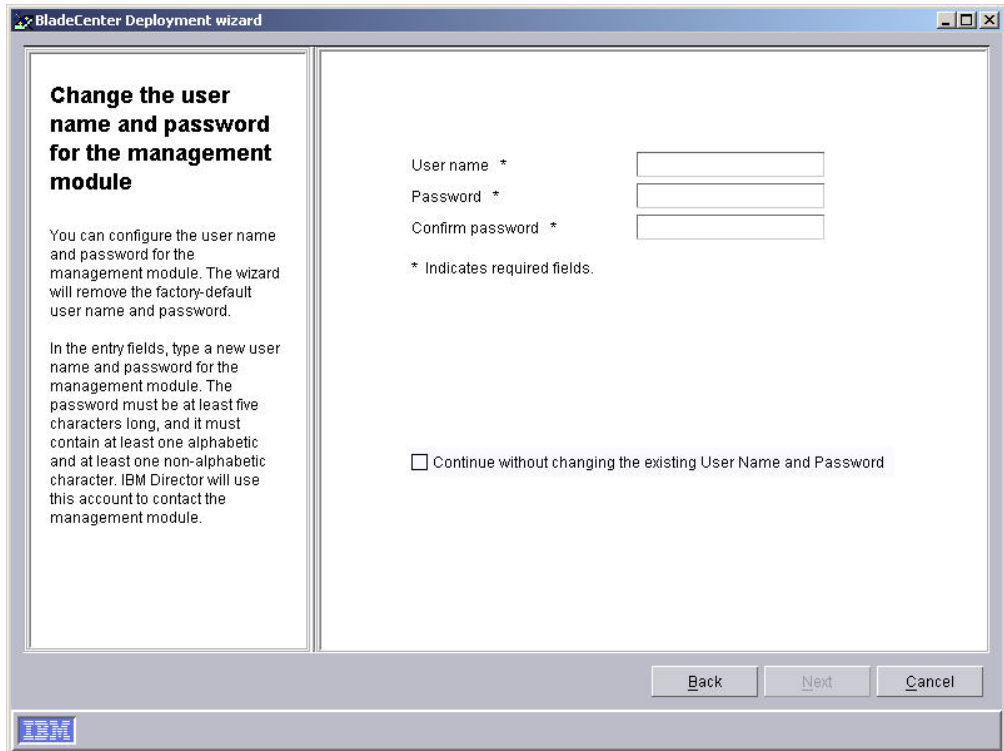


Figure 45. BladeCenter Deployment wizard: “Change the user name and password for the management module” window

6. Configure the user name and password for the BladeCenter chassis:
 - a. In the **User name** field, type a user name.
 - b. In the **Password** and **Confirm password** fields, type a password. It must be at least six characters and contain at least one digit.

If you do not want to change the existing management module user name and password, select the **Continue without changing the existing user name and password** check box.
7. Click **Next**. The “Configure the management module properties” window opens.

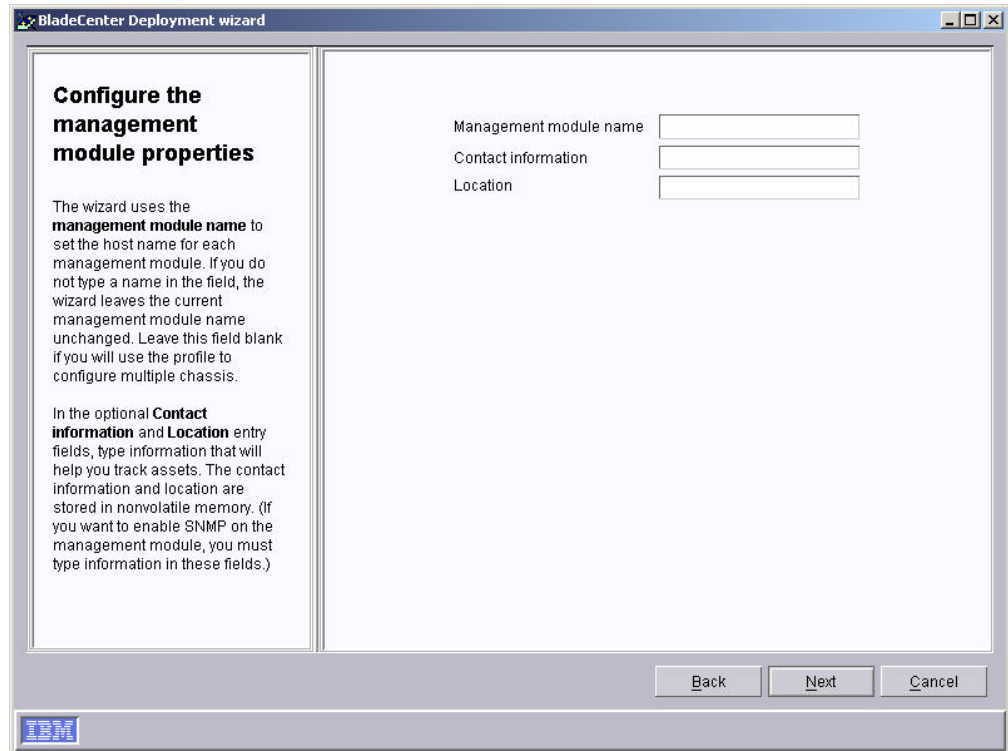


Figure 46. BladeCenter Deployment wizard: “Configure the management module properties” window

8. Configure the management-module properties:
 - a. In the **Management module name** field, type a name for the BladeCenter management module. If you leave this field blank, the BladeCenter management module is assigned the profile name.
 - b. In the **Contact information** field, type the name of the asset owner.
 - c. In the **Location** field, type information about where the BladeCenter is located.

Note: If you want to enable SNMP on the management module, you *must* type information in the **Contact information** and **Location** entry fields.

9. Click **Next**. The “Configure the management module protocols” window opens.

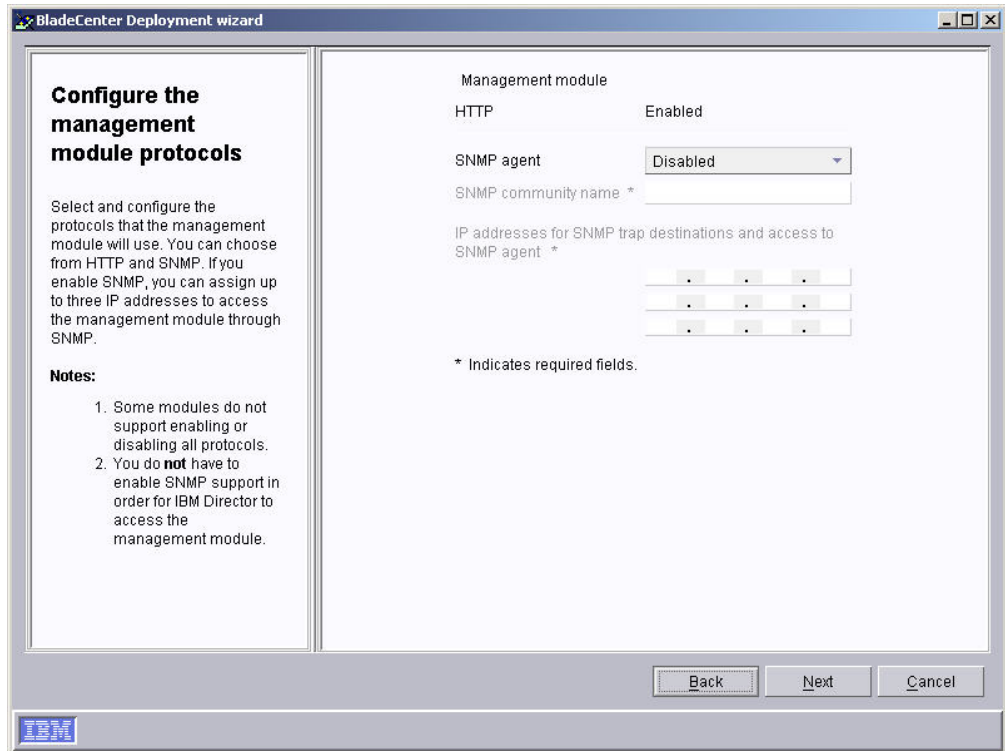


Figure 47. BladeCenter Deployment wizard: “Configure the management module protocols” window

10. Configure the management-module network protocols. Hypertext Transfer Protocol (HTTP) is enabled by default. Complete the following steps to enable SNMP:
 - a. In the **SNMP agent** field, select **Enabled**.
 - b. In the **SNMP community name** field, type a community name. (By default, this is set to public.)
 - c. In the **IP addresses** fields, type at least one and as many as three IP addresses.

Note: To enable SNMP on the management module, you *must* have typed information in the **Contact information** and **Location** entry fields in the previous window. To do so now, click **Back** to return to the “Configure the management module properties” window.

11. Click **Next**. The “Configure the IP addresses” window opens.

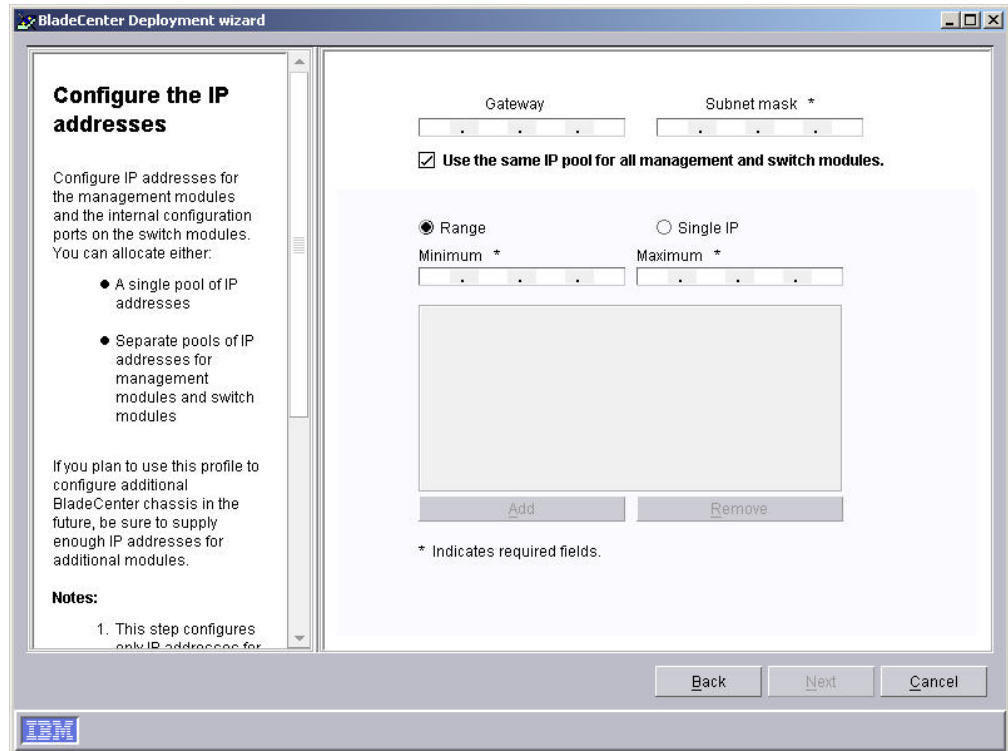


Figure 48. BladeCenter Deployment wizard: “Configure the IP addresses” window

12. Configure the IP settings for the management and switch modules:
 - a. In the **Gateway** field, type the IP address for the network gateway.
 - b. In the **Subnet mask** field, type the IP address for the subnet mask.
13. Assign IP addresses for the management and switch modules:
 - a. To use one pool of IP addresses for both the management and switch modules, create a pool of IP addresses. You can add IP addresses to the pool individually or by specifying a range:
 - To add a single IP address to the pool, click **Single IP**. In the **IP address** field, type the IP address; then, click **Add**.
 - To add a range of IP addresses, click **Range**. In the **Minimum** and **Maximum** fields, type the IP addresses that specify the range. Click **Add**.
 - b. To assign separate pools of IP addresses to the management and switch modules, clear the **Use the same IP pool for all management and switch modules** check box. The **Management module** and **Switch module** tabs are displayed.
 - To create the pool of IP addresses for the management modules, click **Management module** and follow the instructions in step 13a.
 - To create the pool of IP addresses for the switch modules, click **Switch module** and follow the instructions in step 13a.
14. Click **Next**. The “Change the user name and password for switch modules” window opens.

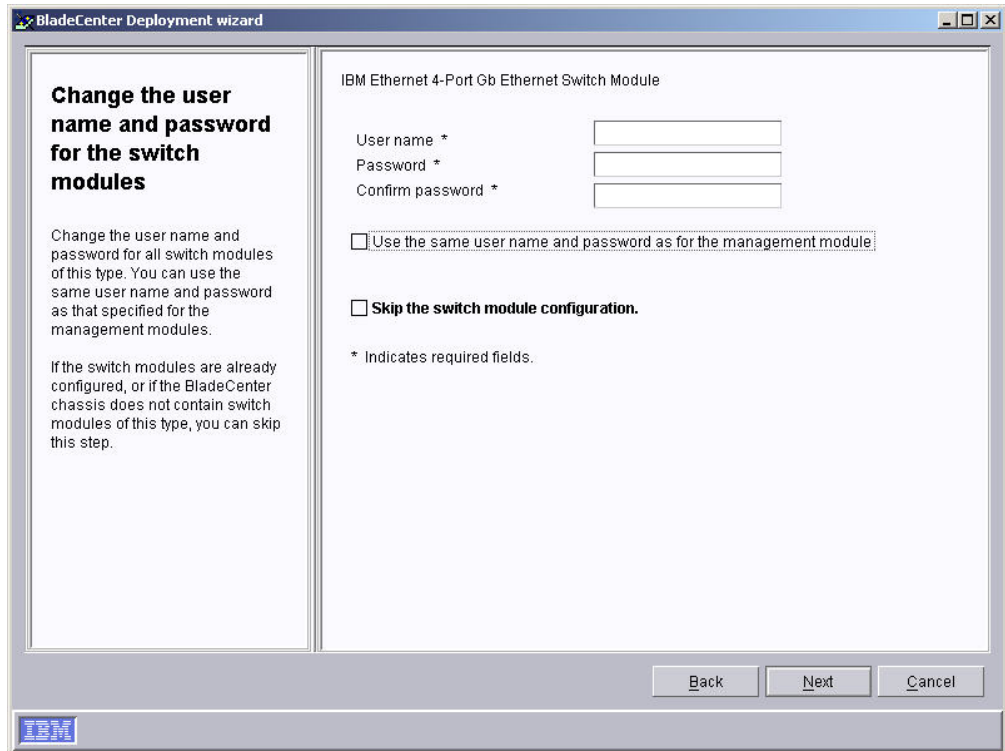


Figure 49. BladeCenter Deployment wizard: “Change the user name and password for switch modules” window

15. Configure the user name and password for this type of switch module. Take one of the following actions:
 - a. To use the same information for both the management module and the switch module, select the **Use the same user name and password as for the management module** check box. (This option is not available if a user name and password for the management module has not been specified.)
 - b. To assign a new user name and password to the switch module, in the applicable fields, type a new user name and password.
 - c. If the switch modules are configured already or you do not want to configure this type of switch module, select the **Skip the module configuration** check box. Go to step 18 on page 120.
16. Click **Next**. The “Configure the switch module” window opens.

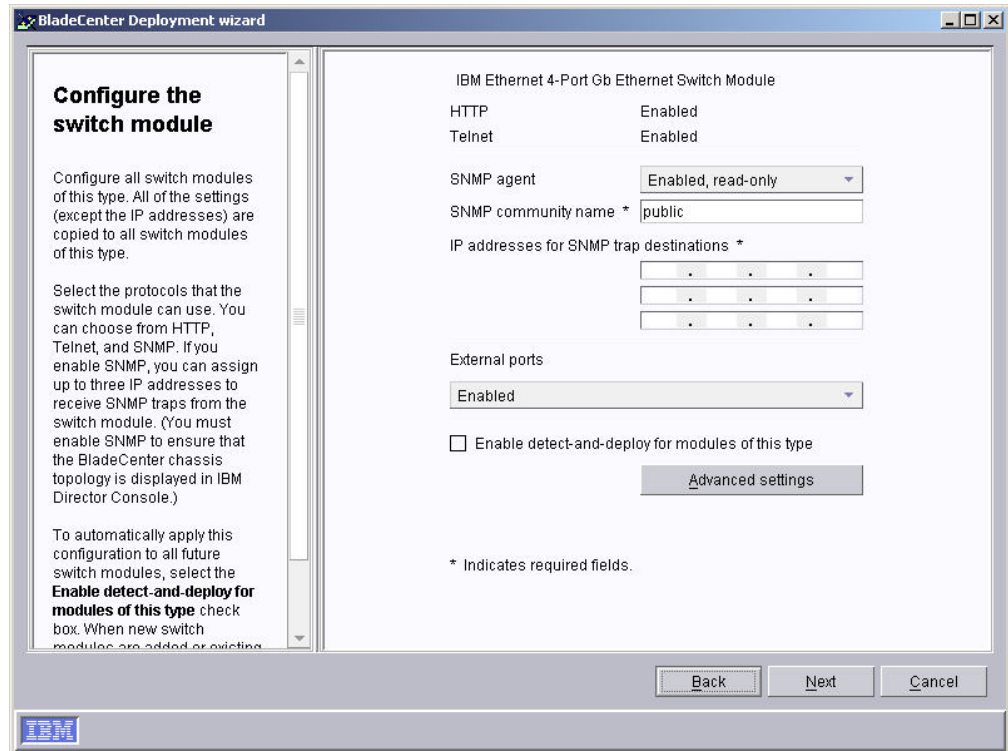


Figure 50. BladeCenter Deployment wizard: “Configure the switch module” window

17. Configure the network protocols for this type of switch module:
 - a. To enable HTTP, in the **HTTP** field, select **Enabled**. (This option is not available for all switch modules.)
 - b. To enable Telnet, in the **Telnet** field, select **Enabled**. (This option is not available for all switch modules.)
 - c. To enable SNMP, in the **SNMP agent** field, select **Enabled** or **Enabled, read-only**. Then, complete the following tasks:
 - 1) In the **SNMP community name** field, type a community name. By default, this is set to `public`.
 - 2) In the **IP addresses** fields, type at least one and as many as three IP addresses. These addresses receive SNMP traps from the switch module.

Note: You must enable SNMP if you want the switch module to appear in the BladeCenter chassis topology that is displayed in IBM Director Console.
 - d. To enable the external ports of the switch modules, select **Enabled**. If you are configuring an IBM Ethernet 4-Port Gb Ethernet Switch Module, you also can configure the external ports as link aggregation groups (trunks). Before you do so, make sure that the LAN switch has a compatible multiport trunk configuration.
 - e. To automatically apply this configuration to all switch modules of this type, select the **Enable detect-and-deploy for modules of this type** check box. When switch modules of this type are inserted in the BladeCenter chassis, this configuration is applied automatically.

f. Click **Advanced settings** to perform one of the following tasks:

If you are running the wizard online	Start the switch vendor software and configure additional settings.
If you are running the wizard offline	Load a configuration file. You can create a configuration file by using the vendor software to back up the switch module configuration.

18. Take one of the following actions:

- If you are running the wizard online and have not yet configured all the switch modules in the BladeCenter chassis, repeat step 14.
- If you are running the wizard online and have configured all the switch modules in the BladeCenter chassis, go to step 19.
- If you are running the wizard offline, repeat steps 14-17 until you have configured each of the supported types of switch modules.
- If you are running the wizard offline and have configured all of the switch modules, go to step 19.

19. Click **Next**. The “Deploy operating systems on the blade servers” window opens.

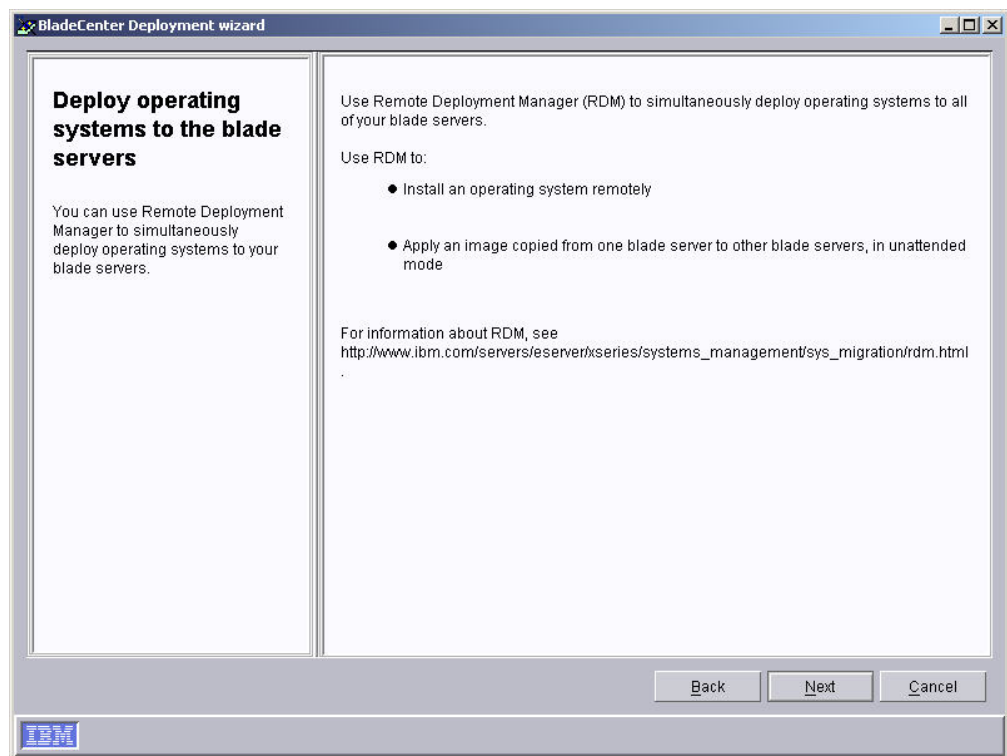


Figure 51. BladeCenter Deployment wizard: “Deploy operating systems on the blade servers” window

20. If Remote Deployment Manager (RDM) is installed on your management server, go to step 21. Otherwise, go to step 24 on page 121.

21. Click **Next**. The “Configure the deployment policies” window opens.

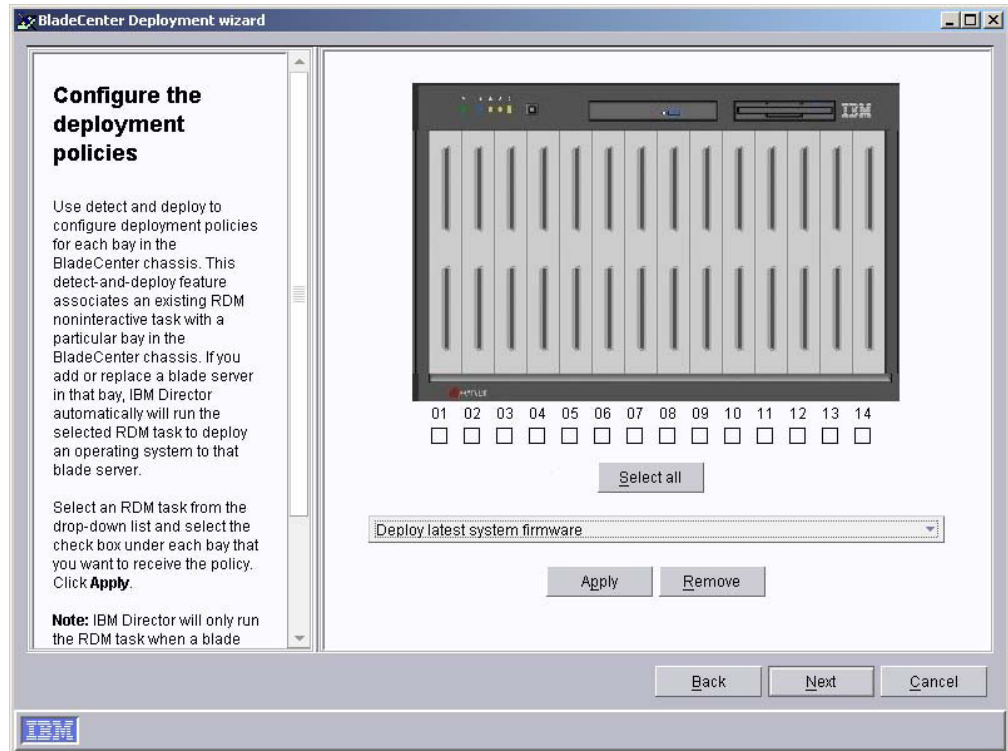


Figure 52. BladeCenter Deployment wizard: “Configure the deployment policies” window

22. Select an RDM task from the drop-down list and select the check box under each bay that you want to receive the policy. Click **Apply**.
23. Repeat step 22 until you have configured all the deployment policies.
24. Click **Next**. The “Setup summary” window opens.

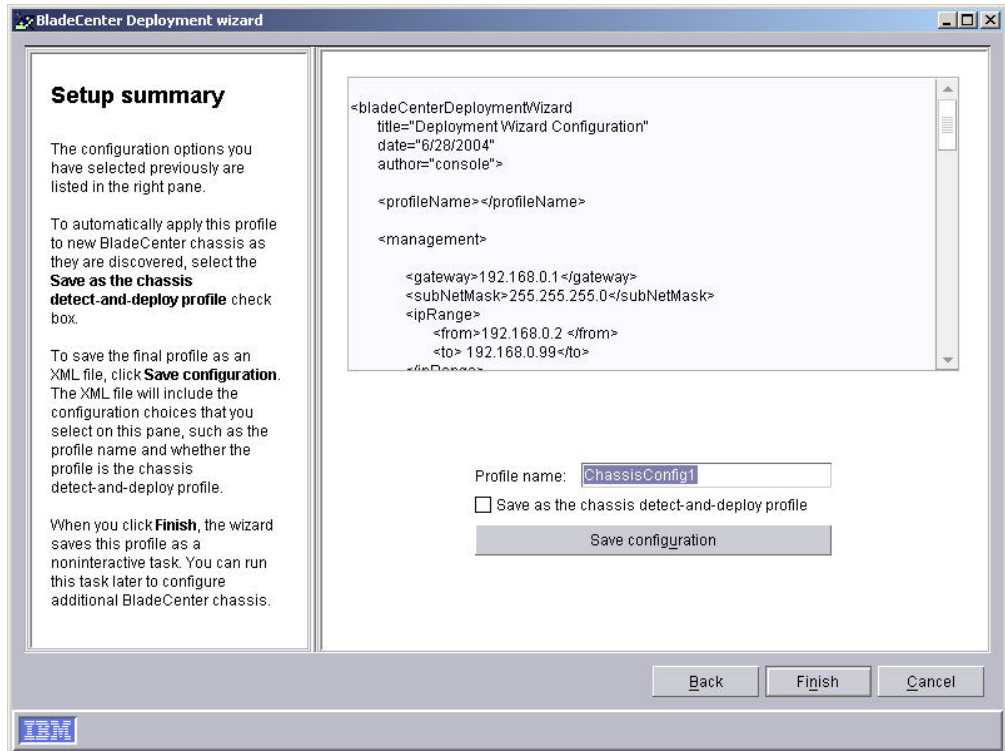


Figure 53. BladeCenter Deployment wizard: “Setup summary” window

25. Review the profile configuration, which is displayed as an XML file in the right pane. The XML file contains all the previously-selected options, but it does not contain the options that you select on this window: profile name and whether the profile is designated as the chassis detect-and-deploy profile.

Complete configuring the profile:

- a. In the **Profile name** field, type a name for the profile. By default, the profile is given the name that you assigned to the management module. When you run the profile against a BladeCenter chassis, the chassis managed object is assigned the profile name.
- b. To apply this profile automatically to all new BladeCenter chassis when they are discovered by IBM Director, select the **Save as the chassis detect-and-deploy profile** check box.

Attention: There can be only one chassis detect-and-deploy profile. If a chassis detect-and-deploy profile already exists and you select the **Save as the chassis detect-and-deploy profile** check box, you will overwrite the existing profile.

- c. To save the profile configuration as an XML file, click **Save configuration**. You can edit the XML file and then use DIRCMD, the IBM Director command-line interface, to create the BladeCenter Deployment wizard profile.
26. Click **Finish**. The profile is created. It appears as a subtask under Deployment Wizard in the Tasks pane of IBM Director Console.

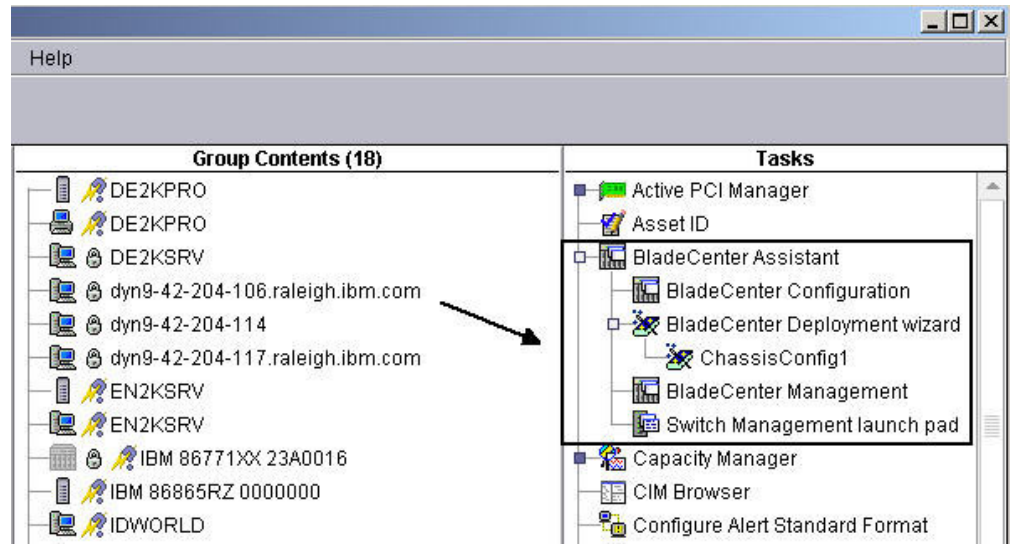


Figure 54. IBM Director Console Tasks pane: BladeCenter Deployment wizard profile

27. To apply the profile, complete one of the following actions:

If you are running the wizard online When prompted, select when you want to run the profile. You can select to run the profile now, schedule a task, or cancel.

If you are running the wizard offline Drag the profile onto the BladeCenter chassis that you want to configure. You can select to run the profile now, schedule a task, or cancel.

Modifying a BladeCenter Deployment wizard profile

Important:

1. If you modify an existing detect-and-deploy profile, be sure to run the profile after you click **Finish**. If you do not run the profile again, the detect-and-deploy profile will not be associated with the BladeCenter chassis to which it was previously applied.
2. When you modify an existing BladeCenter Deployment wizard profile, the wizard fails to save a profile if the profile that you are modifying was running at the time that you clicked **Finish**.

Complete the following steps to modify an existing BladeCenter Deployment wizard profile:

1. In the IBM Director Console Tasks pane, expand the **BladeCenter Assistant** task.
2. To start the BladeCenter Deployment wizard, do one of the following:

To run the wizard off-line Double-click the **Deployment Wizard** task.

To run the wizard on-line Drag the **Deployment Wizard** task onto the BladeCenter chassis that is configured with the profile you want to modify.

The BladeCenter Deployment wizard starts and the “Welcome to the BladeCenter Deployment wizard” window opens.

3. From the **Load existing profile** list in the right pane, select the profile that you want to modify.
4. Click **Next** and continue through the BladeCenter Deployment wizard.
You can edit the information in each BladeCenter Deployment wizard window. For more information about the BladeCenter Deployment wizard, see "Creating and applying a BladeCenter Deployment wizard profile" on page 111.

Note: If the **Use the same IP pool for the management and switch modules** check box was selected when the profile was created, it is not selected now. Instead, the range of IP addresses specified for the IP address pool is displayed for both the management and switch module.

Using an XML configuration file to create or modify a profile

You can use the BladeCenter Deployment wizard to generate an XML file that contains BladeCenter chassis configuration information. To do so, run the BladeCenter Deployment wizard and click **Save configuration** on the "Setup summary" window. You then can edit the XML file in an American Standard Code for Information Interchange (ASCII) text editor and use DIRCMD, the IBM Director command-line interface, to create a profile. You also can use DIRCMD to apply the profile to one or more BladeCenter chassis.

This section contains an example of an XML configuration file and information about the types of data that the file should contain.

Example of an XML configuration file

The following XML configuration file was generated by the BladeCenter Deployment wizard:

```
<bladeCenterDeploymentWizard
  title="Deployment Wizard Configuration"
  date="5/6/2004"
  author="console">
<profileName>ChassisConfig1</profileName>
<management>
  <gateway>192.168.0.1</gateway>
  <subNetMask>255.255.255.0</subNetMask>
  <ipRange>
    <from>192.168.0.2 </from>
    <to> 192.168.0.99</to>
  </ipRange>
</management>
<module>
  <type>BladeCenterManagementModule</type>
  <subProfileName></subProfileName>
  <username>USERID</username>
  <password>PASSWORD</password>
  <name>ChassisConfig1</name>
  <contact>Information Development</contact>
  <protocol>
    <type>snmp</type>
    <communityName>public</communityName>
    <state>enabled</state>
  </protocol>
  <protocol>
    <type>http</type>
    <state>enabled</state>
  </protocol>
  <protocol>
    <type>telnet</type>
    <state>disabled</state>
  </protocol>
  <externalPortState></externalPortState>
</module>
</bladeCenterDeploymentWizard>
```

```

        <detectDeploy>false</detectDeploy>
    </module>
</management>
<switch>
    <gateway>192.168.0.1</gateway>
    <subNetMask>255.255.255.0</subNetMask>
    <ipRange>
        <from>192.168.0.2 </from>
        <to> 192.168.0.99</to>
    </ipRange>
    <module>
        <type>dlink1</type>
    </module>
    <type>nt1</type>
</module>
<module>
    <type>cisco1</type>
</module>
</module>
    <type>qlogic1</type>
</module>
</switch>
<blade>
    <detectAndDeploy>
        <policy>Windows2003</policy>
        <slot>1</slot>
        <slot>2</slot>
        <policy>RHAS30</policy>
        <slot>6</slot>
        <slot>7</slot>
    </detectAndDeploy>
</blade>
</bladeCenterDeploymentWizard>

```

What the XML configuration file should contain

Table 18 contains information about the specific type of data that elements in the XML file can contain.

Table 18. Data types the XML file can contain

Element	Type of data
<gateway> <subNetMask> <ipSingle> <from> <to> <iptrap>	IP address
<type> (Child element of <protocol> only)	One of the following values: <ul style="list-style-type: none"> • snmp • http • telnet
<state>	One of the following values: <ul style="list-style-type: none"> • disabled • enable_read_only • enabled
<externalPortState>	One of the following values: <ul style="list-style-type: none"> • disabled • enabled • untrunked
<detectDeploy>	One of the following values: <ul style="list-style-type: none"> • true • false

Table 18. Data types the XML file can contain (continued)

Element	Type of data
<advancedConfiguration>	String that specifies a fully qualified name of a configuration file. The file must have a CFG extension.
<slot>	A digit in the 1 to 14 range

The elements not specified in the table must either be empty or can contain a string. Review the document type definition (DTD) file for more information. If you installed IBM Director Server in the default location, the abcwizard.dtd file is located in the one of the following directories:

For Linux	opt/IBM/director/classes
For i5/OS	/QIBM/UserData/Director/classes
For Windows	d:\Program Files\IBM\Director\classes

where *d* is the drive letter of the hard disk drive on which IBM Director Server is installed.

Switch Management launch pad subtask

BladeCenter-supported switch modules enable you to use a Web or Telnet interface to configure and manage switches. Some switch vendors might also provide additional advanced switch-specific applications to configure and manage switches.

The Switch Management launch pad subtask detects the supported switch-specific interfaces and applications that are installed and enables you to start them using a supported management tool. For example, you can use the Switch Management launch pad subtask to launch a Web interface to the IBM BladeCenter 4-Port Gb Ethernet Switch Module. You also can launch either a Web or a Telnet interface to the Nortel Network Layer 2-7 GbE Switch Module for IBM @server BladeCenter.

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

Chapter 8. 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 also can use to monitor resource utilization, Capacity Manager can be used to capture resource-monitor trends and for longer-term resource-utilization monitoring. (See “Viewing available resource monitors” on page 217 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 are currently active on a managed system or group. Also, you can activate and deactivate monitors on a managed system. Performance-analysis monitors are a subset of resource monitors that are considered critical and are used to make performance recommendations. 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

Note: You must turn on all four types of performance-analysis monitors for a report to display a Performance Analysis Recommendation.

Capacity Manager automatically discovers new Disk or LAN resource monitors and removes monitors for devices that no longer exist. Performance-analysis monitors for Windows network adapters and physical disks are discovered when the Windows network adapters and physical disks are added to the managed system. If a checked network adapter or physical disk has been removed, Capacity Manager removes the corresponding performance-analysis monitor from the monitor list 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 on which the Capacity Manager Agent is installed. The “Monitor Activator” window opens.

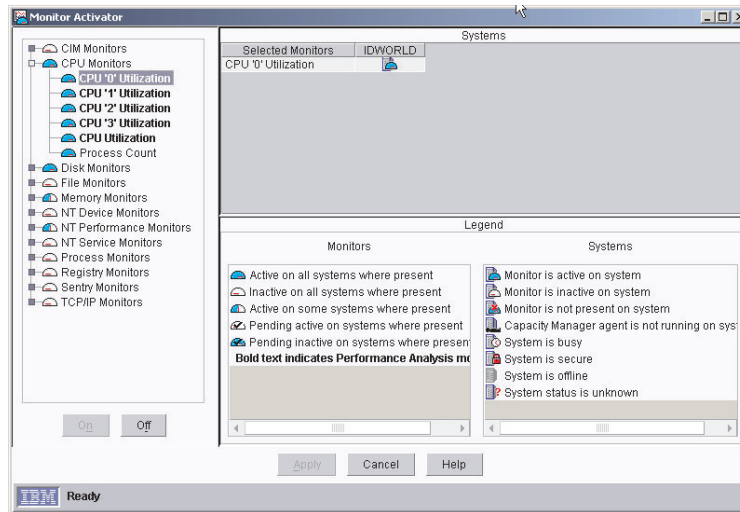


Figure 55. “Monitor Activator” window

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 55, **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. For safety, 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 reactivate it.

Identifying bottlenecks

When you schedule Capacity Manager to check periodically for bottlenecks, or when you select to generate a report, 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 (see “Setting monitor options” on page 142 for more information), but you cannot change the default settings without impairing the performance-analysis function.

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

- CPU (microprocessor)
- 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 occur also. 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. Because systems and devices often interact in this way, each combination of bottlenecks (that is, microprocessor, 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 the following methods to determine whether a managed system or group has bottlenecks:

- Schedule performance analysis to check for bottlenecks and generate an event when a threshold is exceeded or met. (See “Receiving automatic notification of a bottleneck.”)
- Using the Report Generator function, generate a report immediately.

If a bottleneck is found, in the performance-analysis section of the report, the monitor name is shown in bold and in red, and recommendations for correcting the bottleneck are made.

If no bottleneck is found, 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, 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 a Windows or Linux operating system.

Scheduling to check for bottlenecks

You can schedule a report of 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 make sure that the **Generate bottleneck events** check box is selected for the report definition that 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 event actions.

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 that 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 that you have 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 provides information about 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 that you selected to monitor using the Hourly Bottleneck Events report option that is described in the preceding section. For more information about creating and implementing event action plans, see Chapter 4, “Managing and monitoring systems with event action plans,” on page 55.

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**.

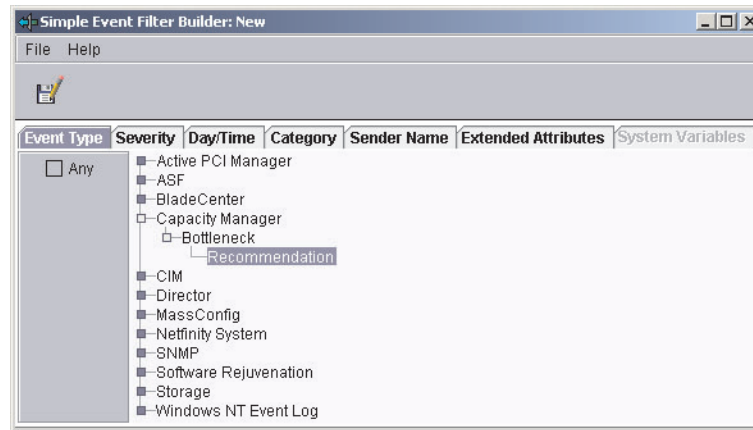


Figure 56. “Simple Event Filter Builder” window

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 that 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 that 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 is saved automatically to the IBM\Director\reports directory (unless you specify another directory in the report definition). Click **Execute Now** to generate the report now, or **Schedule** to set a time to generate the report.

Creating a report definition

Complete the following steps to create a new report definition:

1. Run the **Monitor Activator** subtask on a managed system or group to activate the monitors for that system or group. For more information about the **Monitor Activator** subtask see “Viewing and activating monitors” on page 127.

- Expand the **Report Generator** subtask; then, double-click **New Report Definition**. The “Report Definitions” window opens.

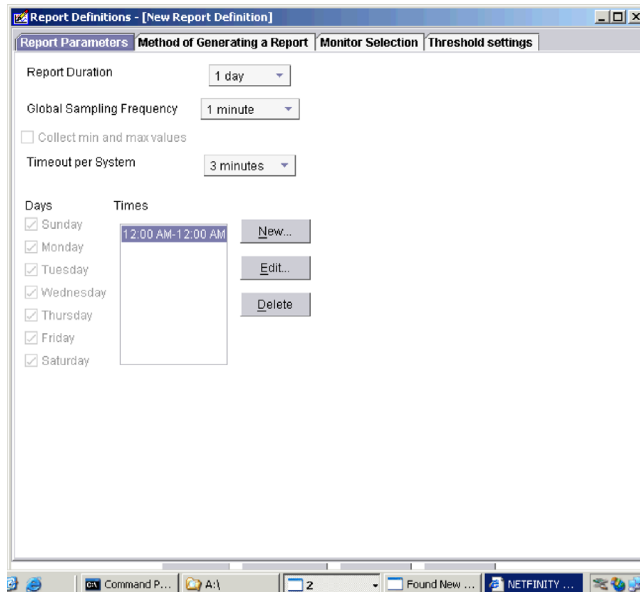


Figure 57. “Report Definitions” window: Report Parameters page

- Click the **Report Parameters** tab.
- Select the report duration, the global sampling frequency, and whether to collect min and max values.

Note: Selecting the **Collect min and max values** check box specifies that the minimum and maximum data points for each sample are collected. An advantage of 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.
- Click **New** to specify the time of the report using the “New Time Interval” window.

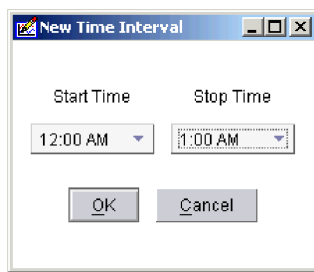


Figure 58. “New Time Interval” window

7. Click the **Method of Generating a Report** tab.

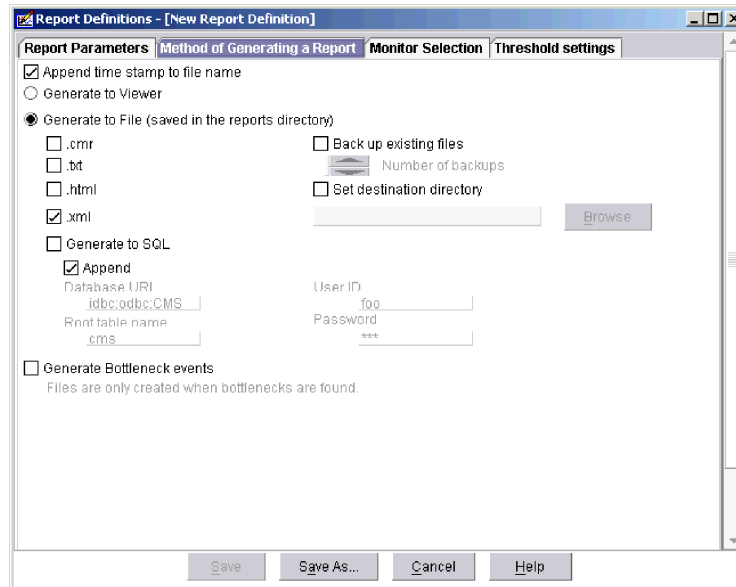


Figure 59. “Report Definitions” window: Method of Generating a Report page

8. Select **Generate to Viewer** or **Generate to File**.
9. Select the file format check boxes to generate the file in the selected formats. The default file format is XML.
10. If you select **Generate to SQL**, type the database URL and root table name in the applicable fields.

Note: Generating a report in SQL format is available on Windows only.

11. If you use SQL authentication, type the user ID and password for the SQL connection in the applicable fields.
12. Select **Generate Bottleneck events** to generate an event in the IBM Director event log.
13. Select **Back up existing files** to archive saved reports.
14. Select **Number of backups** to set the number of reports to keep.
15. Select **Set destination directory** to set the destination directory.

Note: The default destination directory is IBM\Director\reports.

16. Click the **Monitor Selection** tab.

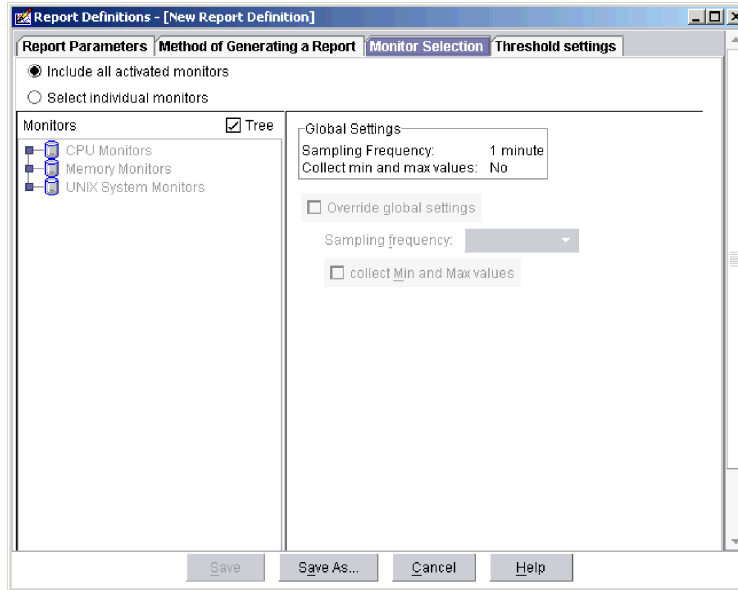


Figure 60. "Report Definitions" window: Monitor Selection page

17. Select **Include all activated monitors** to include all active monitors in the report, or **Select individual monitors** to select specific monitors.
18. Click the monitors in the **Monitors** field, and then click **Include** or **Exclude** to include or exclude the selected monitors.
19. Select the **Override global settings** check box to use a different sampling frequency than is shown.
20. Click the **Threshold Settings** tab.

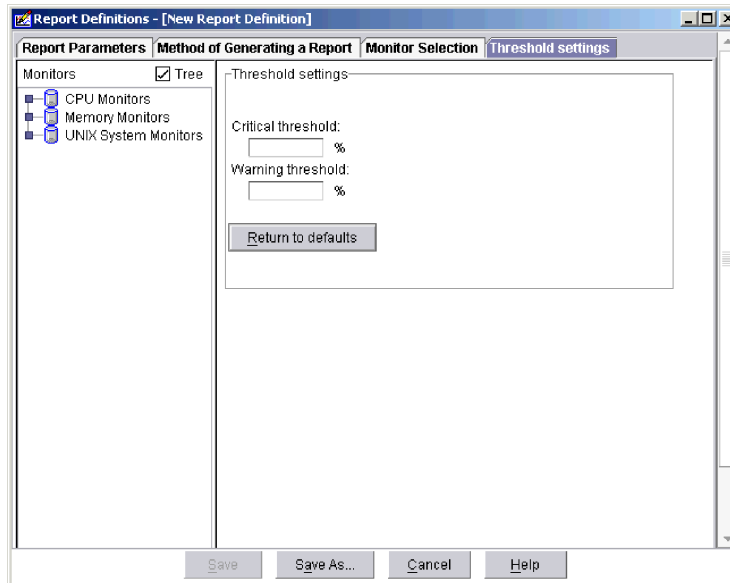


Figure 61. "Report Definitions" window: Threshold Settings page

Note: A threshold setting applies to all managed systems included in the report definition.

21. In the **Critical threshold** field, type the value of the critical threshold.

22. In the **Warning threshold** field, type the value of the warning threshold.
23. Click **Return to defaults** to set the threshold values to default values.
24. Click **Save As**. In the “Save As” window, type the name of the report definition and click **OK**.

After you have customized a report definition, you can generate a report that includes only those parameters that 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 groups.
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 40.)

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.

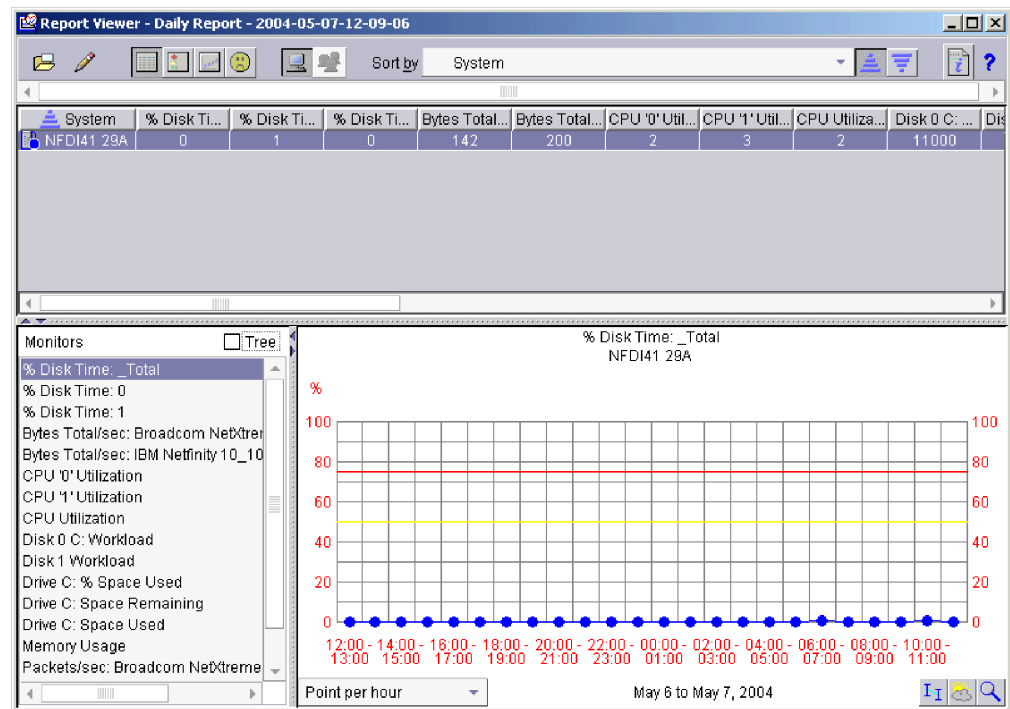


Figure 62. “Report Viewer” window

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 the following 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.



Icon 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 19.)



System View

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










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 Table 19.

Table 19. Performance-analysis icon descriptions

Icon	Description
	The performance-analysis report is ready and will be displayed soon.
	Performance analysis is complete. The report viewer waits while the results are loaded for viewing.
	The performance-analysis report is ready and has no bottleneck recommendations, although the Details section might have information about 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) → Enable Performance Analysis and generate the report again.
	The performance-analysis report could not be prepared. You are missing one or more critical monitors, or you have less than 2 hours of collected data.

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 that is 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” window displays a graph of the monitor that you selected in the Monitors pane. If you click  (System View), a line graph of the performance of the managed system is displayed. If you click  (Group mode), a graph of the performance of all the managed systems in the group is displayed, 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 function uses an average of the raw data points to present the requested number of points for a period of time.



Trend

Displays a trend graph of the data.



Forecast

Displays predicted data according to the least-squares linear regression calculations of future managed-system performance. (See “Viewing a performance forecast graph” on page 139 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 have 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 export the graph pane as a GIF file, in the “Report Viewer” window,

click  (File) → **Export graph to local GIF** or  (File) → **Export graph to remote GIF**. To print the performance-analysis report, click  (File) → **Print** → **Performance analysis report**.

A report that is 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. Right-click **Report Viewer** and click **Open**. 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.

Note: If you use the Report Viewer to display a report that was saved in XML format, you can adjust the threshold settings on performance-analysis monitors.


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 before 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 selected monitor.

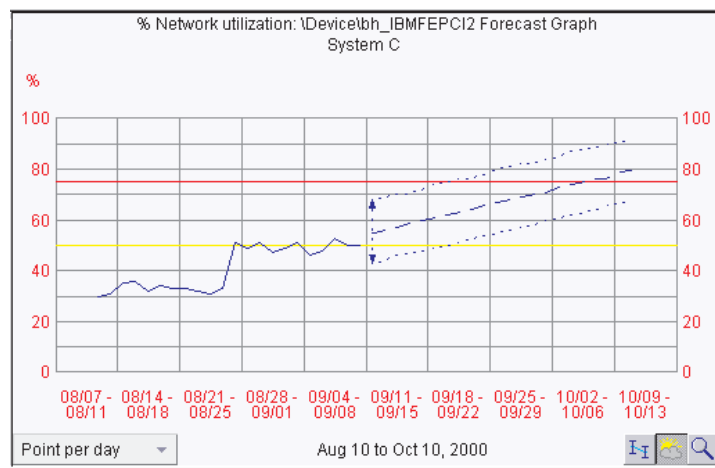


Figure 63. “Report Viewer” window: Lower-right pane displaying a performance-forecast graph

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

To access the “Settings” window through the “Report Viewer” window, click  (Edit) → **Settings**. The “Settings” window consists of three tabbed pages:

Graph Configures the appearance of the graph in the Graph pane.

Window

Configures the appearance of the viewer.

Monitors

Configures the threshold settings for each monitor.

Setting the graph display options

Complete the following steps to set display options for the graphs in a report:

1. Click the **Graph** tab. The Graph page is displayed.

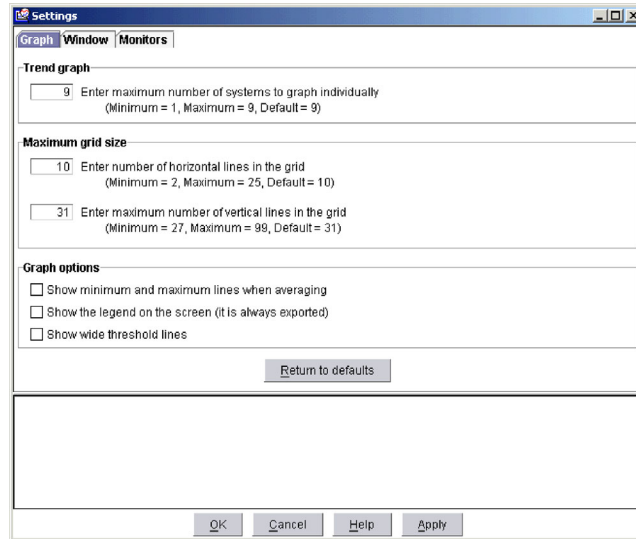


Figure 64. “Settings” window: Graph page

2. Use the Graph page to perform the following tasks:
 - Set the maximum number of systems to individually display on the graph before combining results into a trend
 - Set the dimensions of the grid size
 - Set graph options including displaying maximum and minimum lines for averaged values, displaying the legend on the screen, and setting the thickness of threshold lines
3. Click **Return to defaults** to set the Graph page to the default settings.

Setting the “Report” window display options

Complete the following steps to set display options for a “Report” window:

1. Click the **Window** tab. The Window page is displayed.

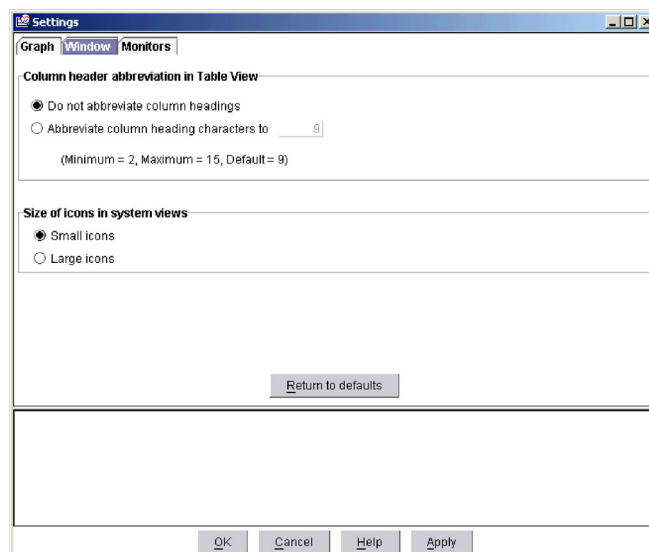


Figure 65. “Settings” window: Window page

2. Select whether to abbreviate column headings. If you choose to abbreviate column headings, type the maximum number of characters in the field.
3. Select **Small icons** or **Large icons**.
4. Click **Return to defaults** to set the Window page to the default settings.

Setting monitor options

You can adjust the threshold settings on performance-analysis monitors to conduct resource planning to discover if a bottleneck appears when capacity is set to a given value.

Complete the following steps to set threshold values and display options for monitors:

1. Click the **Monitors** tab. The Monitors page is displayed.

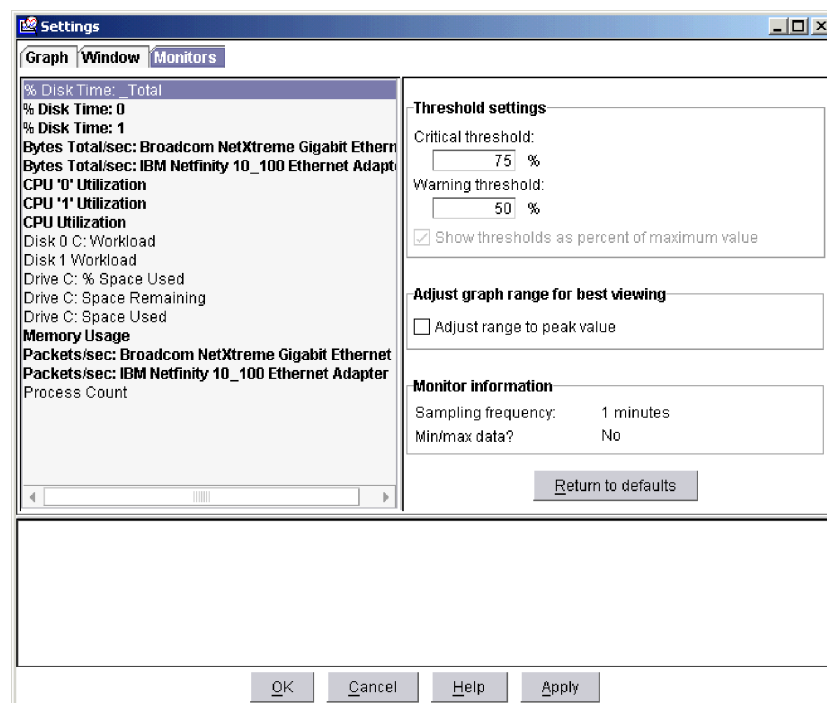


Figure 66. “Settings” window: Monitors page

2. Click a monitor in the left pane to select it.
3. (Optional) Type custom values for the warning threshold and critical threshold settings in the **Threshold settings** fields.

Note: You cannot change the default settings without impairing the performance-analysis function.

4. Select the **Show thresholds as a percent of maximum value** check box to display thresholds as a percentage of the maximum value on the report.
5. Select the **Adjust range to peak value** check box to set the peak value that is reported as the vertical range value of the graph.
6. Click **Return to defaults** to set the Monitors page to the default settings.

Chapter 9. CIM Browser

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

To provide data through the CIM Browser task, a managed system must have an installed Common Information Model Object Manager (CIMOM) 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.

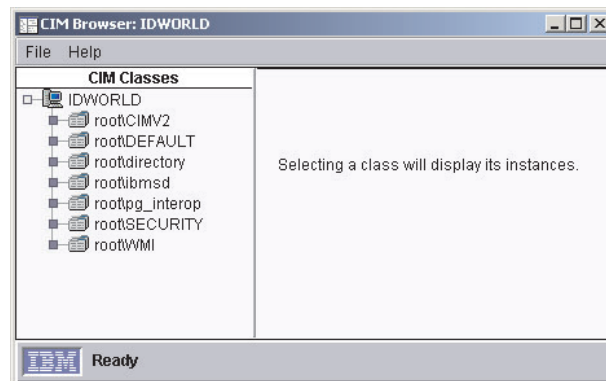


Figure 67. “CIM Browser” window

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 are 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 on or turn off the displaying of managed-system classes, right-click a managed system and click **Show System Classes**. A managed-system class is 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 and then expand a name space to display its classes. The name space that contains the IBM-specific classes is root\IBMSD.

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. 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 canceled. Therefore, you should avoid attempting to view instances of root\cimv2:CIM_DirectoryContainsFile and root\cimv2:Win32_Subdirectory on managed systems running Windows, or root/ibmsd for IBMP5G on managed systems running Linux.

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 that 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 that 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, type the arguments in the input 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 only the instances, properties, and methods that are associated with a specified class on the selected managed system are displayed.
- A user-selected method that 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 that are 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 that you want to run.

Chapter 10. 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. The following criteria must be met before a managed system is recognized by IBM Director Server as ASF-capable:

- The managed system must have an ASF-capable NIC installed with the applicable device drivers.
- In IBM Director Console, inventory collection must be performed on the managed system. If the managed system supports ASF 1.0 it is added to the Systems with ASF group. If the managed system supports ASF 2.0 it is added to both the Systems with ASF group and the Systems with ASF Secure Remote Management group.

Note: You can apply a Configure ASF task to a group of managed systems using Mass Configuration. For more information, see “Mass Configuration” on page 51.

Configuring Alert Standard Format

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, select the **Enable ASF Hardware** check box.
3. (Optional) Select the **Enable All Platform Event Traps** check box.
4. Select the **Enable Remote Management** check box.

Note: This check box enables the secure remote power management functions but does not affect your ability to set authentication keys on the Remote Management page. This option is available only if the managed system is a member of the Systems with ASF Secure Remote Management group.

5. Click the **Configuration** tab.
6. Type all the required settings.

Note: The Alert Standard Format Agent does not perform checks to determine whether 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 whether the correct IP address for the management server has been configured on the managed system.

7. Click **Apply**.

Configuring Secure Power Management

You can configure a managed system to use authentication keys to secure the power management access. To set up a managed system for secure remote management, you must complete the following procedures:

- In IBM Director Console, create a set of authentication keys and save the keys in IBM Director Server (see page 148).

- Using Web-based Access to access the managed system, type the same authentication keys and save the authentication keys to the NIC of the managed system (see page 150).
- (Optional) Test the Secure Power Management configuration (see page 150).

Creating authentication keys and saving the keys in IBM Director Server

Complete the following steps to create a set of authentication keys and save the keys in IBM Director Server:

1. In IBM Director Console, drag the Configure ASF task onto the managed system. The “Alert Standard Format” window opens.
2. Click the **General** tab.

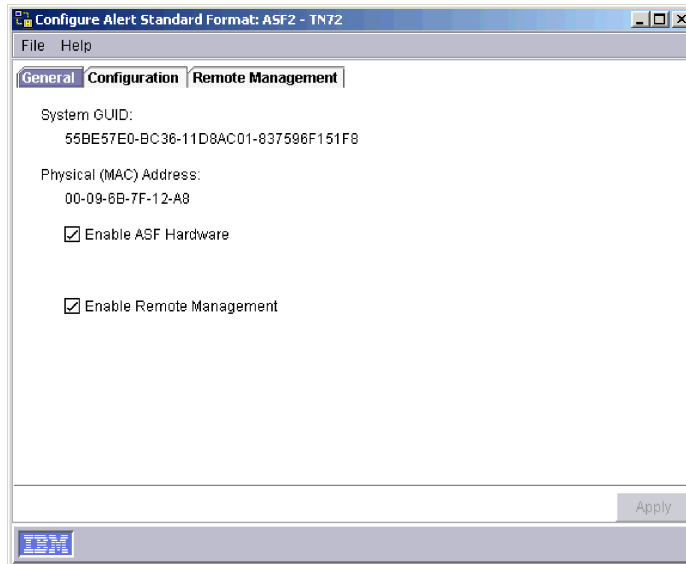


Figure 68. “Configure Alert Standard Format” window: General page

3. Select the **Enable ASF Hardware** check box.
4. Select the **Enable Remote Management** check box.
5. Click the **Configuration** tab.

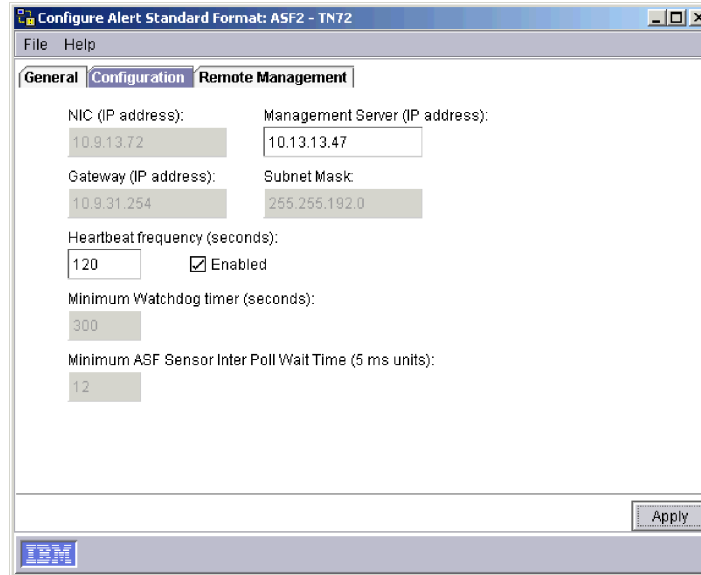


Figure 69. “Configure Alert Standard Format” window: Configuration page

6. If this is the first time ASF is being configured on IBM Director Server, type the IP address of the management server in the **Management Server (IP address)** field.
7. Click the **Remote Management** tab.

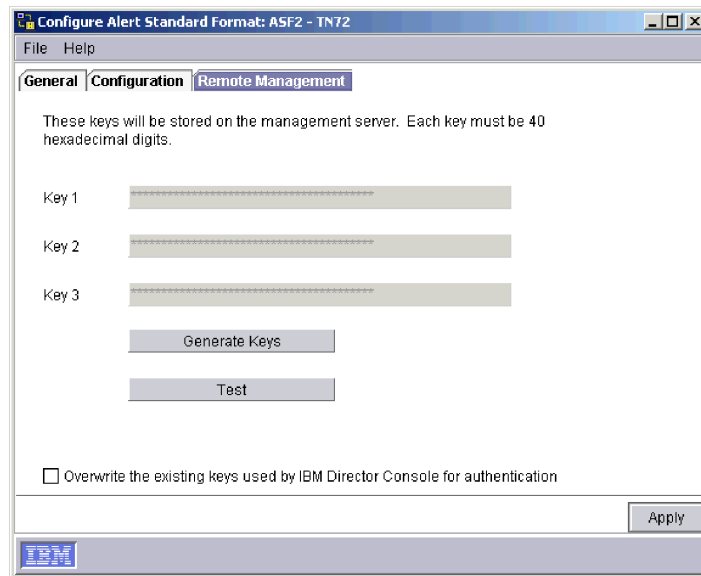


Figure 70. “Configure Alert Standard Format” window: Remote Management page

8. Click **Generate Keys** to create a new set of three authentication keys.

Notes:

- a. This button is not available if the **Overwrite the existing keys used by IBM Director Console for authentication** check box is cleared. This check box is not visible if the three authentication keys have not been saved already.

- b. Clicking **Apply** changes the display of the newly created authentication keys to asterisks. If you want to copy the authentication keys to paste them into Web-based Access or IBM Director Console for another system, do so before you click **Apply**.
9. Click **Apply** to save any entries or changes that you have made.

Saving the authentication keys to the managed system

Complete the following steps to save the authentication keys to the managed system:

1. Using Web-based Access, connect to the managed system.
2. Click the **Tasks** tab.
3. Click the **ASF** task.
4. Click the **Remote Management** tab.

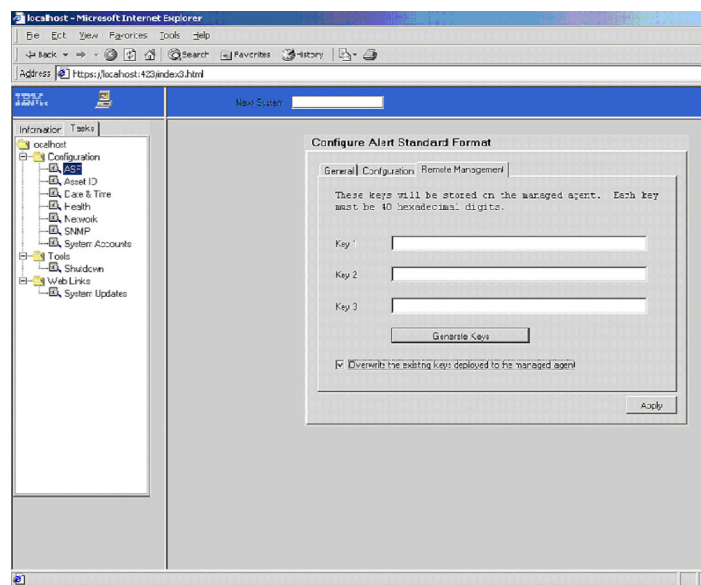


Figure 71. Web-based Access, saving authentication keys

5. Type or paste the three authentication keys into the **Key 1**, **Key 2**, and **Key 3** fields.
6. Click **Apply** to save any entries or changes that you have made.

Testing the Secure Remote Management configuration

Complete the following steps to test the Secure Remote Management configuration:

1. In IBM Director Console, drag the Configure ASF task to the managed system. The “Alert Standard Format” window opens.
2. Click the **Remote Management** tab.
3. Click **Test** to test whether the set of three authentication keys that are saved in IBM Director Server matches the set of authentication keys on the managed system.

Note: The **Test** button is not available if the three authentication key fields are empty.

Using Secure Remote Management

Complete the following steps to use the power-management commands:

1. In the IBM Director Console Groups pane, click the **Systems with ASF Secure Remote Management** group. The managed systems are displayed in the Group Contents pane.
2. (Optional) Click multiple managed systems in the Group Contents pane.
3. Right-click the managed system or systems in the Group Contents pane and click **Power Management**; then, click the command that you want to perform on the managed system or systems.

Chapter 11. DMI Browser

The Desktop Management Interface (DMI) Browser task provides in-depth information about DMI components. DMI is used primarily for systems management, and 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 <http://www.smartdmi.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 are 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 the shortcut is created, you can use it on a managed system to view information that is 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 that is 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 that contains the same group class, separately tabbed pages are displayed for each component that contains 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 that contain the group class, the following error message is displayed: The targeted system does not support this class.

Chapter 12. Event Log

You can use the Event Log task to view details about all events or subsets of events that have been received and logged by IBM Director Server. You can view all events or view events for a managed system or by filter criteria.

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

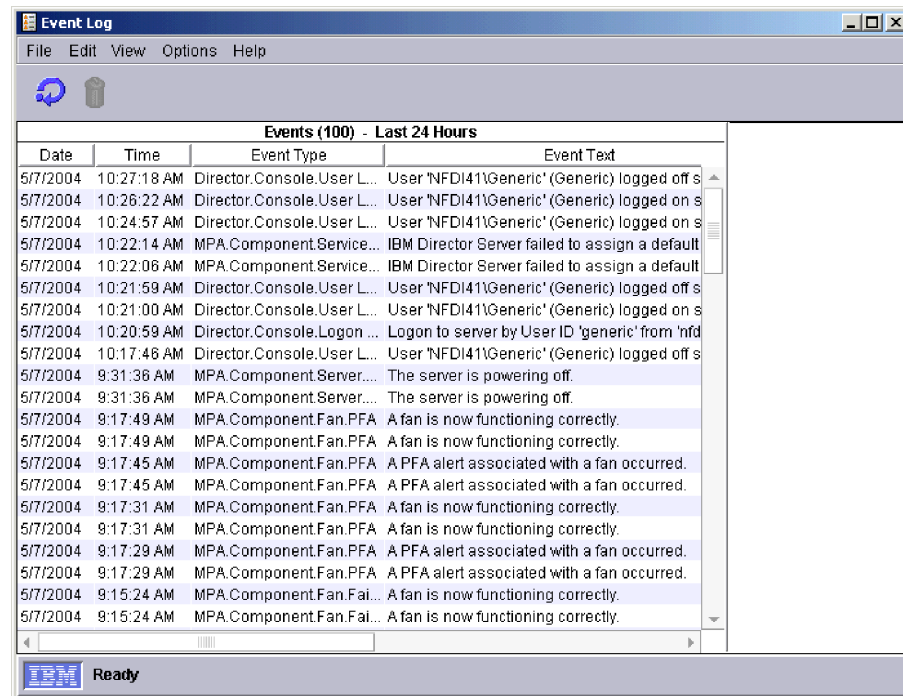


Figure 72. “Event Log” window displaying all events for all managed systems

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 might be displayed, depending on the display options that are set. The default number of events that is displayed is 100, and the default time range is events that have occurred in the past 24 hours.

Complete the following steps to view the currently set time range or change the time range displayed:

1. In the IBM Director Console Tasks pane, double-click the **Event Log** task. The “Event Log” window opens.
2. Click **Options** → **Set Time Range**. The “Set Time Range” window opens.

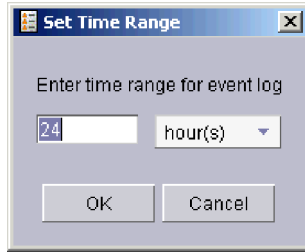


Figure 73. “Set Time Range” window

3. Type the number of units of time in the left field.
4. Select *hour(s)*, *day(s)*, or *week(s)* from the right list.
5. Click **OK**.

Complete the following steps to view the number of events that are displayed or change the number of events that are displayed:

1. In the IBM Director Console Tasks pane, double-click the **Event Log** task. The “Event Log” window opens.
2. Click **Options** → **Set Log View Count**. The “Set Log View Count” window opens.

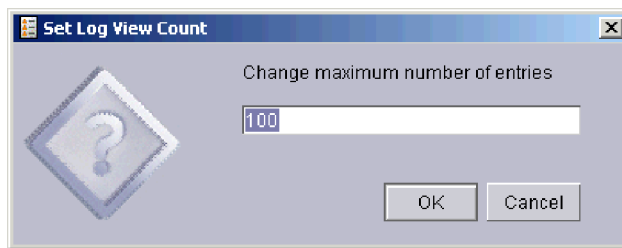


Figure 74. “Set Log View Count” window

3. Type the number events to display in the event log in the **Change maximum number of entries** field.
4. Click **OK**.

You can set the color of types of events in the event log, both by severity and by category. For example, complete the following steps to set the color of a Critical event to blue:

1. In the IBM Director Console Tasks pane, double-click the **Event Log** task. The “Event Log” window opens.
2. Click **Options** → **Customize Color** → **Severity** → **Critical**. The “Choose the Color for Critical” window opens.

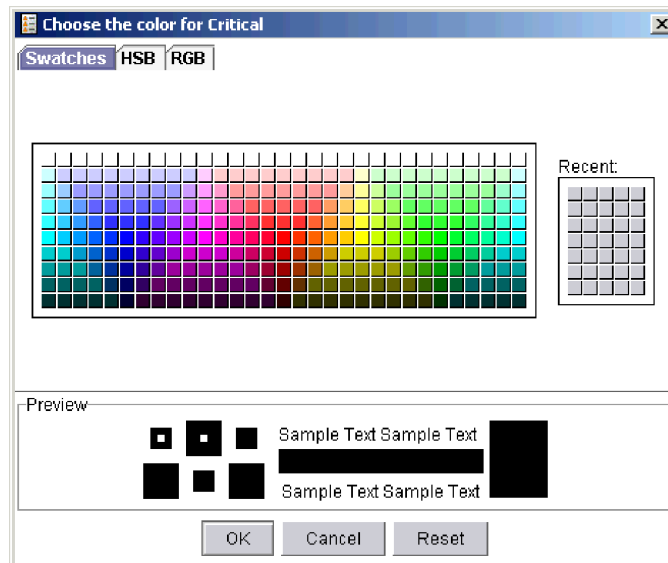


Figure 75. “Choose the Color for Critical” window

3. In the **Swatches** page, click the color you want Critical events to display as shaded in the event log.
4. Click **OK**.

Changing event log settings

You can change the number of events that the event log stores.

Complete the following steps to change the number of events in the event log:

1. In IBM Director Console, click **Options** → **Server Preferences**. The “Server Preferences” window opens.
2. Click the **Event Management** tab to display the Event Management page.

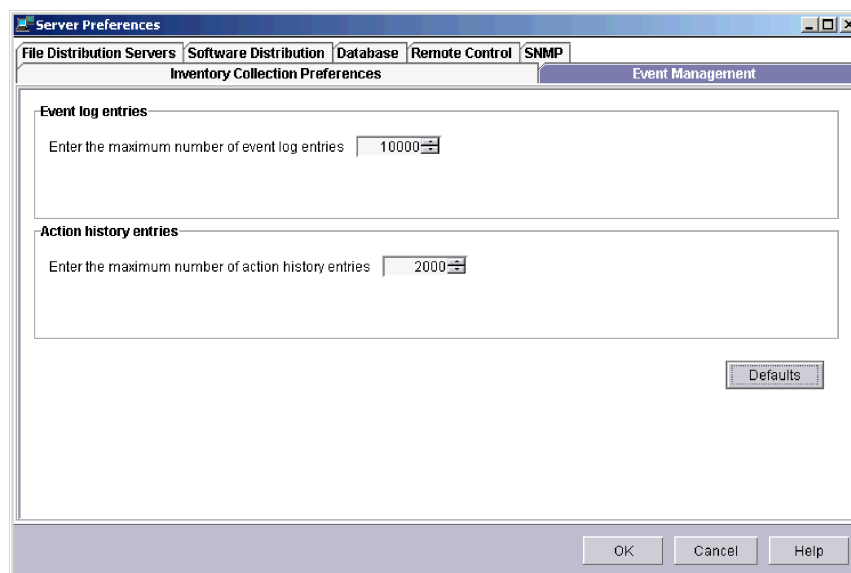


Figure 76. “Server Preferences” window: Event Management page

3. Type the maximum number of event log entries in the **Enter the maximum number of event log entries** field.
4. Click **OK**.

Exporting events from the event log

You can export an event or events that are 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 that 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**.

Chapter 13. File Transfer

The File Transfer task is a secure alternative to File Transfer Protocol (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 the following systems:

- The management console and the management server
- The management console and a managed system
- The 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.

Note: You can use the File Transfer task with only one system at a time. You cannot transfer files to multiple systems or to a group.

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.

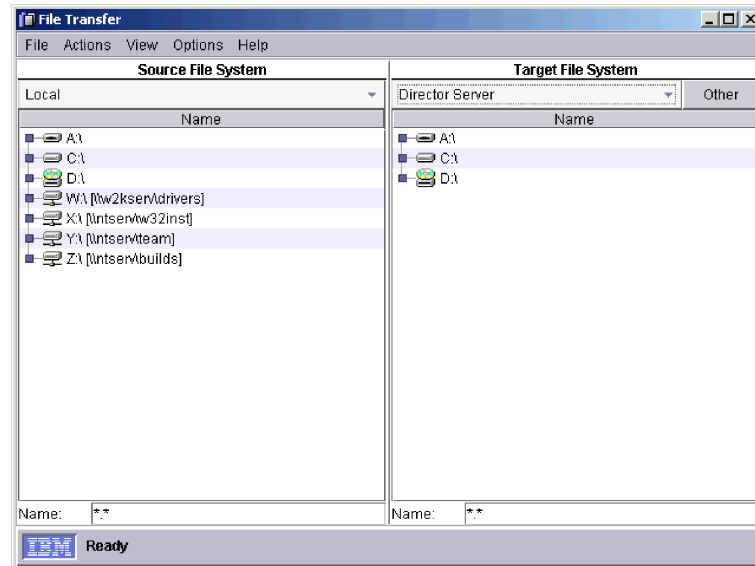


Figure 77. “File Transfer” window

Transferring files

To transfer files or subdirectories, expand a drive in the Source File System pane or Target File System pane. The contents of that drive are displayed, showing subdirectories and files. Use one of the following procedures:

- From the Source File System pane, drag the files or subdirectories that you want to transfer onto the drive or subdirectory that you want the files to be on in the Target File System pane.

- From the Target File System pane, drag the files or subdirectories that you want to transfer onto the drive or subdirectory that you want the files to be on in the Source File System pane.

Using the wild-card function, you can filter which files are displayed in the Source File System or Target File System panes. 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.

Note: The “Choose Target” window does not display locked managed systems.

2. Select the managed system that 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 five managed systems to the list at a time. If you add more than five, the managed system that was 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.

Attention: Files or directories that are present only in the selected files, directories, or drives on the target managed system, but are not present in the selected files, directories, or drives on the source managed system, are deleted after synchronizing.

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. If you receive a message indicating that the selected names are different, click **Yes** to continue. The selected files, directories, or drives are now synchronized.

Disabling TCP session support

By default, the File Transfer task uses TCP. If you disable TCP session support on a managed system, the File Transfer task uses User Datagram Protocol (UDP).

Complete the following steps to disable TCP session support on a managed system running Windows:

1. Using a text editor, create or edit a file named TCP.INI in the IBM\Director\data directory.
2. Add the following line to the file:
`SESSION_SUPPORT=0`
3. Save the file.
4. Stop and restart IBM Director Agent on the managed system.

Note: The file name is TCPIP.INI if TCPIP (All Adapters) is enabled in the “Network Driver Configuration” window. If an individual adapter is enabled, for example TCPIP1, you must create or edit a file named TCPIP1.INI for that adapter. Repeat the procedure for each individual adapter.

Complete the following steps to disable TCP session support on a managed system running Linux, UNIX®, or i5/OS:

1. Using a text editor, edit a file named TCPIPNET.Ext in the IBM\Director\classes\extensions directory.
2. Locate the following line in the file:
`net.session.classname=com.tivoli.twg.netipc.TWGTCPsocketImplFactory`
3. Insert the following character at the beginning of this line:
#
4. Save the file.
5. Stop and restart IBM Director Agent on the managed system.

Chapter 14. 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. If a system or device generates hardware events for more than one group, the system or device is added to the group of the highest-severity hardware event that is generated.

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 next to the managed system or device in the Group Contents pane. See Figure 78 for an example.

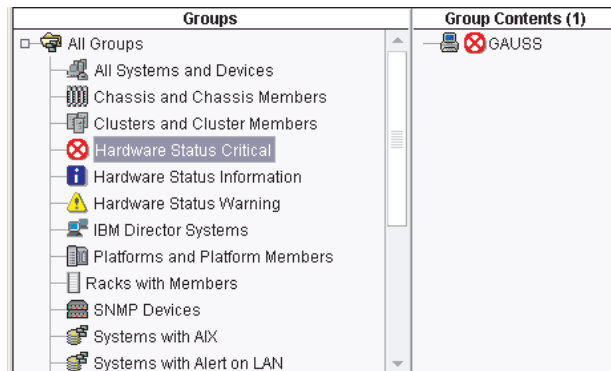


Figure 78. IBM Director Console displaying hardware-status groups

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. See Figure 79 for an example.



Figure 79. IBM Director Console, hardware-status icons located in the bottom-right portion

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.

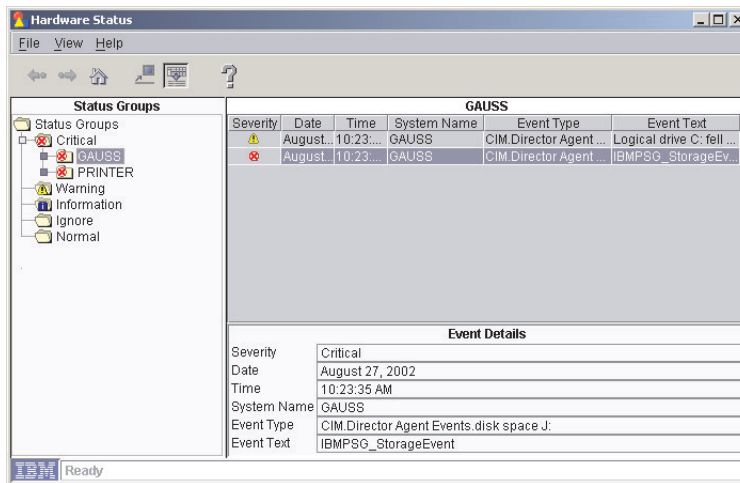


Figure 80. “Hardware Status” window showing all hardware-status events

You also can view the event details for an individual managed system or device by double-clicking the hardware-status icon next to the system or device in the Group Contents pane of IBM Director Console (for an example of a critical icon that is displayed next to a managed system, see Figure 78 on page 163). A “Hardware Status” window such as the one in Figure 81 opens.

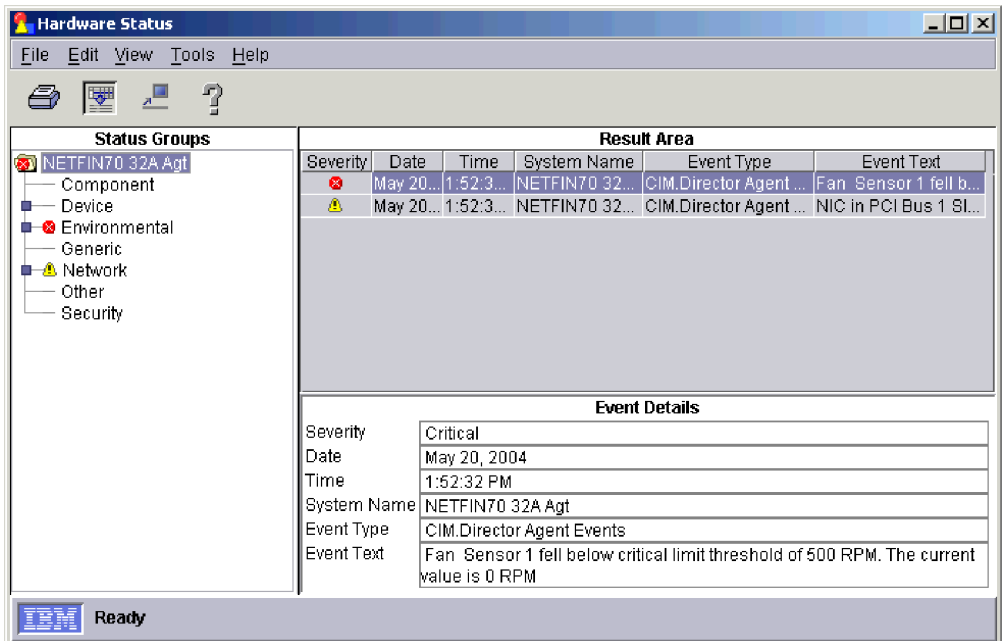


Figure 81. “Hardware Status” window showing events for a single managed system

To set a managed-system or device status to normal and ignore all future hardware events that are 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**.

Chapter 15. Inventory

You can use the Inventory task to collect data about the hardware and software that is 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 feature (see “Scheduler” on page 40 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 about properties of a managed system, such as remaining disk space. You can use a standard query that is provided or create your own custom query.

You can use the inventory-software dictionary to track the software that is installed on your managed systems. You do not specify drives or directories that you want the Inventory task to search during the software-inventory collection process; 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 that is included with IBM Director, you can edit the software-dictionary file to update your software inventory. Typically, this includes software that is developed internally in your organization or a new version of software that is released after this version of IBM Director. See “Viewing and editing the inventory-software dictionary” on page 170 for more information.

Viewing inventory data

You can use any query from the Available Queries pane in the “Inventory Query Browser” window to view inventory data. The Standard folder contains predefined queries, and 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.

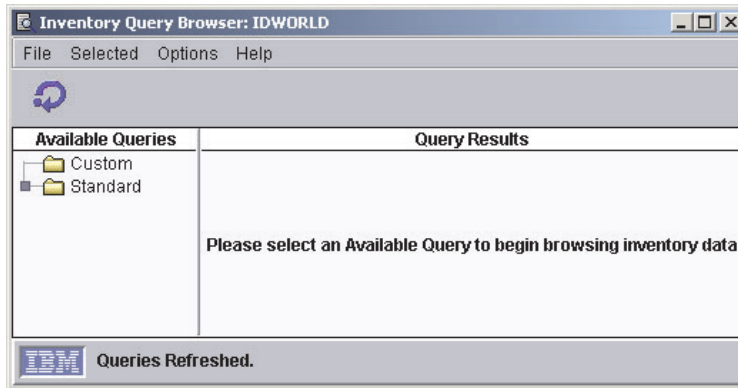


Figure 82. “Inventory Query Browser” window

The “Inventory Query Browser” window 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 about 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 feature. See “Scheduler” on page 40 for more information. 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 the IBM Director Console Tasks pane, right-click the **Inventory** task; then click **Build Custom Query**. The “Inventory Query Builder” window opens.

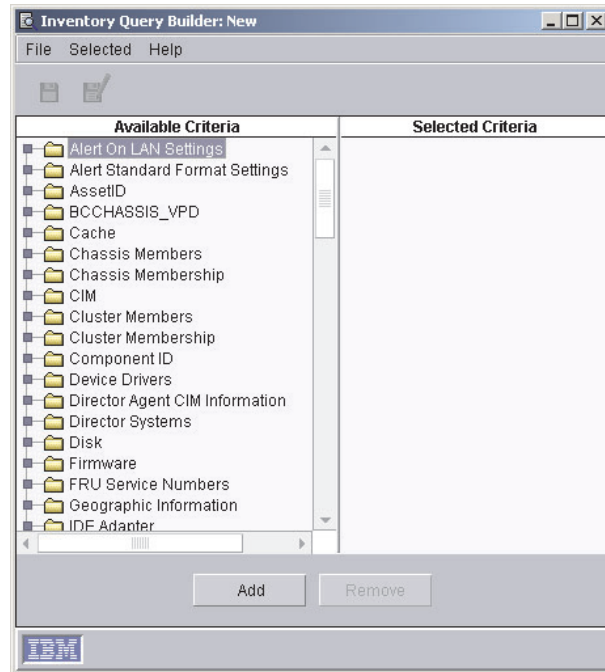


Figure 83. “Inventory Query Builder” window

2. In the Available Criteria pane, drag the data items that 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 in which 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 about that query, a message is displayed.

Editing a custom query

You can modify a query that 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 that 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.

Note: If you edit and save a custom query, the Inventory task might not be able to interpret the new query and the saved query might not be displayed in the Available Queries pane of the “Inventory Query Browser” window. Restart the Inventory task to open the “Inventory Query Browser: All Systems and Devices” window. The saved query is displayed in the Available Queries pane.

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 that you want to export.
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.

Software-inventory collection is disabled by default. Complete these steps to enable software-inventory collection:

1. In the IBM Director Console, click **Options** → **Server Preferences** to display the “Server Preferences” window.
2. Click the **Inventory Collection Preferences** tab to display the Inventory Collection Preferences page.
3. Select the **Collect Software Data** check box.
4. Click **OK**.

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 is displayed 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.

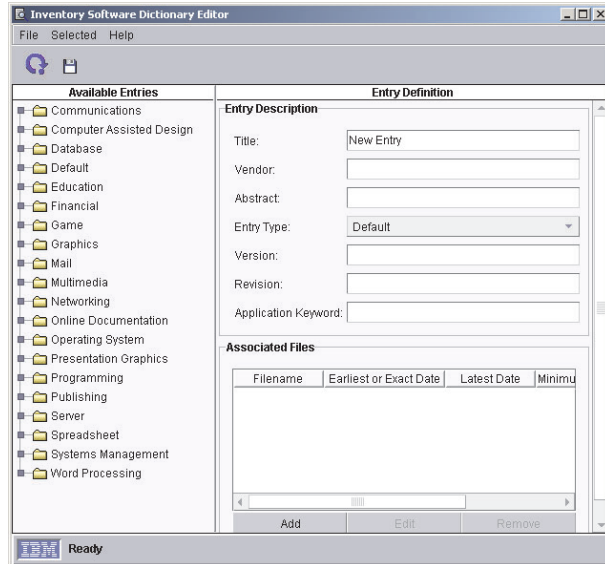


Figure 84. “Inventory Software Dictionary Editor” window

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

The **Title** and **Entry Type** fields are the only required fields. However, any information that 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 you are collecting inventory data. The information that is 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 through step 6.
8. Click the **Save Entry** icon to save the entry. The definition is added immediately to the software dictionary. The next time inventory data is collected, the data that 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 that are 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 84 on page 171.)
2. In the Entry Definition pane, use the **Title** and **Entry Type** fields to identify and classify each entry that you create in the inventory-software dictionary. You also can complete the other fields as needed.
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 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 that identifies the file (or set of files, if you specified more than one file) that corresponds 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 that is 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 that you created; then, click **Add** to add the entry to the Selected Criteria pane.
13. Locate and click the second software-dictionary entry that 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 that you selected are located on that managed system or device.
15. Locate and add the rest of the entries that you created. For each subsequent entry that 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 that 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 that 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.

Chapter 16. 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)
- Intelligent Platform Management Interface (IPMI) Baseboard Management Controller
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

Using Management Processor Assistant, you can configure, monitor, and manage the service processors in xSeries and Netfinity servers.

With Management Processor Assistant, you can view environmental data such as temperature, voltage, and fan speeds; view server and component data; and view the event log that is stored on the service processor. You also can configure systems-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

Complete the following steps to start a Management Processor Assistant subtask:

1. In the IBM Director Console Tasks pane, expand the **Management Processor Assistant** task. There are three subtasks:
 - Communications
 - Configuration
 - Management
2. Drag the applicable subtask onto a supported managed object. The “Management Processor Assistant” window opens.

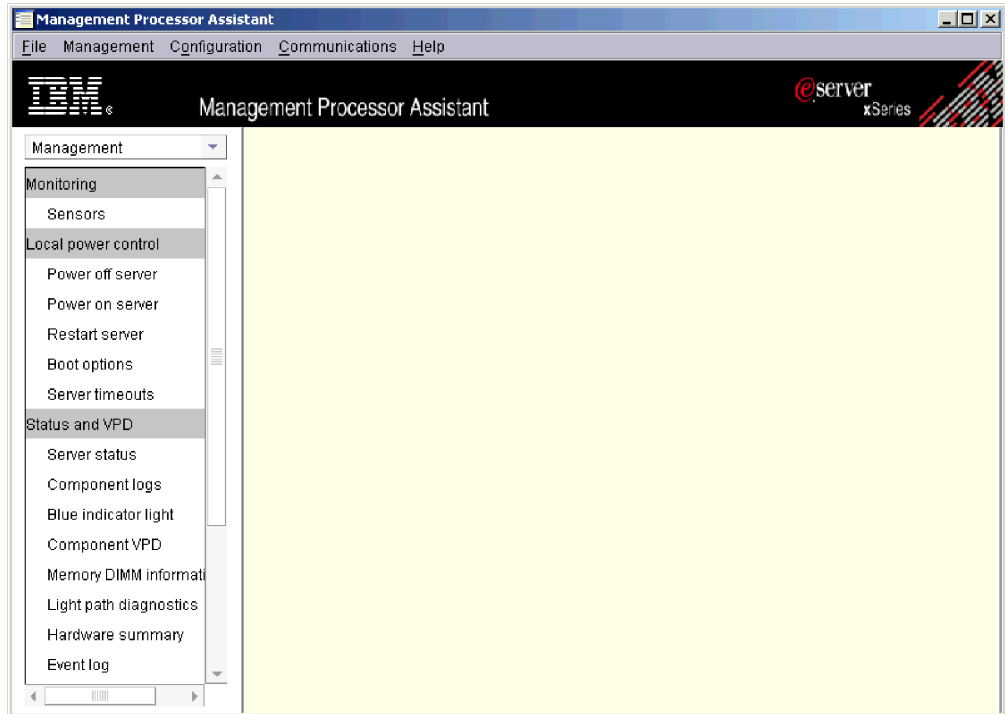


Figure 85. “Management Processor Assistant” window: Management subtask

The left pane contains menu options for the subtask that you selected.

After you start the Management Processor Assistant subtask, use the menus and commands within the window to view, configure, and manage the service processor.

Changing subtasks

To change to another Management Processor Assistant subtask, click the list in the upper-left, above the left pane. The menu options for the selected menu are displayed in the left pane.

Selecting servers to work with

To display a hierarchical tree of servers that you can work with, click **File → Show/Hide server tree**. The right pane is subdivided, and the servers that you selected when starting the task are displayed in the Server tree pane.

All the servers that you targeted and other systems that contain a meaningful association with those servers are displayed in the Server tree pane. For example, if you target an RXE-100 Remote Expansion Enclosure, the Management Processor Assistant task is activated against it, and the physical platform that represents the xSeries server or servers to which the enclosure is connected.

If Management Processor Assistant is unable to establish communications with the service processor for a selected system, a message is displayed that tells you to right-click the server in the Server tree pane and click **Communication**. The Communication Configuration pane opens, and you can provide the applicable parameters. If you do not do this, you will not be able to connect to that system, and the system will be unavailable in the Server tree pane.

Note: You can type up to 127 characters in the **UserID** field of the Communications Configuration pane. You can use both alphabetic and numeric characters. You also can use the special characters @ (at), . (period), _ (underscore) and - (dash). You can use only one @, and it must not be the first or last character of the user ID. A letter or a digit must follow an @. You cannot use more than one consecutive period (.). You cannot use spaces in the user ID.

To select the servers that you want to work with, expand the **Servers** icon in the Server tree pane. Select the check box for each server that you want to work with.

Configuring multiple servers once

Use the Repeat option to configure multiple servers at once by copying the values from the row for one system to other selected systems. When the source row provides parameters that are not applicable for a target system, the row for that system is skipped.

Complete the following steps to copy the values from one row to other selected entries in a table:

1. Select a row with information that you want to copy.
2. Using the Ctrl key, select the other rows to which you want to copy the source row.
3. Click **Repeat**. A confirmation window is displayed.
4. Click **OK**. You must click **Apply** to execute or save the changes.

Saving changes

After you add or modify information in the “Management Processor Assistant” window, you must click **Apply** to execute or save the changes. Depending on the subtask, the Apply option updates the information that is stored in IBM Director Server, modifies the configuration information on a service processor, or runs a management action.

Sorting columns

To sort the information that is displayed, click on the column heading that you want to use as the sort criterion. To reverse the sort order, click the column heading again.

Communications subtask

You can use the Communications subtask to configure how IBM Director Server communicates with service processors. You can configure IP, ASM interconnect, and interprocess communication (IPC) settings and prioritize network communications.

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

Any changes that you make using the Communications 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.

Viewing IP settings for MPA communications

You can view and modify the IP settings that are used to communicate with a service processor. You also can enable or disable IP communications.

Complete the following steps to configure the IP settings for MPA communications:

1. Click **Communications** → **Communication configuration** → **IP settings**. The IP settings that are used to connect to the selected service processor are displayed.
2. Select the **Enable** check box to enable IP communications.
3. Click **Apply**.

Establishing out-of-band communication with a service processor

In IBM Director Console, an informational status icon is displayed next to managed objects that support out-of-band connectivity but have not been validated.

Note: You can click the status icon next to the object to configure the communication settings for the object.

After IBM Director successfully connects to the managed object, the informational icon is removed. If the managed object is created using an out-of-band connectivity path, the connection path is validated when the object is created and the status icon is not displayed.

Complete the following steps to connect out-of-band to IBM Director Server from a server that contains an ASM processor and an optional Remote Supervisor Adapter:

1. Create a management processor managed object to represent the Remote Supervisor Adapter. For more information, see the *IBM Director 4.20 Installation and Configuration Guide*.
2. In the IBM Director Console Tasks pane, expand the **Management Processor Assistant** task. Drag the **Communications** subtask and drop it onto both the ASM processor managed object and the 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 pane is displayed.
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 **ASM interconnect 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, make sure that **ASM interconnect** 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, specify the user ID and password in the **Global settings** group box.

Note: You can type up to 127 characters in the **UserID** field of the Communications Configuration pane. You can use both alphabetic and numeric characters. You also can use the special characters @ (at), . (period), _ (underscore) and - (dash). You can use only one @, and it

must not be the first or last character of the user ID. A letter or a digit must follow an @. You cannot use more than one consecutive period (.). You cannot use spaces in the user ID.

11. Select the **Store password** check box to enable the ASM processor to auto-connect 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 Management Processor Assistant task immediately.

The connection settings are used for both interactive and noninteractive Management Processor Assistant 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 that you provided in the Communications subtask. For more information about service processors and communicating with IBM Director Server, see the *IBM Director 4.20 Installation and Configuration Guide*, specifically the “Managing service processors” section in Chapter 3.

Configuration subtask

You can use the 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

Use the Configuration subtask to view service processor data, including build information, such as firmware type, file name, and microcontroller.

Complete the following steps to view service processor data for a server:

1. Click **Configuration** → **Service Processor Configuration** → **Service processor VPD**. The Build information page is displayed.
2. To view the Microcontroller VPD page, click the **Microcontroller VPD** tab.

Configuring alert settings

You can configure the information that is sent in critical, system, warning, and other alert messages. Complete the following steps to configure an alert:

1. Click **Configuration** → **Remote-alert settings** → **General-alert settings**. The General-alert settings pane is displayed.
2. Click the tab of the alert that you want to configure.
3. Select the information that you want to send for the selected alert.
4. Click **Apply**.

Adding or modifying an alert-forwarding profile

The Configuration subtask provides access to alert-forwarding profiles that automatically send alerts to the systems that you specify. Alert forwarding ensures that alerts are sent, even if a managed system experiences a catastrophic failure, such as an operating-system failure. You can create up to 12 alert-forwarding profiles for a service processor.

Complete the following steps to add or modify an alert-forwarding profile:

1. Click **Configuration** → **Remote-alert settings** → **Alert-forwarding profiles**. The Alert-forwarding profiles pane is displayed.
2. Click an existing profile, and then click **Add an entry**. The selected profile is copied and added as a new record to the bottom of the profile list. By default, the **Entry number** field is filled in automatically with the number of the next profile record in the list.
3. To change the entry number for the new record, from the **Entry Number** field, select an unused entry number.
4. Complete the alert-forwarding profile fields:
 - a. From the **Status** list, select **Enabled** to turn on the selected profile, **Disabled** to turn off the selected profile, or **Unused** to delete the selected profile.
 - b. In the **Description** field, type a brief description to help identify the selected profile.
 - c. From the **Connection type** list, select the delivery method that you want to use for the selected profile.

IBM Director Comprehensive

Receive all alerts that are generated by the management module regardless of whether the type of alert is enabled. You also must specify an IP address if you select this notification method.

SNMP over LAN

You must configure SNMP for this notification method to work properly.

E-mail over LAN

You must configure SMTP for this notification method to work properly.

- d. In the **IP address or host name** field, type the IP address or host name of the device that you want to receive the alerts. For you to edit this field, the connection type must be set to IBM Director Comprehensive or IBM Director over LAN.
 - e. In the **E-mail address** field, type the e-mail address of the mail account that you want to receive the alerts.
 - f. To forward alerts only for critical events, select the **Critical events only** check box.
 - g. In the **Phone number** field, type the phone number that you want to receive calls. To be notified by a numeric page, follow the phone number with a comma and a personal identification number (PIN).
 - h. For alphanumeric pages only, in the **Pager PIN** field, type the alphanumeric pager PIN.
 - i. In the **PPP login ID** field, type the login ID for the alert recipient account. A Point-to-Point Protocol (PPP) login ID consists of a secure IP address, an account name, and a user ID, separated by periods.
 - j. In the **PPP Password** field, type the PPP password.
5. Click **Apply** to save the changes.

Sending a test alert

Complete the following steps to send a test alert:

1. Click **Configuration** → **Remote-alert settings** → **Alert-forwarding profiles**. The Alert-forwarding profiles pane opens.

2. Click an existing profile, and then click **Send test alert**. A confirmation window is displayed.
3. Click **OK**.

Configuring network settings for the service processor

From the Network settings pane, you can restart selected service processors or view or modify the following settings for selected managed systems:

- IP properties
- Hardware
- DHCP
- DNS
- Restart service processor

Complete the following steps to configure network settings:

1. Click **Configuration** → **Network settings** → **Network interfaces**. The Network interfaces pane is displayed.
2. To configure the IP properties, click the **IP properties** tab.

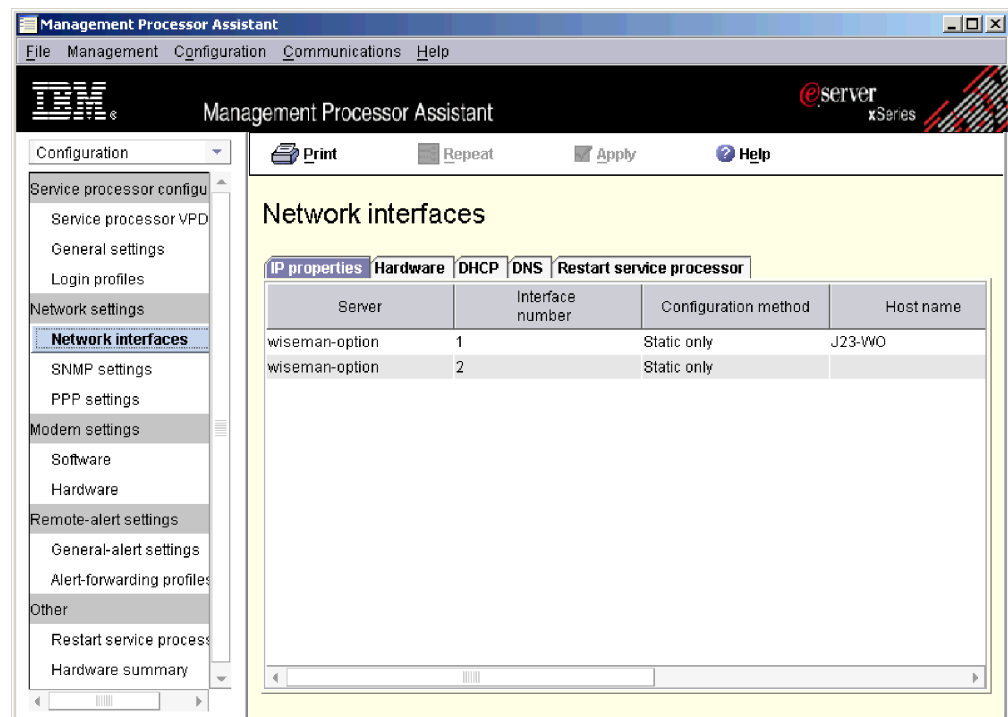


Figure 86. “Management Processor Assistant” window: IP properties page

3. Modify the applicable fields:
 - a. From the **Configuration** list, select a configuration method. Select **Static only** to use the current configuration values. Select **DHCP only** to automatically obtain an IP address from the DHCP server.

Note: If you enable DHCP, you must have an accessible, active, and configured DHCP server on your network. The configuration settings that are assigned by a DHCP server override all static IP settings that you have provided.

- b. In the **Host name** field, type the host name of the service processor. The host name can be a maximum of 63 characters long. If the host name that

you provide conflicts with the IP address and DHCP is selected as the configuration type, the DHCP server assigns the applicable IP address to the host name.

- c. In the **IP address** field, type the IP address of the service processor.
 - d. In the **Subnet mask** field, type the subnet mask that is used by the service processor.
 - e. In the **Gateway** field, type the gateway address that is used by the service processor.
4. To configure the hardware-network settings, click the **Hardware** tab. The Hardware page is displayed.

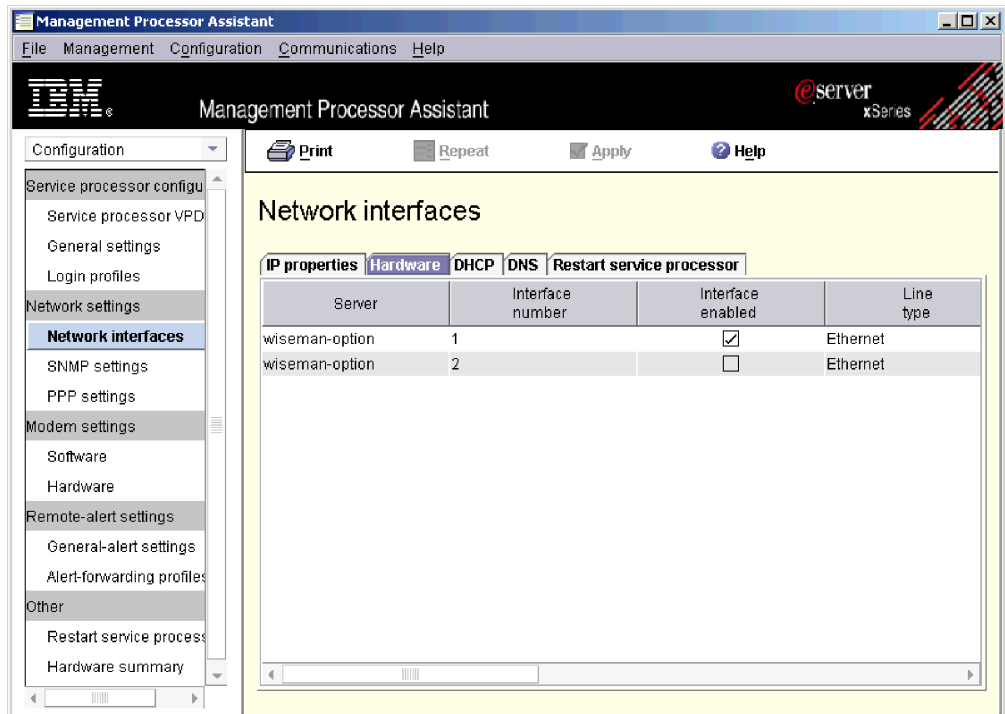


Figure 87. “Management Processor Assistant” window: Hardware page

5. Modify the applicable fields:
 - a. From the **Line type** list, select **Ethernet**.
 - b. From the **Data rate** list, select the data-transfer rate for the service processor. Make sure that your selection corresponds to the capabilities of your network. To automatically detect the data-transfer rate, select **Auto**.
 - c. From the **Duplex** list, select the type of communication channel that is used in your network. Only **Full Duplex** can be used for the internal network interface.
 - d. In the **MTU size** field, type the maximum transmission unit (MTU) size. The MTU value that you type indicates the maximum packet size (in bytes) for your network. For Ethernet, the MTU range is 60-1500. Only **1500** can be used for the internal network interface.
 - e. In the **Administrator assigned MAC address** field, type a physical address for the service processor. If you specify an address, this locally administered address will override the burned-in MAC address. The address must be in the form of xx xx xx xx xx xx (six hexadecimal digits separated by blanks).

- f. To enable routing, select the **Routing bytes** check box. This option is available only if your line type is set to Token Ring.
6. To view the DHCP settings, click the **DHCP** tab. The DHCP page is displayed.
7. To configure DNS, click the **DNS** tab. The DNS page is displayed.

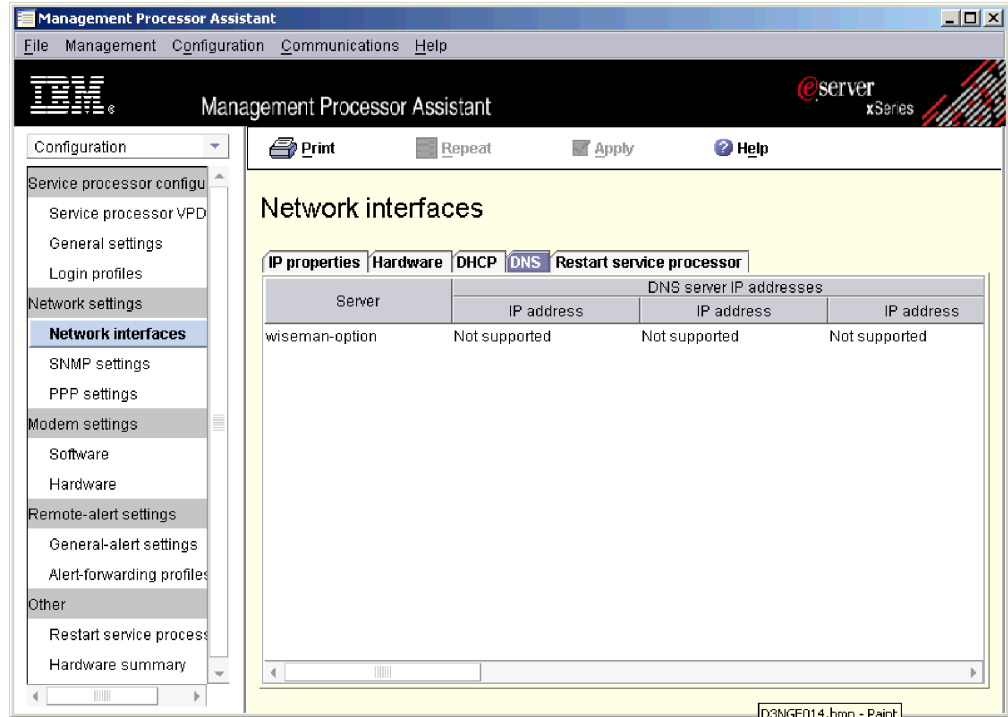


Figure 88. "Management Processor Assistant" window: DNS page

8. Modify the applicable fields:
 - a. In the **IP address** fields, type the IP addresses of the DNS servers that are on your network. You can specify a maximum of three DNS servers.
 - b. Select the **Enable DNS lookup** check box to use a DNS server on your network to translate host names into IP addresses.
9. To restart a service processor, click the **Restart service processor** tab. The Restart service processor page is displayed.

Note: If you have not changed any settings, you cannot select **Restart now** on the Restart service processor page.

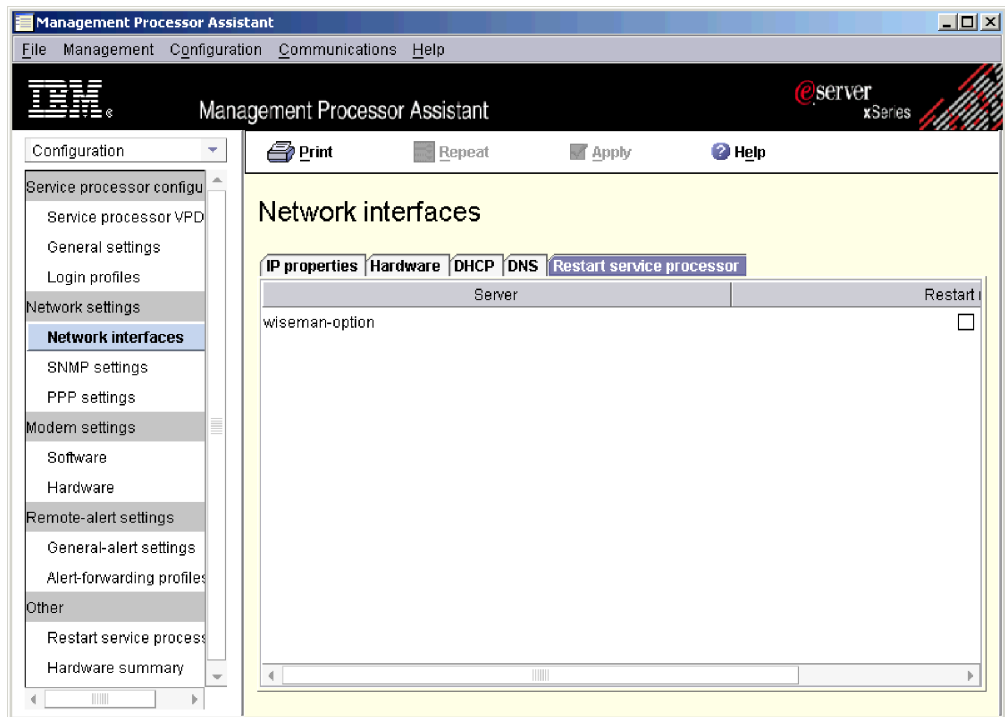


Figure 89. “Management Processor Assistant” window: Restart service processor page

10. Modify the applicable fields:
 - a. Click the service processor that you want to restart.
 - b. Select the **Restart now** check box to restart the service processor after you apply your changes.
11. Click **Apply** to save the changes.

Configuring SNMP settings

Complete the following steps to configure SNMP settings:

1. Click **Configuration** → **Network settings** → **SNMP settings**. The SNMP settings pane is displayed.
2. Select the server that you want to configure.
3. Modify the applicable fields:
 - a. In the **Contact** field, type the contact information for the system contact. For example, you might include the person’s name and phone number.
 - b. In the **Location** field, type a location for the server.
 - c. Select the **Agent enabled** check box to enable the SNMP agent. This check box must be selected for alerts to be sent.
 - d. Select the **Traps disabled** check box to disable SNMP traps. This check box must be cleared for alerts to be sent.
4. Configure a community:
 - a. Select the applicable server.
 - b. In the **Community name** field, type the name of the community.
 - c. In the applicable **IP address** field, type an IP address for each community. You can provide up to three valid IP addresses/host names for each community. The new IP address must be in the form xxx.xxx.xxx.xxx where xxx is a decimal number from 0 to 255.

5. To restart a service processor, click the **Restart service processor** tab. The Restart service processor page is displayed.

Note: If you have not changed any settings, you cannot select **Restart now** on the Restart service processor page.

6. Modify the applicable fields:
 - a. Click the service processor that you want to restart.
 - b. Select the **Restart now** check box to restart the service processor after you apply your changes.
7. Click **Apply**.

Configuring PPP settings

Use this task to view and configure Point-to-Point Protocol (PPP) settings.

Complete the following steps to configure PPP settings:

1. Click **Configuration** → **Network settings** → **PPP settings**. The PPP settings pane is displayed.
2. Select the server that you want to configure.
3. Modify the applicable fields:
 - a. Select the **Enable PPP interface** check box to enable the PPP interface. If you enable PPP, the service processor cannot use the serial port for serial remote access.
 - b. In the **Remote IP address** field, type the IP address that the service processor assigns to a remote user.
 - c. In the **Server IP address** field, type the IP address for the PPP interface on the service processor.
 - d. In the **Subnet mask** field, type the subnet mask that is used by the service processor.
 - e. In the **Authentication select** field, select the type of authentication protocol that is negotiated when a PPP connection is attempted.
4. To restart a service processor, click the **Restart service processor** tab. The Restart service processor page is displayed.

Note: If you have not changed any settings, you cannot select **Restart now** on the Restart service processor page.

5. Modify the applicable fields:
 - a. Click the service processor that you want to restart.
 - b. Select the **Restart now** check box to restart the service processor after you apply your changes.
6. 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 for a service processor.
3. Click **Apply**.

Configuring modem settings

You can configure the modem hardware and the modem software settings.

Complete the following steps to configure modem hardware settings:

1. Click **Configuration** → **Modem settings** → **Hardware**. The Modem settings - Hardware pane is displayed, and the Basic page is displayed.

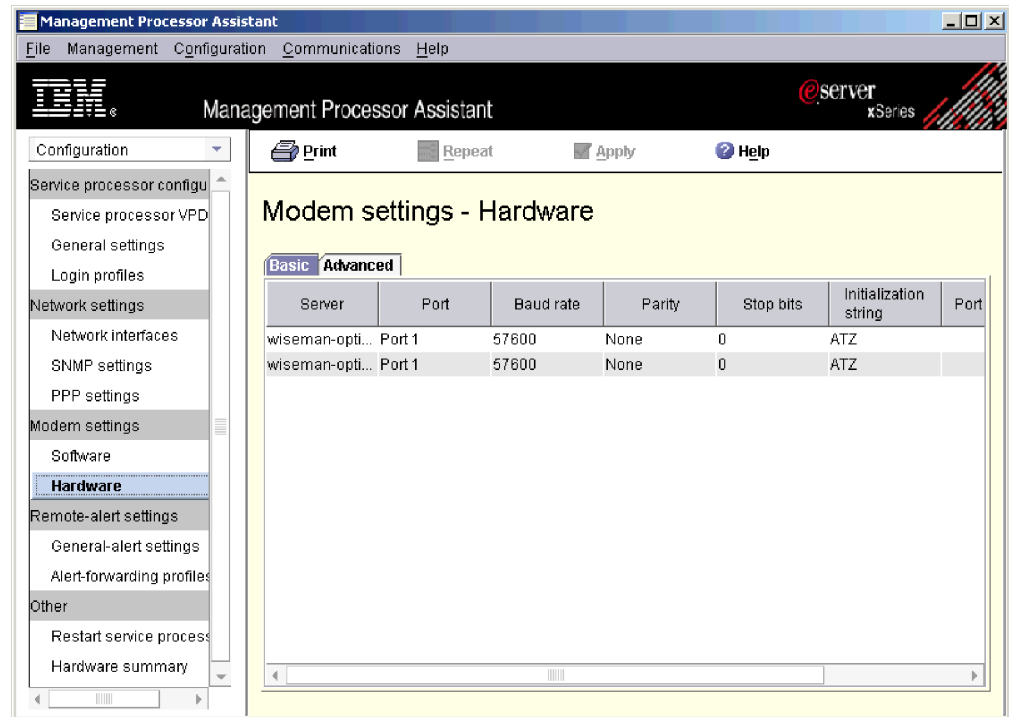


Figure 90. “Management Processor Assistant” window: Modem settings - Hardware pane

2. Configure the following basic modem settings:
 - a. From the **Baud rate** list, select the data-transfer rate (bits per second) of your serial port connection.
 - b. From the **Parity** list, select the error detection bit: **Even**, **Odd**, or **None**. This enables the server to detect whether received data has been damaged during transmission.
 - c. From the **Stop bits** list, select the number of data-terminating 1-bits that follows the data or any parity bit to mark the end of a transmission.
 - d. To reserve the port for the use of the service processor, select the **Port enabled** check box.
 - e. In the **Caller ID** field, type the initialization string that is used to get caller ID information from the modem.
3. Click the **Advanced** tab. The Advanced modem settings page is displayed.
4. Configure the advanced modem settings:
 - a. In the **Escape guard time** field, type the length of time (in 10-millisecond intervals) that you want to elapse before and after the escape string is issued to the modem. The value must be between 1 and 250. By default, the value is set to 100 (1 second).
 - b. In the **Escape string** field, type the initialization string that returns the modem to command mode while it is communicating with another modem.

- c. In the **Dial prefix** field, type the initialization string that is used before the telephone number to be dialed. By default, this is set to ATDT.
 - d. In the **Dial postfix** field, type the initialization string that is issued after the phone number is dialed to tell the modem to stop dialing.
 - e. In the **Auto answer** field, type the initialization string that determines the number of rings before the modem answers. By default, this is set to ATSO=1, which causes the modem to answer after two rings.
 - f. In the **Auto answer stop** field, type the initialization string that stops the modem from answering the phone automatically when it rings. The default is ATSO=0.
 - g. In the **Query** field, type the string that determines whether the modem is attached. By default, this is set to AT.
 - h. In the **Hangup** field, type the initialization string to instruct the modem to hang up. By default, this is set to ATH0.
5. Click **Apply**.

Complete the following steps to configure modem software settings:

1. Click **Configuration** → **Modem settings** → **Software**. The Modem settings - Software pane is displayed.

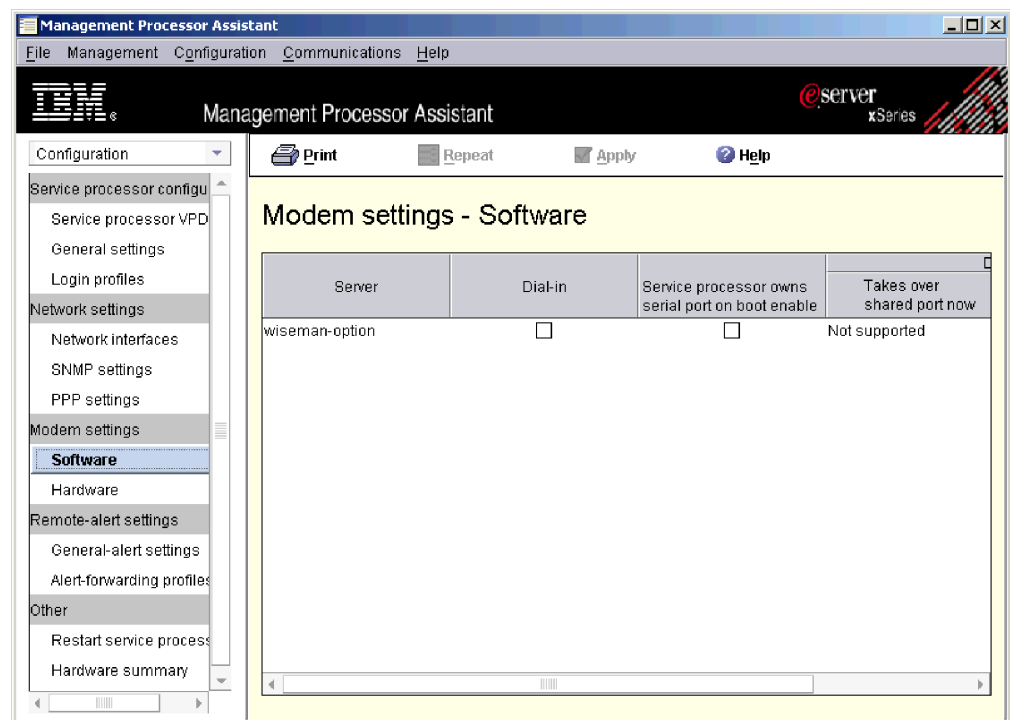


Figure 91. “Management Processor Assistant” window: Modem settings - Software pane

2. Configure the modem software settings:
 - a. To enable remote users to dial into the service processor through a serial connection, select the **Dial-in** check box.
 - b. To reserve a serial port for exclusive use by the service processor, select the **SP owns shared port on boot enable** check box. On some systems, the service processor shares the server serial port with the operating system. See your hardware documentation for details.

- c. To cause the service processor to immediately take over the shared serial port from the operating system, select the **Takes over shared port now** check box.
 - d. In the **Dial-in tamper delay** field, type the number of minutes that dial-in access is disabled after an incorrect user ID or password has been used in six successive attempts. The range for the dial-in tamper delay is 4 to 240 minutes.
3. Click **Apply**.

Creating a login profile

Login profiles control network and dial-in access to out-of-band service processors. The login profile that you use to access a service processor must be configured with read/write access. You can create up to 12 login profiles for a service processor.

Note: Some managed objects do not support login profiles.

Complete the following steps to create a login profile:

1. Click **Configuration** → **Service processor configuration** → **Login profiles**. The Login profiles pane is displayed.
2. Click an existing profile.
3. Click **Add an entry**. A new record is displayed in the Login profiles pane. You can click the **Entry number** field to select from a list of available entry numbers.

Note: Click **Repeat** to configure multiple systems at once to use the same user ID and password.

4. Create the login profile.

Note: Both the **User ID** and **Password** fields are case sensitive.

- a. In the **User ID** field, type the user ID for the new login profile.
- b. In the **Password** field, type the password for the new login profile. The password that you create must be five to 12 characters long, contain no spaces, and have at least one alphabetic character and one numeric character.
- c. In the **Confirm password** field, retype the password for the new login.
- d. From the **Authority** list, select the level of access for the new profile. A sublist is displayed.

Supervisor

Enables the user to view and modify all supported fields and actions that are provided within the interface.

Read only

Enables the user to view data only. The user cannot make changes to information, perform file transfers, or turn on or turn off any managed objects.

Custom

Enables the user to have read-only access or supervisor access to specific functions that you explicitly select from a sublist.

- e. If needed, from the sublist, select the applicable access levels; then, click **Done**. Select an access-level check box to provide read/write access for that function. Clear an access-level check box to provide read-only access to that function.

User account management

Enables the user to add, modify, or delete user IDs and change global login settings.

Remote console access

Enables the user to access the remote server.

Remote console and virtual media access

Enables the user to access the remote server console and to modify the virtual media functions for that remote server.

Remote server and power/restart access

Enables the user to access the remote server console and to modify the power-on and restart functions for the remote server.

Ability to clear event logs

Enables the user to clear the event logs.

Adapter configuration - Basic

Enables the user to modify the basic configuration parameters for the system, such as system settings and alerts.

Adapter configuration - Networking and security

Enables the user to modify the configuration parameters that relate to network interfaces, network protocols, and serial ports.

Adapter configuration - Advanced

Enables the user to modify basic configuration parameters and the configuration parameters that relate to the network interfaces. It also enables the user access to the following advanced configuration settings and functions: firmware upgrades, restore adapter factory-default settings, modify and restore or reset adapter configuration from a configuration file, and restart and reset the adapter.

- f. In the **Dial-back number** field, type the telephone number that is dialed after a successful login.
- g. To enable the dial-back option, select the **Dial-back enabled** check box.
5. To delete a user profile, click the user profile that you want to delete, and delete the information that is displayed in the **User ID** field.
6. Click **Apply**.

Management subtask

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

Viewing server status

You can view current values and status for all monitored components, such as power-on hours, number of restarts, basic input/output system (BIOS) level, system status, and much more.

To view server status information, click **Management** → **Status and VPD** → **Server status**. The data is displayed.

Viewing sensor data

You can view environmental data, such as temperature, voltage, fan speeds and power supply, that is recorded by sensors in a server.

To view sensor data, click **Management** → **Monitoring** → **Sensors**. The data is displayed.

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.

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 that is stored on the service processor, click **Management** → **Status and VPD** → **Event log**.

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

Viewing hardware summary

The hardware summary includes information such 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.

Viewing light path diagnostics

You can view the light path diagnostics LEDs 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 that 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 state of the blue-indicator light on a server:

1. Click **Management** → **Status and VPD** → **Blue-indicator light**. The blue-indicator-light information is displayed.
2. In the table, click the row for the server that you want to work with; then, click the **State** field and select a light-indicator option. The options are **On**, **Off**, or **Flashing**.

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

3. Click **Apply**.

Viewing the memory DIMM information

To view information about the dual inline memory module (DIMM) in a server, click **Management** → **Status and VPD** → **Memory DIMM**. The DIMM information is displayed.

Turning servers on and off

You can turn on or turn off a server remotely.

Note: The service processor device driver and, depending on the operating system of the server, either the MPA Agent or System Health Monitoring must be installed.

Complete the following steps to turn off a server:

1. Click **Management** → **Local power control** → **Power off server**.
2. Select the applicable check box. The options are **Power off immediately** or **Power off with OS shutdown**.
3. Click **Apply**.

Complete the following steps to turn on a server:

1. Click **Management** → **Local power control** → **Power on server**.
2. To turn on the server immediately, select the **Power on immediately** check box. To turn on the server at a specified date and time, double-click the **Power on date and time** field and select the date and time.
3. Click **Apply**.

Restarting a managed system

Complete the following steps to restart a managed system:

1. Click **Management** → **Local power control** → **Restart server**.
2. Select the applicable check box. The options are **Restart immediately** or **Restart with OS shutdown**.
3. Click **Apply**.

Viewing and changing startup (boot) options

You can select whether a PXE restart (reboot) occurs the next time the server is restarted.

Complete the following steps to view and change startup options:

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

Chapter 17. Microsoft Cluster Browser

You can use the Microsoft Cluster Browser task to view the structure, nodes, and resources that are 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.

To start 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.

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

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

Chapter 18. Network Configuration

You can use the Network Configuration task to view and edit settings for Ethernet adapters, IP addresses, DNS configurations, Windows Internet Naming Service (WINS) configurations, Windows domains and workgroups, and modems of a managed system.

Note: You can apply the Network Configuration task to a group of managed systems using Mass Configuration. For more information, see “Mass Configuration” on page 51.

Viewing and configuring IP addresses

Complete the following steps to view and configure IP addresses:

1. In the IBM Director Console Tasks pane, drag the **Network Configuration** task onto a managed system or group. The “Network Configuration” window opens.
2. Click the **IP Address** tab. The IP Address page is displayed.

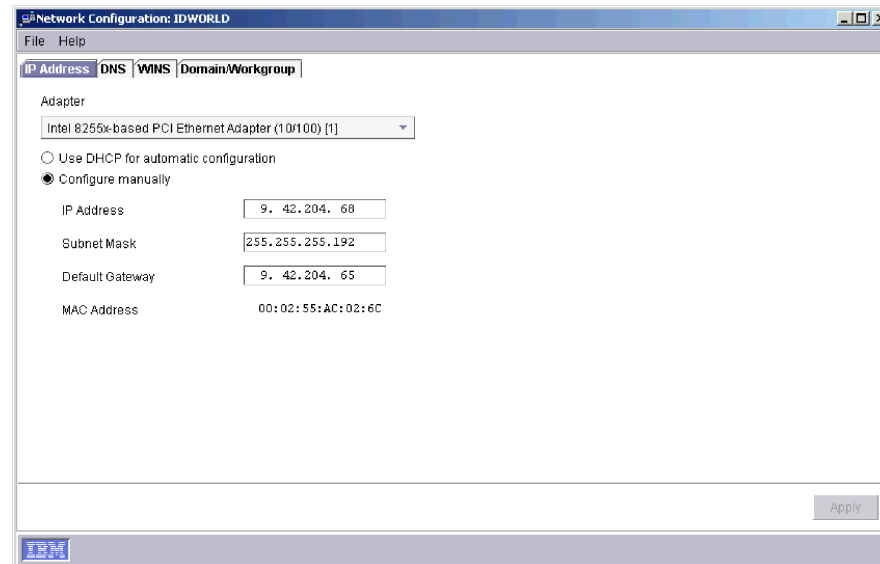


Figure 92. “Network Configuration” window: IP Address page

3. In the **Adapter** field, select the network adapter.
4. Click **Use DHCP for automatic configuration** to automatically obtain an IP address from a DHCP server.
5. (Optional) Complete the following steps to manually configure the IP address:
 - a. Click **Configure manually**.
 - b. In the **IP Address** field, type the IP address of the managed system.
 - c. In the **Subnet Mask** field, type the subnet mask that is used by the managed system.
 - d. In the **Default Gateway** field, type the gateway address that is used by the managed system.
6. Click **Apply** to save the changes.
7. Click **File → Close**.

Chapter 19. 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 events whenever applications change state. You can issue commands on managed systems also. However, you cannot use the Process Management task or any subtasks on BladeCenter chassis or platforms.

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

- Process Monitors
- Process Tasks
- Remove Process Monitors

Notes:

1. (Managed systems running Caldera Open UNIX only) The only Process Management task or subtask that you can use is Process Tasks.
2. (SNMP devices only) You can only view processes on SNMP devices, but you cannot affect the processes.
3. (SNMP printers only) The Process Management task is not supported on SNMP printers.

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 up to three pages:

Applications

Shows all processes that are running on that managed system or group.

Services

Shows the status and description 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 that are installed on that managed system or group. (This is available for managed systems running Windows operating systems only.)

Subsystems

Shows the status of i5/OS subsystems. (This is available for managed systems running the i5/OS operating system only.)

Servers

Shows the status of servers that are installed. (This is available for managed systems running the i5/OS operating system only.)

Name	Process ID	User	Thread Count	Priority	Memory Usage
Idle	0		1	Idle	16K
System	8	SYSTEM	35	Normal	48K
SystemRoot\System32\smss.exe	148	SYSTEM	6	Normal	52K
SystemRoot\System32\csrss.exe	172	SYSTEM	12	Normal	1436K
SystemRoot\System32\winlogon.exe	192	SYSTEM	16	High	2008K
System32\services.exe	220	SYSTEM	37	Normal	4016K
System32\lsass.exe	232	SYSTEM	15	Normal	952K
System32\svchost.exe	404	SYSTEM	8	Normal	1636K
System32\spoolsv.exe	444	SYSTEM	12	Normal	1736K
Program Files\IBM\Director\websrv\dirw...	472	SYSTEM	4	Normal	272K
System32\svchost.exe	488	SYSTEM	25	Normal	1240K
System32\ibmsmbus.exe	504	SYSTEM	1	Normal	268K
System32\regsvcs.exe	552	SYSTEM	2	Normal	200K
System32\MSTask.exe	572	SYSTEM	6	Normal	736K
System32\cpusvc.exe	584	SYSTEM	3	Normal	320K
System32\snmp.exe	616	SYSTEM	11	Normal	732K
Program Files\Analog Devices\SoundM...	652	SYSTEM	2	Normal	176K
Program Files\IBM\Director\bin\twgipc.v...	676	SYSTEM	2	Normal	200K
Program Files\IBM\Director\bin\twgifran...	680	SYSTEM	2	Normal	3582K
Program Files\IBM\Director\bin\twgagen...	696	SYSTEM	14	Normal	6784K
Program Files\IBM\Director\bin\twgipc.exe	704	SYSTEM	6	High	2108K
System32\WBEM\WinMgmt.exe	712	SYSTEM	13	Normal	4712K
System32\mspmprsv.exe	724	SYSTEM	2	Normal	284K

Figure 93. "Process Management" window

Closing a Windows application (process)

Complete the following steps to close a Windows 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) that 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 Windows 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**.

Setting priority of a Windows application (process)

Complete the following steps to set the priority of a Windows 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) that you want to close, and click **Set Priority**; then click the priority level. A confirmation window is displayed.
3. Click **Yes**.

Closing a Linux application (process)

Complete the following steps to close a Linux 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) that you want to close, and click **Kill process** or **Terminate signal**. A confirmation window is displayed.
3. Click **Yes**.

Unloading a NetWare module

Complete the following steps to unload a module of a managed system running NetWare:

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) that you want to close, and click **Unload Module**. A confirmation window is displayed.
3. Click **Yes**.

Ending a job on i5/OS

Complete the following steps to end a job on a managed system running i5/OS:

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) that you want to close, and click **End Job** or **End Job Immediate**. A confirmation window is displayed.
3. Click **Yes**.

Starting subsystems, ending subsystems, and showing jobs on i5/OS

Complete the following steps to start or stop i5/OS subsystems or show jobs on an i5/OS subsystem:

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 **Subsystems** tab. Right-click the subsystem that you want to manage and click **Start Subsystem**, **End Subsystem**, or **Show Jobs**.

Starting servers, ending servers, and showing jobs on i5/OS

Complete the following steps to start or stop installed servers running on i5/OS or show jobs on the installed server:

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 **Servers** tab. Right-click the server that you want to manage and click **Start Server**, **End Server**, or **Show Jobs**.

Note: IBM Director does not currently support starting and stopping all types of servers. Some servers might be displayed that you cannot start or stop through IBM Director.

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.

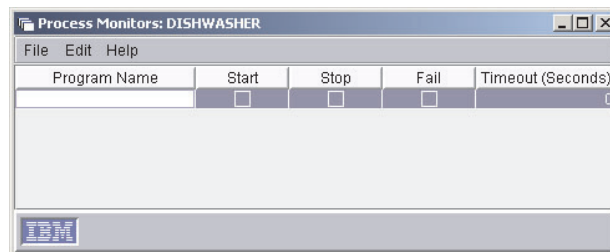


Figure 94. “Process Monitors” window

3. Type the executable file name of the application process that 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 6 until you have listed the executable file names of all the processes that 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 that 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 40 for more information about how to schedule tasks.

Removing process monitors

When you no longer need to monitor a process on a managed system, remove the process-monitor task, to 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 that 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 40 for more information about how to schedule tasks.

Viewing process monitors

To view a list of the process monitors that are 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 that are 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 40 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 who is logged in on the managed system.

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

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

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.

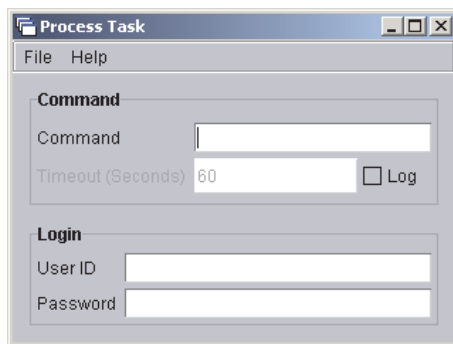


Figure 95. “Process Task” window

3. Type the command-line program that is to be run.

Notes:

- a. (Managed systems running Windows only) If the command is a command-line instruction, preface that command with the following command so it will run in a Windows command-shell window:
`cmd /c`
 - b. (Managed systems running i5/OS only) The command is run in the QShell environment.
 - c. (Managed systems running i5/OS only) For security purposes, i5/OS managed systems do not allow commands to be performed anonymously under the default user ID that is shipped with IBM Director. Either select to specify a user ID, or remove the default user ID from the registered function and add a new default user ID that has the required authority to perform the command.
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 40 for more information about scheduling tasks.)

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

Using the “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. Using 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 96. “Execute Command” window

It has three pages:

Command

Type a command that is to be issued on the managed system.

Notes:

- a. If you do not specify the fully-qualified path of the command, the task uses the PATH environment variable.
- b. (Managed systems running Windows only) If the command is a command-line instruction, preface that command with the following command so it will run in a Windows command-shell window:
`cmd /c`
- c. (Managed systems running i5/OS only) By default, i5/OS commands run in the QShell environment.
 - Run native commands using the syntax in the following example:
`system -v "WRKUSRJOB"`

- Run QShell commands using the syntax in the following example:

```
pwd;ls -al
```

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

Notes:

- (Managed systems running i5/OS only) For security purposes, i5/OS managed systems do not allow commands to be performed anonymously under the default user ID that is shipped with IBM Director. Either select to specify a user ID, or remove the default user ID from the registered function and add a new default user ID that has the required authority to perform the command.
- (Managed systems running NetWare only) The Login page is not available when using this task.

Output

Displays any output that the command would normally provide.

Notes:

- When using this option, you can set a timeout value for the command that you specify on the Command page.
 - (Managed systems running NetWare only) The Output page is not available when using this task.
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.

Note: (Managed systems running i5/OS only) Commands cannot run anonymously under the default user ID used by IBM Director Agent on i5/OS managed systems.

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/IBM/director/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.

Chapter 20. Rack Manager

You can use the Rack Manager task, which is 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 that 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.

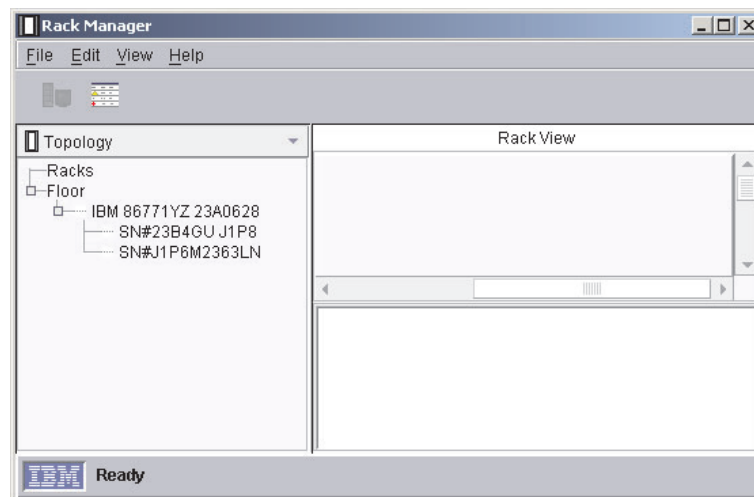


Figure 97. “Rack Manager” window

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 that are available for association and for inclusion in a rack.

Cluster

Displays clusters and cluster members, if any cluster components exist. If there are no cluster components, this option is disabled.

Multi-Node Systems

Displays complexes, partitions, virtual nodes, and I/O expansion units, if any exist. If there are none, 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 that is 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 that is selected in the left pane, Unknown is displayed for some of the properties that are 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 predefined components. 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 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 and then 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 that 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 and 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 “Add Rack” window opens.
2. Type a name and description for the rack. Select the type of rack from the list.
3. Click **OK**. The new rack is displayed in the right pane.
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 that is 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 whether 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 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 whether 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 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 that 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.

Chapter 21. 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 cut, copy, and paste text on both the managed system and the management console.

Note: You can use Remote Control on managed systems running Windows 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 managed system in the active state; all other attached management consoles can only monitor the managed-system display.

Monitor

View-only mode. A management console that is attached to the managed system display the screen image and cursor movements of the managed system.

Suspend

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

Note: By default, Remote Control uses TCP. If you disable TCP-session support on a managed system, Remote Control uses UDP. For more information, see “Disabling TCP session support” on page 161.

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.

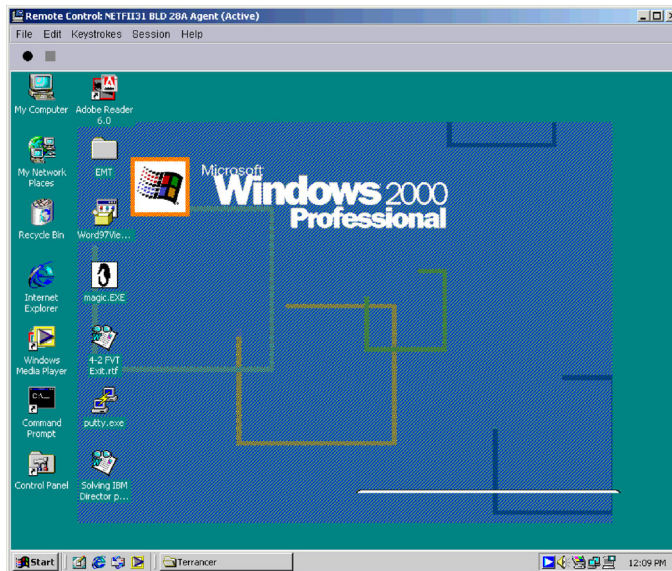


Figure 98. "Remote Control" window

You can select to start a remote-control session in either the Active or Monitor state.

Complete these steps to set the startup mode of a remote-control session:

1. In IBM Director Console, click **Options** → **Server Preferences**. The "Server Preferences" window opens.
2. Click the **Remote Control** tab.
3. In the **Default session state when connecting to an agent** field, select either **Active** or **Monitor**.
4. Click **OK**.

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 that 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 either 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. You can configure this option 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 4.20 Installation and Configuration Guide* for more information.

User administration

Using this method, you can specify the tasks that 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 that you do not add the Remote Control task to the Tasks User Can Access pane.
6. Click **OK**.

Sending key combinations

When you are 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 that 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.

Transferring the clipboard

To copy from the management console to the managed system, complete the following steps:

1. From the management console desktop, select and copy the text.

Note: This function supports text only.

2. In the Remote Control task window, click **Edit → Transfer Clipboard**. The contents of the management console clipboard are transferred to the managed system clipboard.
3. Using the Remote Control task, open a text file and click **Edit → Paste** in the application window.

Chapter 22. Remote Session

As you would use the Remote Control task, 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.

Note: You can have multiple remote sessions active at the same time, but you can have only one remote session through a management server to a single managed system.

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 you are targeting a managed system that is running UNIX or Linux, Remote Session uses the SSH protocol. If the SSH server on the managed system does not respond, the Remote Session task attempts to use the Telnet protocol to connect to the managed system.

Note: (Managed systems running i5/OS only) The Remote Session task uses the Telnet protocol only.

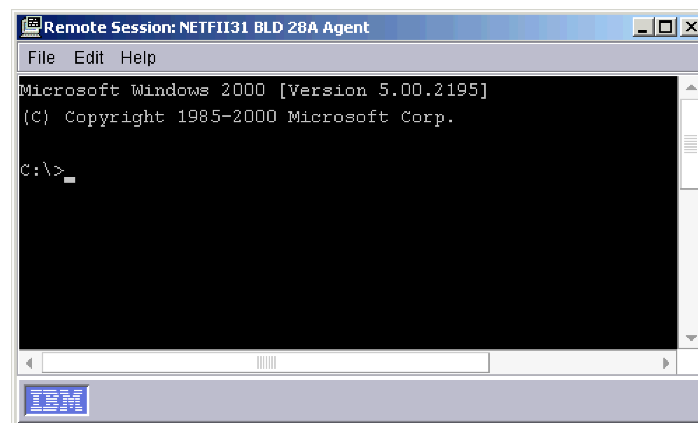


Figure 99. "Remote Session" window for a managed system running Windows

You can select text within the "Remote Session" window and click **Edit → Copy** to copy the selected text. You also can import text into a remote session by clicking **Edit → Paste**.

Chapter 23. 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 also can 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 Chapter 4, “Managing and monitoring systems with event action plans,” on page 55 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

View information about previously configured resource-monitor recordings.

All Available Thresholds

View information about previously configured resource-monitor thresholds.

Viewing available resource monitors

You can view the resource monitors that are available for a managed system, device, or group. (For more information on resource-monitor attributes, see Appendix A, “Resource-monitor attributes,” on page 353.)

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 that you want to monitor. The resource is displayed in the Selected Resources pane.

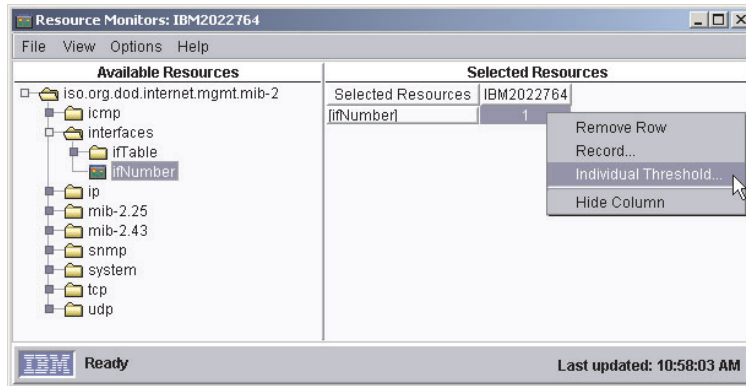


Figure 100. "Resource Monitors" window for a managed device

- In the Selected Resources pane, right-click the resource attribute that 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 101) or a text string (Figure 102 on page 219), you see the applicable window.

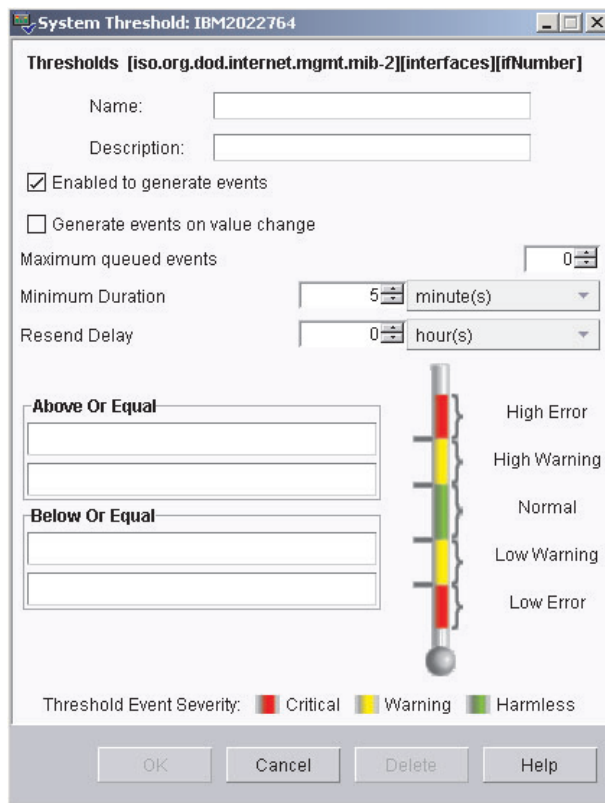


Figure 101. "System Threshold" window for setting numeric thresholds

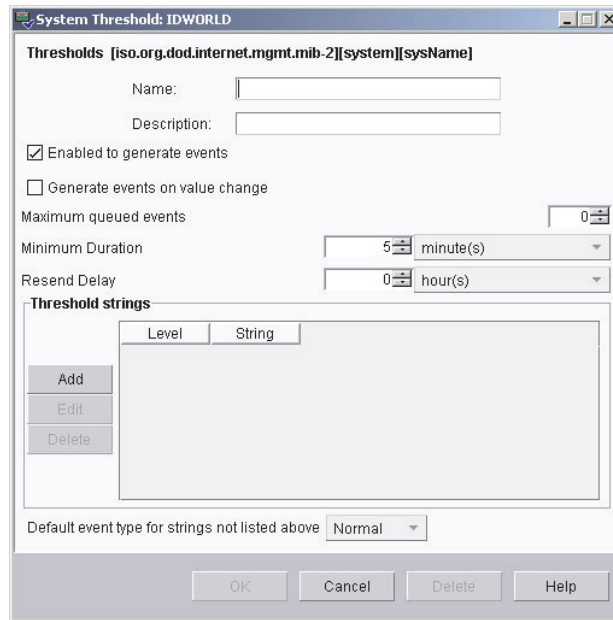


Figure 102. “System Threshold” window for setting text-string thresholds

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 “Building an event action plan” on page 59 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 that 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.

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.

Table 20 on page 220 lists the resource-monitor status icons and what each icon indicates.

Table 20. 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 that were created.

To view all the thresholds that are 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 that have been 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 that you want to record. The “Resource Monitors” window opens.
2. In the Available Resources pane, expand the tree; then, double-click the resource that 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 that you want to monitor, and click **Record**. See Figure 103 on page 221.

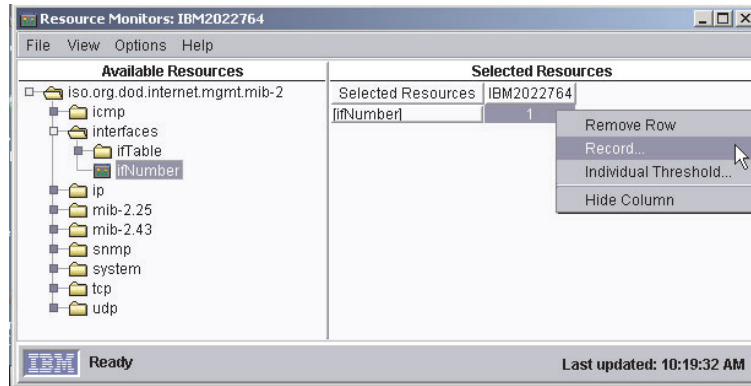


Figure 103. “Resource Monitors” window, clicking **Record**

The “Resource Monitor Recording” window opens.

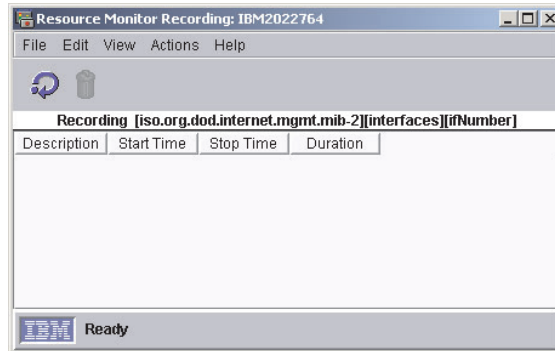


Figure 104. “Resource Monitor Recording” window

4. Click **File** → **New**. The “New Record” window opens.
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 that 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 that 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 that you want to export. The “All Available Recordings” window opens.
3. Right-click the recording that 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 set of conditions on multiple groups or managed systems. Create a threshold task 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. Double-click the **All Available Thresholds** icon. The “All Available Thresholds” window opens.
4. Right-click the threshold that 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.
2. Double-click the **All Available Thresholds** icon. The “All Available Thresholds” window opens.
3. Right-click the threshold that you want to export to a task, and click **Export to Property File**. The “Export threshold to property file” window opens.
4. Type a file name in the **File Name** field, specifying .thrshplan for the file extension.
5. Click **OK**.

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 **OK**.

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 that 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**. To remove an individual monitor, select **Remove Monitor** and click the individual monitor you want to remove.

Chapter 24. ServeRAID Manager

You can use the ServeRAID Manager task to monitor the following adapter or controllers that are installed locally or remotely on servers:

- ServeRAID adapters
- Integrated SCSI controllers with RAID capabilities
- Serial ATA controllers with integrated RAID
- Ultra320 SCSI controllers with integrated RAID

In IBM Director, you can use ServeRAID Manager to view information that is related to arrays, logical drives, hot-spare drives, and physical drives and to view configuration settings. You also can 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.

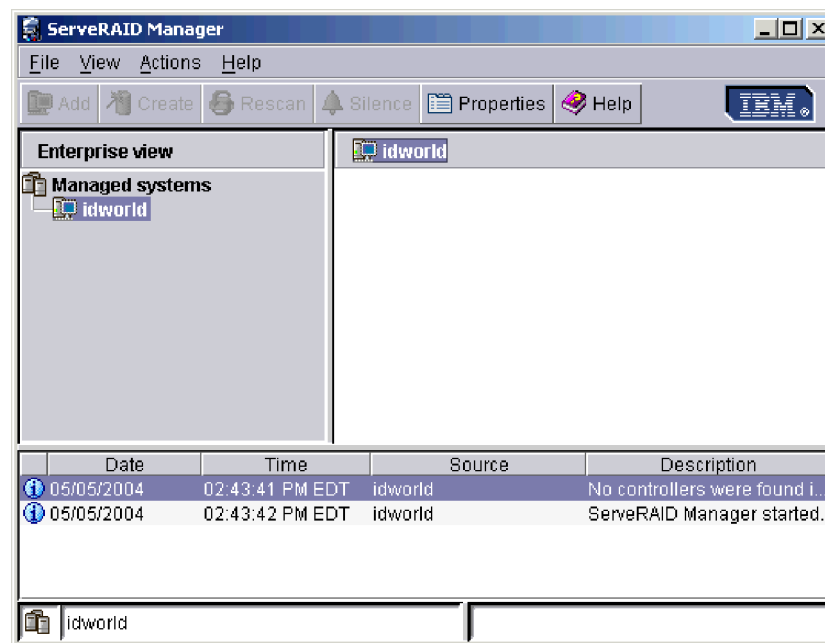


Figure 105. “ServeRAID Manager” window

The left pane is the Enterprise view pane, and the right pane is the Physical and Logical devices 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 **Managed systems** tree in the Enterprise view pane; 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 Enterprise view pane click the controller; then, click the relevant tree object. In the Physical devices pane, a red icon identifies any defunct disk drives.

Date	Time	Source	Description
05/11/2004	02:54:24 PM EDT	NETYP74	Logical drive 1 is offline on controller 1.
05/11/2004	02:54:24 PM EDT	NETYP74	Defunct drive (FRU Part # 37L5741) - User marked failed on controll...
05/11/2004	01:52:44 PM EDT	NETYP74	Set drive to defunct: controller 1, channel 1, SCSI ID 2.
05/11/2004	01:52:31 PM EDT	NETYP74	Initialized logical drive: controller 1, logical drive 1.
05/11/2004	01:51:58 PM EDT	NETYP74	Could not initialize logical drive: controller 1, logical drive 1. Result ...
05/11/2004	01:51:58 PM EDT	ManagedSystem	Unable to connect to the remote system
05/11/2004	01:51:57 PM EDT	NETYP74	Added logical drive: controller 1, logical drive 1. Size = 150 MB, RAID...
05/11/2004	01:51:55 PM EDT	NETYP74	Array A storage space is still available.
05/11/2004	01:51:50 PM EDT	NETYP74	There are 4 ready drives still available.
05/11/2004	01:48:31 PM EDT	NETYP74	ServeRAID Manager started.

Figure 106. "ServeRAID Manager" window displaying a defunct disk drive

Chapter 25. SNMP Browser and SNMP devices

IBM Director discovers SNMP devices in your network according to discovery parameters that you can specify. The process that is used to discover SNMP devices in your network uses lists of initial IP addresses, SNMPv1 and SNMPv2c community names, subnet masks, and SNMPv3 profiles.

IBM Director works with SNMPv1, SNMPv2c, and SNMPv3 for all communications and recognizes Management Information Bases (MIBs) in System Management Information (SMI) version 1 and version 2 formats.

SNMPv1 and SNMPv2c 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 a device. SNMPv3 devices and agents use profiles to control their access.

The subnet mask enables 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 whether the address is associated with a valid SNMP device. A valid SNMP device for IBM Director has the following accessible values: `sysName`, `sysObjectID`, `sysLocation`, `sysContact`, `sysDescr`, 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-device managed-object names default to the value of `sysName`. If `sysName` has no value, the host name of the device is used. If no host name is assigned, the IP address is used.

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

Setting discovery parameters

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

1. In IBM Director Console, click **Options** → **Discovery Preferences**. The “Discovery Preferences” window opens.
2. Click the **SNMP Devices** tab.
3. Click **SNMP version** to select **SNMPv1**, **SNMPv2c**, or **SNMPv3**.
4. If you selected **SNMPv1** or **SNMPv2c**, use the **Add**, **Import**, **Replace**, and **Remove** buttons to create your lists of IP addresses, corresponding subnet masks, and community names.

If you selected **SNMPv3**, use the **Add**, **Import**, **Replace**, and **Remove** buttons to create your lists of IP addresses, corresponding subnet masks, and profile 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. Click **SNMP version** to select **SNMPv1**, **SNMPv2c**, or **SNMPv3**.
3. If you selected **SNMPv1** or **SNMPv2c**, type the network address and the community name.
If you selected **SNMPv3**, select the profile name. See “Creating an SNMPv3 profile” on page 231 for more information.
4. 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.
5. Click **OK** to add the SNMP device to the Group Contents pane.

Configuring SNMP trap forwarding

You can forward SNMP traps in one of two ways: either through the Event Action Plan Builder or by configuring the `SNMPServer.properties` file. If you use the Event Action Plan Builder to forward SNMP traps, the traps are converted to IBM Director traps. For more information on the Event Action Plan Builder, see “Creating a new event action plan” on page 60.

Complete the following steps to forward SNMP traps without modification:

1. Using a text editor, edit a file named `SNMPServer.properties` in the `IBM\Director\data\snmp` directory.
2. To forward SNMPv1 traps:
 - a. Locate the following line in the file:
`#snmp.trap.v1.forward.address.1=`
 - b. Remove the following character at the beginning of this line:
`#`
 - c. Type the IP address of the SNMPv1 trap destination after the equal sign (=).
 - d. Locate the following line in the file:
`#snmp.trap.v1.forward.port.1=`
 - e. Remove the following character at the beginning of this line:
`#`
 - f. Type the port number of the SNMPv1 trap destination after the equal sign (=).
3. To forward SNMPv2 traps:
 - a. Locate the following line in the file:
`#snmp.trap.v2.forward.address.1=`
 - b. Remove the following character at the beginning of this line:
`#`
 - c. Type the IP address of the SNMPv2 trap destination after the equal sign (=).
 - d. Locate the following line in the file:
`#snmp.trap.v2.forward.port.1=`

- e. Remove the following character at the beginning of this line:
#
 - f. Type the port number of the SNMPv2 trap destination after the equal sign (=).
4. (Optional) To set a second or a third destination, edit the applicable lines in the SNMPServer.properties file.
 5. Save the file.
 6. Stop and restart IBM Director Server.

Note: Do not configure a trap destination that is sending traps to the management server. Avoid creating a loop.

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, or monitoring the performance of SNMP devices.

Compiling a MIB file

The SNMP Browser initially displays a tree view of the MIB structure for the selected SNMP devices. If no compiled MIBs are available on IBM Director Server to format the information, or if the device returns information that is not found in a compiled MIB, the information is displayed in a dotted-decimal numeric format. IBM Director comes with various MIB files that are typically needed for SNMP browsing for commonly defined devices. They are in the Director\proddata\snmp directory. When IBM Director Server starts, it compiles all MIB files that are in the Director\proddata\snmp directory.

Note: (i5/OS only) The MIB files in the i5/OS library QUANMIB are compiled MIB files.

MIB data is stored in its own persistent-storage file, snmpmib.dat, 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.

Complete the following steps to compile a MIB file:

1. In the IBM Director Console Tasks pane, right-click **SNMP Browser** and click **Compile a New MIB**. The “Select MIB to Compile” window opens.

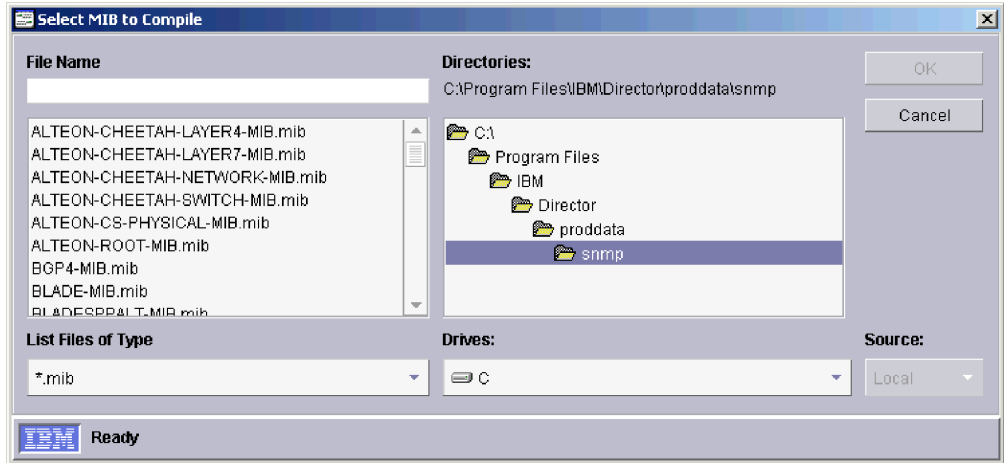


Figure 107. “Select MIB to Compile” window.

2. Specify the directory and file name of the MIB file that you want to compile, and click **OK**. A status 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.

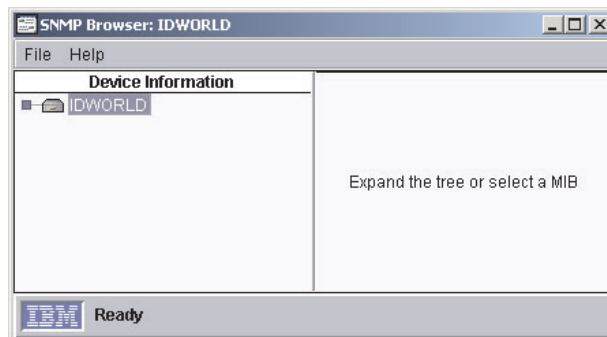


Figure 108. “SNMP Browser” window

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

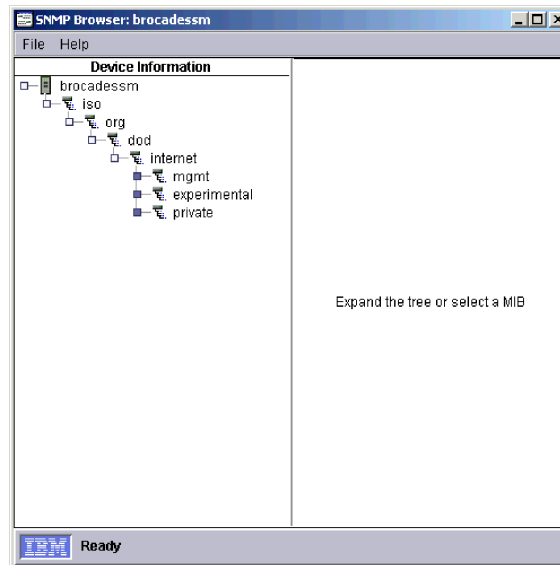



Figure 109. “SNMP Browser” window with a device tree expanded

When you select an attribute in the Device Information pane, the right pane splits and displays the Value and Details panes. 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 that is displaying a  icon. The community name on your SNMP device must also allow the change. Those

attributes that are 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 is displayed in the Value pane. Type the new value and click **Set**.

Note: To discover SNMP devices, you must define an SNMP device to use as a discovery seed (see “Creating a new SNMP device” on page 228 for more information), or an SNMP service must be installed and running on the management server.

Creating an SNMPv3 profile

Complete the following steps to create an SNMPv3 profile:

1. In IBM Director Console, click **Options** → **Server Preferences**. The “Server Preferences” window opens.
2. Click the **SNMP** tab.
3. Click **Add**. The “Add Profile” window opens.

The image shows a dialog box titled "Add Profile". It contains the following fields and controls:

- Profile Name: Text input field
- User Name: Text input field
- Authentication Protocol: Dropdown menu (currently set to "None")
- Password: Text input field
- Confirm Password: Text input field
- Privacy Protocol: Dropdown menu (currently set to "None")
- Password: Text input field
- Confirm Password: Text input field
- Optional** section:
 - Context Name: Text input field
 - Context Engine ID: Text input field
- Buttons: "Add" and "Cancel" at the bottom right.

Figure 110. "Add Profile" window

4. Type the profile name.
5. Type the user name.
6. Select the authentication protocol.
7. (Optional) If you select an authentication protocol other than the default **None**, type the password in both the **Password** and **Confirm Password** fields.
8. (Optional) If you select an authentication protocol other than the default **None**, select a privacy protocol.
9. (Optional) Type a context name.
10. Type a context engine ID.
11. Click **Add**.

Chapter 26. Software Distribution

You can use the Software Distribution task to 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.

Note: The Software Distribution task refers to the i5/OS operating system as OS/400.

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

- Import non-IBM or IBM software and build software packages that use the following wizards:
 - InstallShield Package wizard (Windows)
 - Microsoft Windows Installer wizard (Windows)
 - RPM Package wizard (AIX and Linux)
 - AIX InstallP wizard (AIX)
- Import non-IBM or IBM software and build a software package by using the Custom Package Editor
- Import a software package created in IBM Director by using the Director File Package wizard
- Export a software package for use on another management server
- Restore OS/400 libraries, objects and installed programs

Note: By default, Software Distribution uses TCP. If you disable TCP-session support on a managed system, Software Distribution uses UDP. For more information, see “Disabling TCP session support” on page 161.

Understanding software distribution

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

1. Obtain the software.
2. Import the software into IBM Director Server and build a software package.
3. Distribute the software package to managed systems using one of the following methods:
 - Streamed distribution
 - Redirected distribution

A *streamed distribution* copies the software package from the management server to the managed system and then installs the software package onto the managed system. The one advantage of 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 sent again.

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

One benefit of redirected distribution is to reduce network congestion. With redirected distribution, the managed system receives only the minimum installation code that is needed to access the share and install the software from the management server.

Note: If the installation is interrupted, for example, if the connection is lost, the installation must be started again.

During a redirected distribution, IBM Director Server first determines which of its defined redirector shares that the managed systems to which the software package is being distributed can access. Then, IBM Director Server determines whether the software package is already cached on any of the mutually accessible redirector 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.

For you 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 universal naming convention (UNC)-based share. See the *IBM Director 4.20 Installation and Configuration Guide* for more information about setting up a share.

Notes:

1. The redirector shares keep an archive of all redirected software packages. To avoid exceeding available space on the shares, you should periodically examine the shares and delete cached software packages that are no longer needed. For more information, see “Viewing details about file-distribution servers and software packages” on page 254.
2. Because a system account cannot write to a Microsoft network share, you cannot distribute software packages to a managed system that uses a network share. If a package is distributed to a folder on a Microsoft network share, the distribution fails, and the system log reports a lack of hard disk space. Modify the distribution to distribute to a local drive.

For software that uses Microsoft Windows Installer or InstallShield Professional as the installation utility, when you use 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 “Distribution Preferences” window for a managed system or a group.

You must install the software packages by using the applicable wizard.

Importing software and building software packages

You can use the following wizards or the Custom Package Editor to import files and build a software package:

- Director Update Assistant wizard
- InstallShield Package wizard
- Microsoft Windows Installer Package wizard

- RPM Package wizard
- AIX InstallP Package wizard
- OS/400 Restore Library Package wizard
- OS/400 Restore Licensed Program Package wizard
- OS/400 Restore Object Package wizard

You can import files and packages from the following hardware only:

- A UNC-based share
- A local hard disk drive of the management console
- A local hard disk drive of the management server

Using Director Update Assistant

The Director Update Assistant is a wizard that imports software that is distributed by IBM into IBM Director and creates the software package or packages. Each software update consists of two files:

- The software-update file
- An XML file that describes the software-update file

Complete the following steps to import the software and create one or more software packages:

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

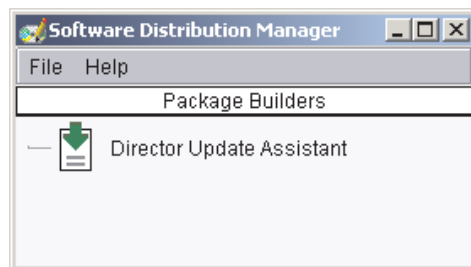


Figure 111. “Software Distribution Manager” window (Standard Edition)

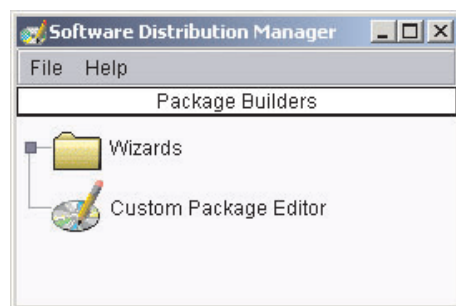


Figure 112. “Software Distribution Manager” window (Premium Edition)

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



Figure 113. Director Update Assistant wizard

3. Specify whether the files are on the local management console or on the management server by clicking the applicable button.
4. Type the location of the XML file that describes the software package or packages that you want to import, or click **Browse** to locate the XML file.
5. Select the **Make Category Private** check box to make the new category visible to only the IBM Director account that created it.
6. 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 that is 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 beside each package in the Packages pane.

7. 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**. The red X beside a package in the Packages pane changes to a green check mark to indicate that the package will be imported.

Notes:

- a. (Managed systems running Windows only) In the Options pane, you can specify an alternative installation script to run by typing the path name in the **Alternate install script** field. Options are not displayed when you are working with Server Plus Pack software packages for managed systems running Windows.
- b. (Upgrading IBM Director Agent on managed systems running Linux only) In the Options pane, you can specify an alternative installation script to run by typing the path name in the **Alternate install script** field.

- c. (Managed systems running Linux only) In the Options pane, you can specify an alternative installation directory for Server Plus Pack software packages by typing the path name in the **Alternate install directory** field.
 - d. (Managed systems running AIX only) In the Options pane, you can specify an alternative installation script to run by typing the path name in the **Alternate install script** field
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 selected software package. Individual software packages are displayed under each category. The packages also are 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 that you want to distribute now, or you can set a time to distribute the software package or software-package category using Scheduler. For more information, see “Distributing a software package” on page 250.

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 Professional as its installation program. You can create packages for software that uses InstallShield Professional 5, 6, or 7 for Windows. InstallShield Professional requires a response file during installation to allow and perform an unattended installation. You can create a response file either by recording an installation or by using an editor. Note that you can distribute a software package that is created with this wizard to managed systems running Windows only.

Most applications do not indicate anywhere in the documentation that they use InstallShield Professional as their installation program. To determine whether an application uses InstallShield Professional, 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**. A window similar to Figure 114 opens.



Figure 114. “About InstallShield” window

If you see the word *InstallShield* in this window, use the InstallShield Package wizard in the Software Distribution task to build a software package.

Next, determine whether a response file is included with the software that you want to distribute. To determine whether a response file is included with the software for which you want to build a package, search for an ISS file (typically setup.iss). The response file is plain-text format so that you can edit the response file for use in

your specific environment. If a response file is included, you must test the response file to make sure that it can be used to install the software on each managed-system type you intend to use it with, and that any customizations that you make are correct. If no response file is included, you must create a response file and test it.

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.

If no response file is included, record one by using the installation command for the software, typically `setup.exe` or `install.exe`. For example:

```
setup -r -f1x:\response_filename.iss -f2logfile
```

where:

- `setup` is the installation command for the product.
- `x:\response_filename` is the path 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`.
- `logfile` is the path where you want to save the installation log file. If you do not specify the `-f2` parameter, InstallShield does not create an installation log file.

When the installation command runs, you are prompted for required information. The responses that you provide must reflect how you want the application to be installed on the managed system. For more information about response files, go to <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 recorded response file or the response file that is included with the software. Type the following command:

```
setup -s -f1x:\response_filename.iss -f2logfile
```

where:

- `setup` is the installation command for the product.
- `x:\response_filename` is the path of the response file that you recorded or the response file that is included with the software. If you do not specify the `-f1` parameter, InstallShield assumes that the response file is in `c:\windows\setup.iss`.
- `logfile` is the path where you want to save the log file. If you do not specify the `-f2` parameter, InstallShield does not create a log file.

When the command is completed, check the system log file. If the software was installed successfully, the result code is 0. If the software was not installed successfully, you cannot distribute it by using IBM Director.

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 **InstallShield Package**. The InstallShield Package wizard starts.

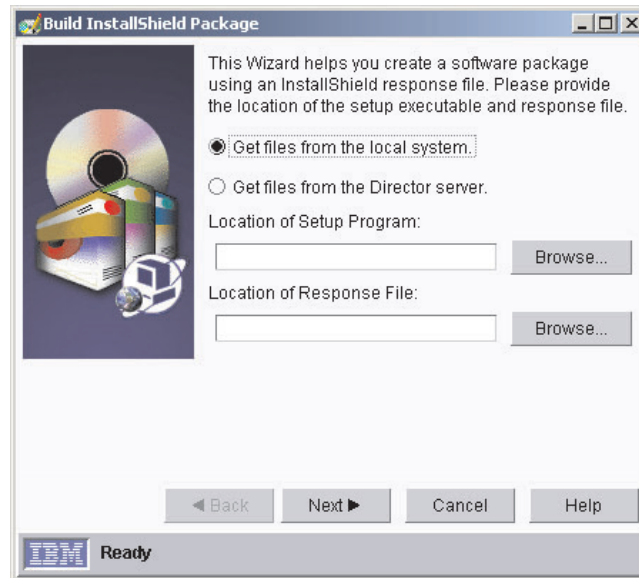


Figure 115. InstallShield Package wizard

3. Specify whether the files are 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) Specify additional command-line parameters that are specific to the application that you are importing by typing the applicable command-line parameters.
6. (Optional) To install the software under a different user name and password, click **Advanced**. Type the applicable information and click **OK**.
7. Click **Finish**. Individual software packages are displayed under the **All Software Distribution Packages** category.

You can distribute the software package now or schedule a later time for distribution. For more information, see “Distributing a software package” on page 250.

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 program.

Note: To determine whether an application uses Windows Installer technology, search for an MSI file in the top level of the application directory.

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 only to managed systems running Windows.

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 116. Microsoft Windows Installer Package wizard

3. In the **Package Name** field, type the package name.
4. Specify whether the files are 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**.
5. (Optional) Specify a Microsoft software transformation (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.
6. (Optional) To install the software under 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**. 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 now or schedule a later time for distribution. For more information, see “Distributing a software package” on page 250.

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 program. The RPM program is the common installer for all IBM Director-supported Linux operating systems. An RPM is an archive of files that are 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 RPM software packages for distribution only to managed systems running Linux or AIX.

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.

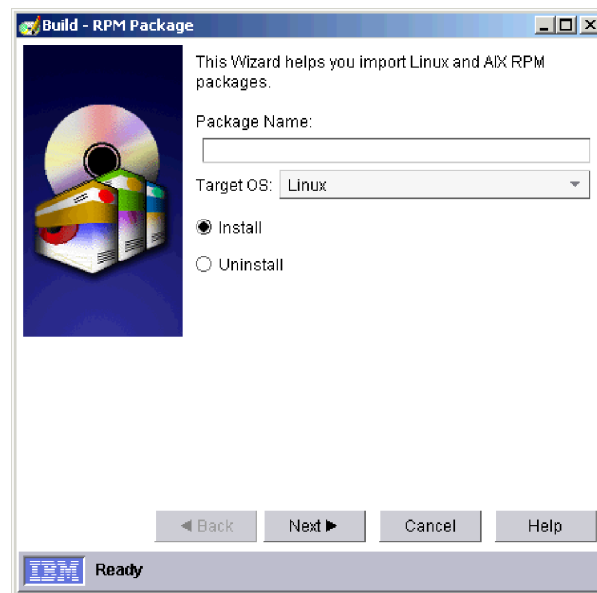


Figure 117. RPM Package wizard

3. In the **Package Name** field, type the package name.
4. In the **Target OS** field, select **Linux** or **AIX**.
5. Select **Install** to install the software package.
6. Click **Next**.
7. Specify whether the files are on the local management console or on the management server by clicking the applicable button. Then, select the RPMs that you want to import by clicking **Add**. A separate window opens in which you can select the files that you want to import. You can select more than one RPM to import at a time.
8. Click **Finish**. The software package name is displayed in the IBM Director Console Tasks pane under the **All Software Distribution Packages** category.

You can distribute the software package now or schedule a later time for distribution. For more information see “Distributing a software package” on page 250.

Complete the following steps to uninstall 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.
3. In the **Package Name** field, type the package name.
4. In the **Target OS** field, select **Linux** or **AIX**.
5. Click **Uninstall** to uninstall the software package.
6. Click **Next**.
7. Select the RPM that you want to uninstall by clicking **Add** and entering the RPM name.
8. Click **Finish**.

Using the AIX InstallP Package wizard

Use the AIX InstallP Package wizard to install or uninstall an AIX InstallP format package.

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 **AIX InstallP Package**. The AIX InstallP Package wizard starts.

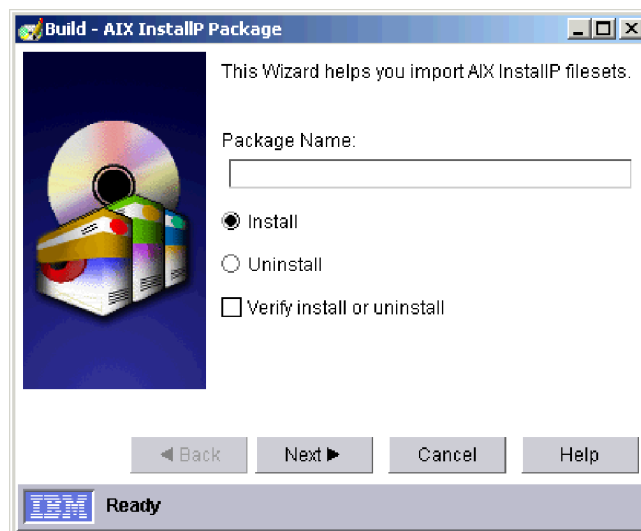


Figure 118. AIX InstallP Package wizard

3. In the **Package Name** field, type the package name.
4. Select **Install** to install the software package.
5. (Optional) Select the **Verify install or uninstall** check box.
6. Click **Next**.
7. Specify whether the files are on the local management console or on the management server by clicking the applicable button. Then, select the InstallP filesets that you want to import by clicking **Add**. A separate window opens in which you can select the files that you want to import. You can select more than one fileset to import at a time.

8. Click **Finish**.

Using the OS/400 Restore Library Package wizard

An OS/400 (i5/OS) library is an object that is used to find other OS/400 objects in the file system. Use the OS/400 Restore Library Package wizard to build a package to restore a library to a managed system running OS/400.

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 **OS/400 Restore Library Package**. The OS/400 Restore Library Package wizard starts.

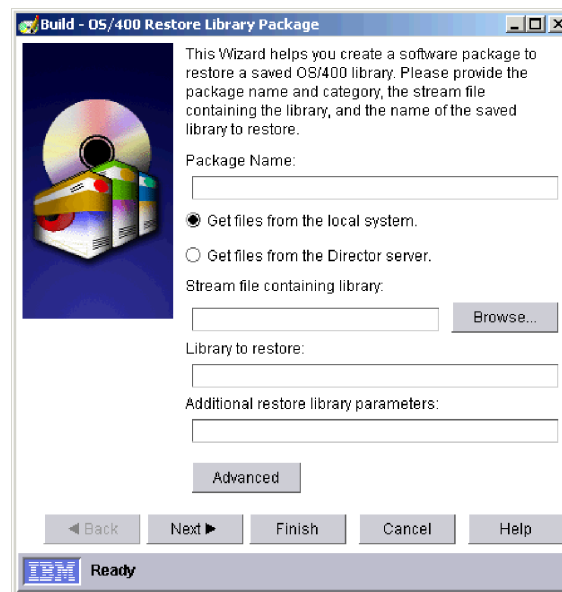


Figure 119. OS/400 Restore Library Package wizard

3. In the **Package Name** field, type the package name.
4. Specify whether the files are on the local management console or on the management server by clicking the applicable button.
5. Type the name of the stream file that contains the library or click **Browse** to locate it.
6. Type the name of the library to restore from the stream file.
7. (Optional) Type any additional library restore parameters.
8. (Optional) Click **Advanced** to open the “Advanced Options” window.

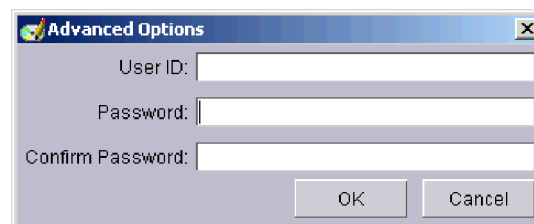


Figure 120. OS/400 Restore Library Package wizard: “Advanced Options” window

Type the user ID and password; then click **OK**.

9. Click **Next**.
10. Click **Finish**.

Using the OS/400 Restore Licensed Program Package wizard

Use the OS/400 Restore Licensed Program Package wizard to build a package to restore a program to a managed system running OS/400.

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 **OS/400 Restore Licensed Program Package**. The OS/400 Restore Licensed Program Package wizard starts.

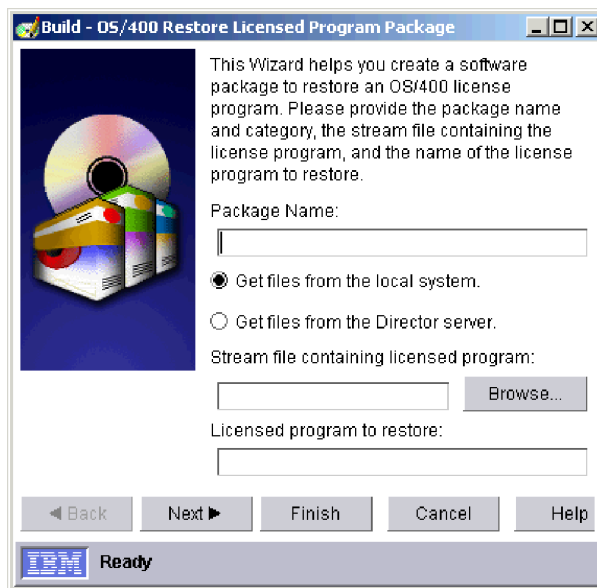


Figure 121. OS/400 Restore Licensed Program Package wizard

3. In the **Package Name** field, type the package name.
4. Specify whether the files are on the local management console or on the management server by clicking the applicable button.
5. Type the name of the stream file that contains the licensed program or click **Browse** to locate it.
6. Type the name of the licensed program to restore from the stream file.
7. Click **Next**.
8. Click **Finish**.

Using the OS/400 Restore Object Package wizard

Use the OS/400 Restore Object Package wizard to build a package to restore an object to a managed system running OS/400.

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 **OS/400 Restore Object Package**. The OS/400 Restore Object Package wizard starts.

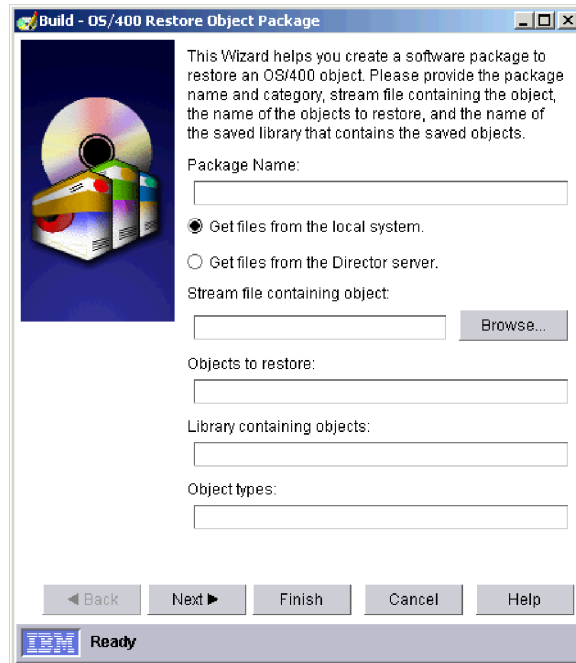


Figure 122. OS/400 Restore Object Package wizard

3. In the **Package Name** field, type the package name.
4. Specify whether the files are on the local management console or on the management server by clicking the applicable button.
5. Type the name of the stream file that contains the object or click **Browse** to locate it.
6. Type the name of the object to restore from the stream file.
7. Type the name of the objects.
8. Type the name of the library that contains the objects.
9. Type the object types.
10. Click **Next**.
11. (Optional) Type any additional object parameters.
12. Click **Finish**.

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. You can specify the 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.

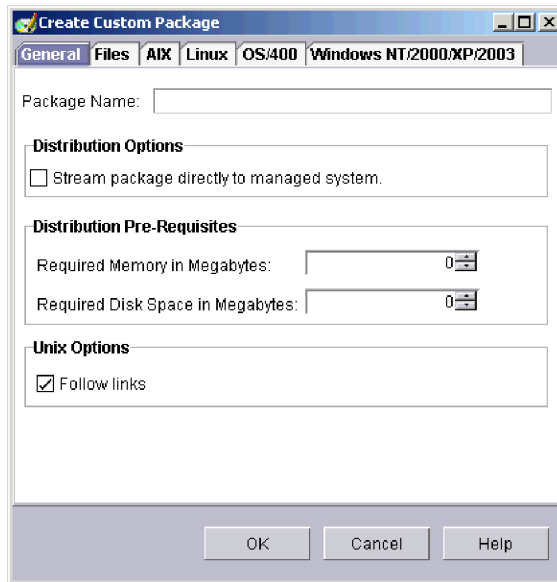


Figure 123. Custom Package Editor: “Create Custom Package” window

This window has the following tabs:

- General
- Files
- AIX
- Linux
- OS/400
- Windows NT/2000/XP/2003

3. On the General page, specify the package name and any distribution options and prerequisites.
4. On the Files page, specify the files to use by navigating to each file in the Source File System pane and clicking **Add**. You can change whether the files are displayed from the local management console or from the management server by selecting from the list at the top of the pane.

Note: If you want to include all subdirectories in a parent directory, select the **Include subfolders** check box or the **Save full path information** check box if maintaining the file structure is important; then, select the directory and click **Add**.

5. Select to distribute a software package to a managed system running an AIX, Linux, OS/400, or Windows operating system by selecting the applicable check box on the applicable page.
6. (Optional) In the Execute Pre-Distribution pane, click **Advanced**. The “Pre-Distribution” window opens.

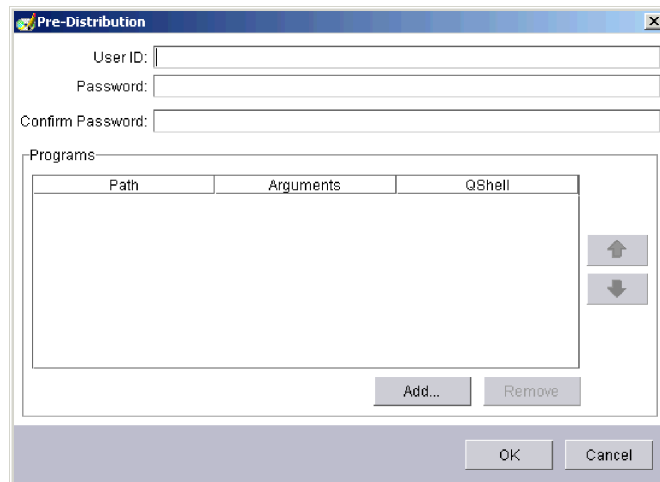


Figure 124. Custom Package Editor: “Pre-Distribution” window

7. (Optional) Select an application to run on the managed system before the software distribution occurs. You can select multiple applications and specify the order in which they run. When complete, click **OK**.
8. (Optional) In the Execute Pre-Distribution pane, select the **File exists on target system** check box if the specified application exists on the managed system.
9. (Optional, OS/400 only) In the Execute Pre-Distribution pane, click **Native** or **QShell** to select how the application is to be run.
10. (Optional) In the Execute Post-Distribution pane, click **Advanced**. The “Post-Distribution” window opens.

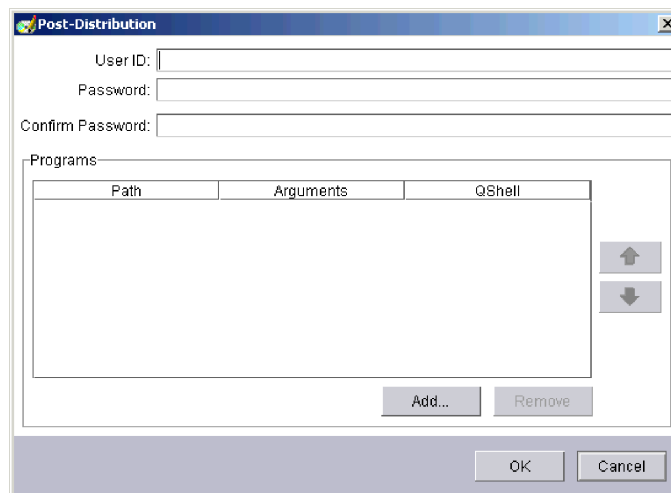


Figure 125. Custom Package Editor: “Post-Distribution” window

11. (Optional) Select an application to run on the managed system before the software distribution occurs. You can select multiple applications and specify the order in which they run. When complete, click **OK**.
12. (Optional, OS/400 only) In the Execute Post-Distribution pane, click **Native** or **QShell** to select how the application is to be run.

- (Optional, AIX, Linux, and OS/400 only) Click **File Permissions**. The “File Permissions” window opens.

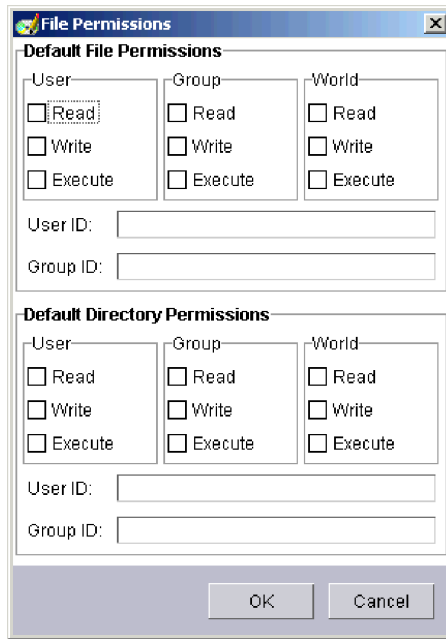


Figure 126. Custom Package Editor: “File Permissions” window

- (Optional, AIX, Linux, and OS/400 only) Set the file and directory permissions for the software distribution and click **OK**.

Note: (Managed systems running Linux only) By default, files that are copied to a managed system running Linux are set with the default permission or the account that IBM Director Agent runs as, which is the root account. Use the “File Permissions” window to set alternative permissions for the software distribution.

- (Optional, Windows only) Click **Do Nothing** or **Restart Computer** to select whether to restart the managed system after the software distribution is completed.
- (Optional, Windows only) Click **Windows NT/2000/XP/2003 Configuration**. The “Windows NT/2000/XP/2003 Configuration” window opens.

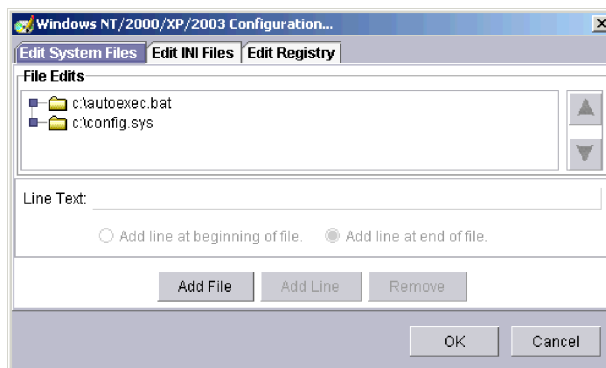


Figure 127. Custom Package Editor: “Windows NT/2000/XP/2003 Configuration” window

17. (Optional, Windows only) Specify that changes in Windows system files, INI files, and Registry keys are to be distributed to the managed system and click **OK**.
18. Click **OK**. 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 now or schedule a later time for distribution. For more information, see “Distributing a software package” on page 250.

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. Create these files by exporting an IBM Director software package. If you want to import a software package that was created in IBM Director, you must use this wizard.

Note: You cannot use the Director File Package wizard to import SPB files that were created by Tivoli software or signed package (BFP) format software packages that were created with IBM Director version 3.1 or earlier.

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.

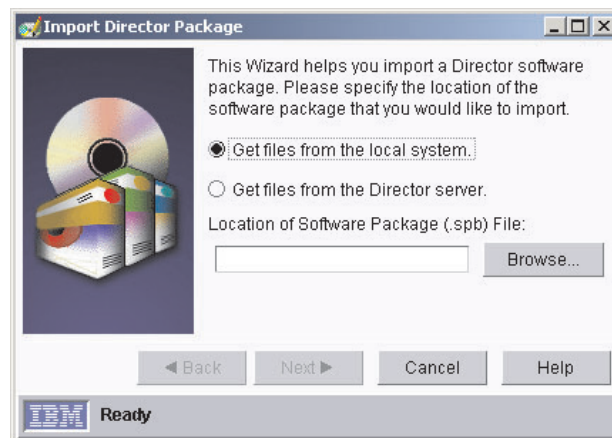


Figure 128. Director File Package wizard

3. Specify whether the files are 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.
4. Click **Next**.
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 now or schedule a later time for distribution. For more information, 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 40.)

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 that is 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.

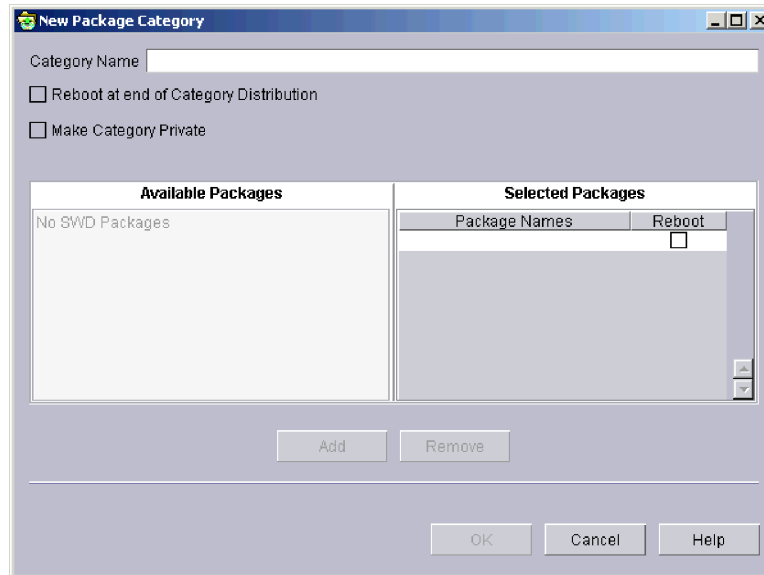


Figure 129. “New Package Category” window

2. In the **Category Name** field, type a category name.
3. In the Available Packages pane, click a package; then, click **Add**. The order in which the software packages are displayed in the Selected Packages pane specifies the order of delivery when that category is distributed. To modify the order in which software packages are delivered, in the Package Names column, select a package; then, drag the package to its new location.
4. (Optional) Set the managed system to restart after delivery of a specific software package by selecting the **Reboot** check box for that package in the Selected Packages pane.
5. (Optional, Windows only) To restart the managed system after all software packages in that category are delivered, select the **Reboot at end of Category Distribution** check box.
6. (Optional) Select the **Make Category Private** check box to make the new category visible to only the IBM Director account that created it.
7. Click **OK** 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 that you want to edit and click **Open**. The “Edit Package Category” window opens.
3. In the Available Packages pane, click a package; then, click **Add** to add the package to the category, or right-click a software package in the Selected Packages pane and click **Remove** to delete it from the category. The order in which the software packages are displayed in the Selected Packages pane specifies the order of delivery when that category is distributed. To modify the order in which software packages are delivered, in the Package Names column, select a package; then drag the package to its new location.
4. (Optional) To specify that the managed system is to restart after delivery of a specific software package, select the **Reboot** check box for that package in the

Selected Packages pane. Or, to restart the managed system after all software packages in that category are delivered, select the **Reboot at end of Category Distribution** check box.

5. (Optional) Select the **Make Category Private** check box to make the new category visible to only the IBM Director account that created it.
6. Click **OK** to save any changes that you 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 system 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 the package, and click **OK**.

Exporting a software package (Premium Edition)

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**.

Notes:

1. Exporting a software package is not supported when IBM Director Server is installed on a server running OS/400.

2. Software Distribution does not support exporting packages to a network share. If a package is exported to a network share, the export fails, and the following error message is displayed: Unable to export package. Modify the export to export to a local drive.

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.

Complete the following steps to change your software-distribution server preferences:

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

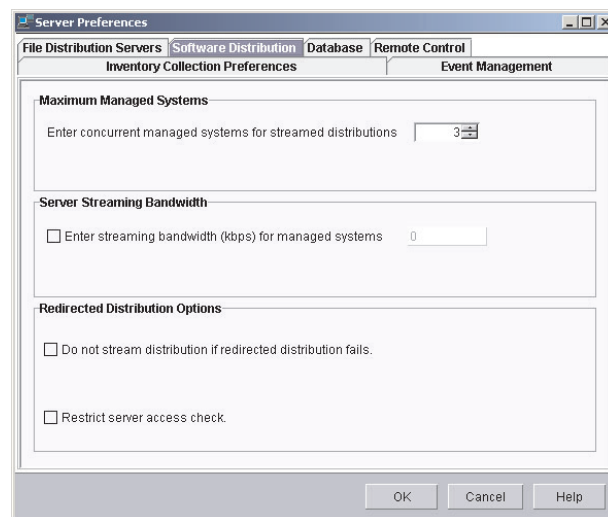


Figure 130. “Server Preferences” window: Software Distribution page

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

Complete the following steps to change your software-distribution preferences for a managed system or group:

1. In the IBM Director Console Group Contents pane, right-click a managed system or group of managed systems and click **Distribution Preferences**. The “Distribution Preferences” window opens.

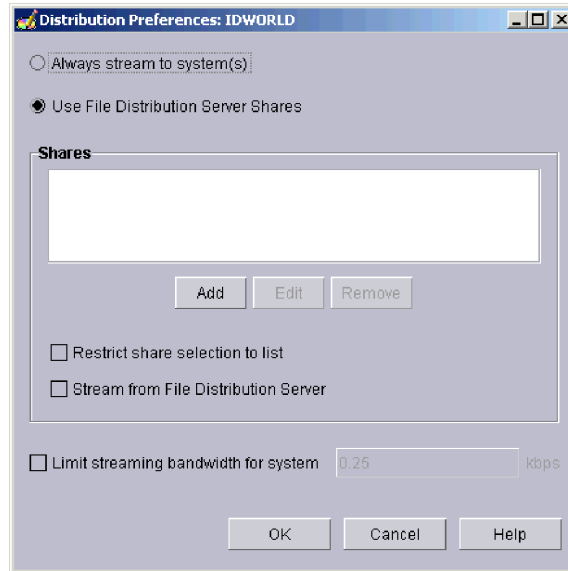


Figure 131. “Distribution Preferences” window

2. Select **Always stream to system(s)** to stream the software-distribution package from the management server to that managed system.
3. Select **Use File Distribution Server Shares** to stream the software-distribution package from a shared directory (share) to that managed system. If you select **Use File Distribution Server Shares**, you can select specific shares to use from the shares that are defined on the File Distribution Servers page of the “Server Preferences” window. Click **Add** to select a share.
4. Select the **Restrict share selection to list** check box to use only the shares that are listed in the **Shares** field.

Note: If this check box is selected and the managed system is unable to connect to any of the defined shares, the software distribution will fail.

5. Select the **Stream from File Distribution Server** check box to copy the contents of a software-distribution package to the managed system before installation.
6. Click **OK** to update the distribution preferences for that managed system or group.

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 that are 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**.

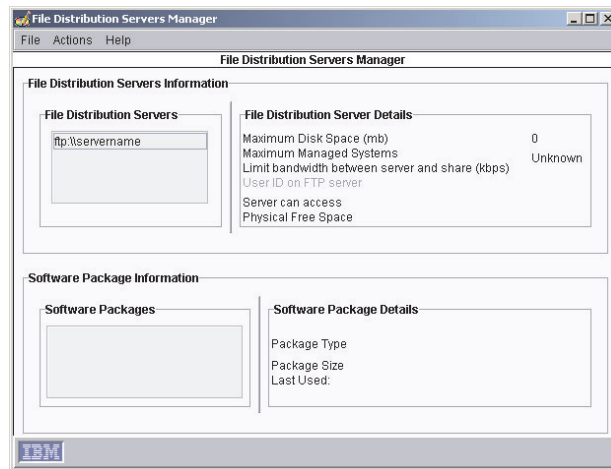


Figure 132. “File Distribution Servers Manager” window

The software packages that are stored on the file-distribution server that is selected in the **File Distribution Servers** group box are displayed in the **Software Packages** group box. In the **File Distribution Server Details** group box, **Maximum Managed Systems** indicates the maximum number of managed systems that can access the file-distribution server at one time.

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**.

Chapter 27. Software Rejuvenation

You can use the Software Rejuvenation task, which is part of the Server Plus Pack, to avoid unplanned system outages that are 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 resource exhaustion and system outages, and generates resource exhaustion events; after being 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, 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 according to 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 systems. The “Software Rejuvenation” window opens.

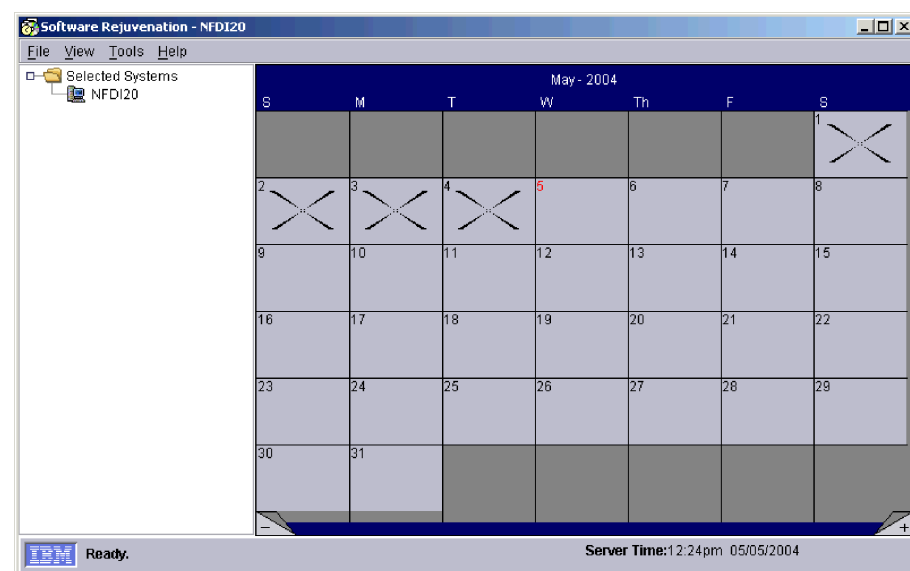


Figure 133. “Software Rejuvenation” window

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

You can start Software Rejuvenation by dragging the **Software Rejuvenation** task onto a single system, a single group, or a single Windows cluster in the Groups pane of IBM Director Console. You also can select multiple systems in the Groups pane and drag the **Software Rejuvenation** task onto any of the selected systems. The left pane of the “Software Rejuvenation” window displays the selected managed system or systems, and managed systems of a group as individual managed systems.

Configuring a service rejuvenation

You must configure Software Rejuvenation 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 systems. The “Software Rejuvenation” window opens.
2. Select a managed system or systems in the left pane.
3. Click **Tools** → **Service Rejuvenation**. The “Service Rejuvenation” window opens. See Figure 134. The **Selected Systems** field displays the managed system or systems that you selected in the **Selected Systems** pane of the “Software Rejuvenation” window.

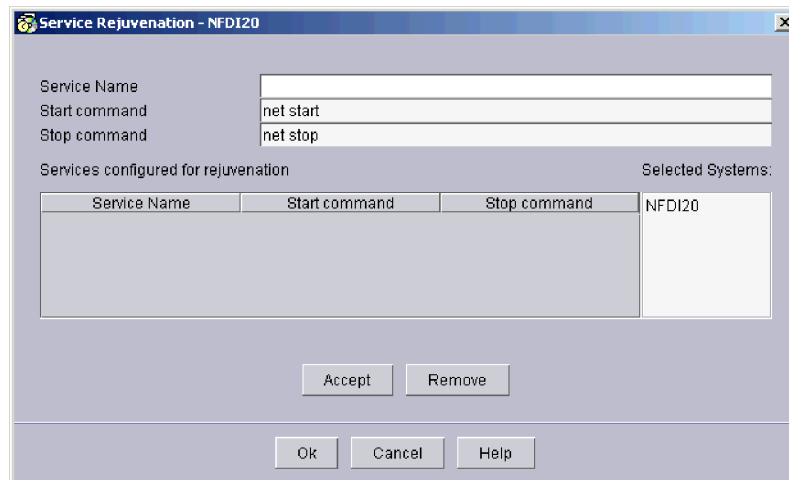


Figure 134. “Service Rejuvenation” Window

4. 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 7 on page 259.
5. In the **Start command** field, type the command that is used to start this daemon. (For Windows services, this field is filled automatically with net start and cannot be changed.)
6. In the **Stop command** field, type the command that is used to stop this daemon. (For Windows services, this field is filled automatically with net stop and cannot be changed.)

7. Click **Accept**. The Windows service or Linux daemon name, start command, and stop command are displayed in the list of services that are configured for rejuvenation.
8. Click **OK** to complete the configuration.
9. Click **View** → **Refresh**. 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. For more information, see “Scheduling a software rejuvenation.”

Scheduling a software rejuvenation

You can schedule a software rejuvenation for a managed system or a service to occur on a specific day or time or at a specified frequency.

Scheduling a software rejuvenation for one or more managed systems

Complete the following steps to schedule a software rejuvenation for a managed system or systems:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or systems. The “Software Rejuvenation” window opens.
2. In the left pane, click one or more managed systems for which you want to schedule a rejuvenation; then, drag the selected managed system or systems onto the calendar date (in the right pane) on which you want the first rejuvenation to occur. The “Repeat Schedule - Server” window opens. See Figure 135. The **Selected Systems** field displays the target objects that you selected in the “Software Rejuvenation” window.

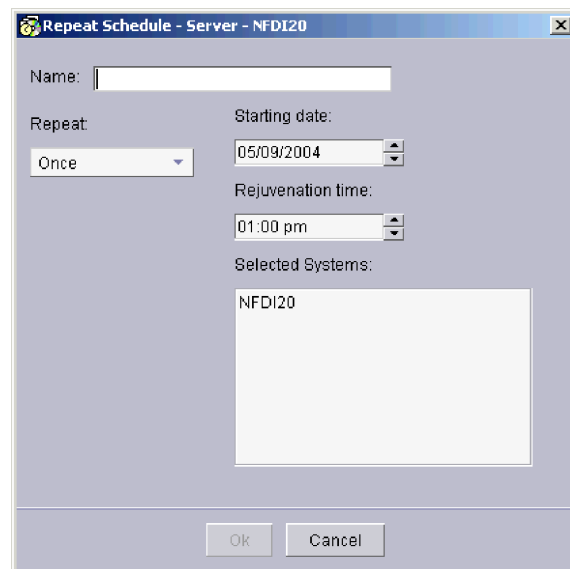


Figure 135. “Repeat Schedule - Server” window

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.

Scheduling a software rejuvenation for a service

Complete the following steps to schedule a software rejuvenation for a service:

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or systems. The “Software Rejuvenation” window opens.
2. In the left pane, click the managed system or systems and a single service on which you want to schedule a rejuvenation; then, drag the managed system or systems onto the calendar date (in the right pane) on which you want the first rejuvenation to occur. The “Repeat Schedule - Service” window opens. See Figure 136. The **Selected Systems** field displays the managed system or systems that you selected in the “Software Rejuvenation” window.

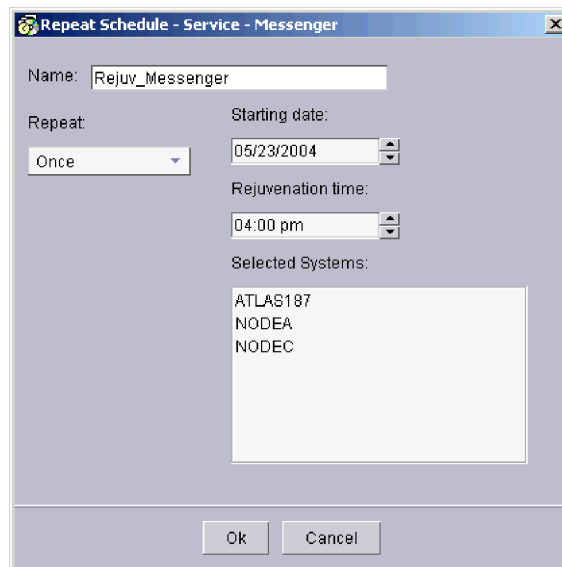


Figure 136. “Repeat Schedule - Service” window

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 systems. The “Software Rejuvenation” window opens.
2. In the Calendar pane, right-click the schedule that you want to edit, and 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

Note: If a managed system is scheduled for rejuvenation using a repeating schedule, such as every Tuesday, deleting the schedule for one date deletes the entire named 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 systems. The “Software Rejuvenation” window opens.
2. In the Calendar pane, right-click the schedule that 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.

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.

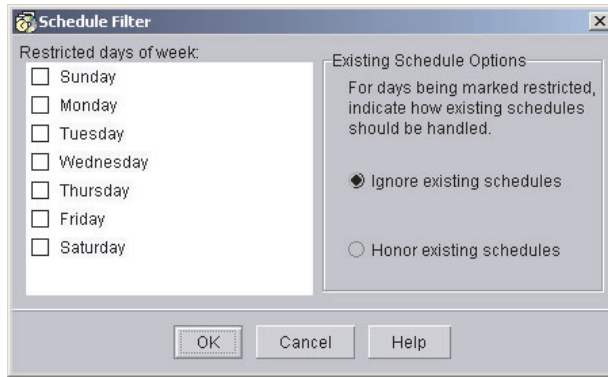


Figure 137. “Schedule Filter” window

3. Select the check boxes of the days of the week on which you want to prevent rejuvenations from occurring.
4. In the **Existing Schedule Options** group box, specify whether 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 systems. The “Software Rejuvenation” window opens.
2. Click **Tools** → **Rejuvenation Options**. The “Rejuvenation Options” window opens.

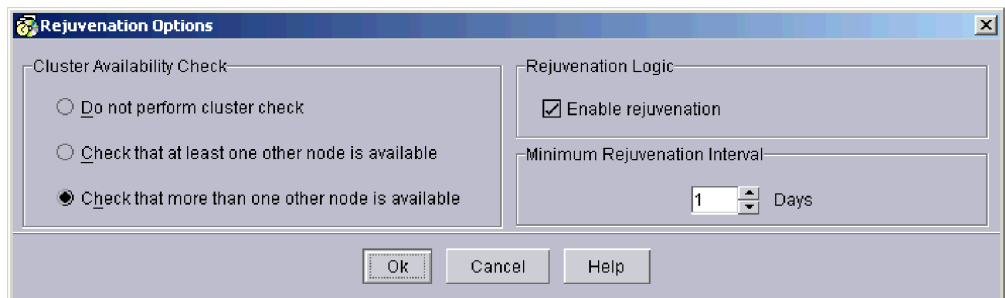


Figure 138. “Rejuvenation Options” window

You can set the following parameters:

Cluster Availability Check group box

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

Enables or disables all rejuvenations. This setting is maintained by IBM Director Server and applies to all rejuvenations that are scheduled through that management server.

Minimum Rejuvenation Interval

Specifies the number of days that must elapse between rejuvenations.

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

Predicting resource exhaustion

You can predict resource exhaustion for a managed system or systems according to trends in resource utilization. When resource exhaustion is predicted, an alert is generated, and a rejuvenation can be scheduled automatically. Before you can use the prediction option, you must configure this option using the Prediction Configuration wizard.

Table 21 lists the resource monitors that Software Rejuvenation monitors for resource-exhaustion prediction.

Table 21. Resource monitors for resource-exhaustion prediction

Managed systems running	Resource monitors
Windows	<ul style="list-style-type: none"> • Pooled Paged Bytes • Pooled NonPaged Bytes • Committed Bytes • Logical Disk
Linux	<ul style="list-style-type: none"> • Logical Disk Space • Logical Disk Inodes • Swap Space • File Descriptors • Processes

Configuring the prediction option

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

1. In the IBM Director Console Tasks pane, drag the **Software Rejuvenation** task onto a managed system or systems. The “Software Rejuvenation” window opens.
2. In the left pane, click a managed system or systems.
3. Click **Tools** → **Prediction** → **Configure Wizard** to start the wizard. The “Modify Configuration Forecasting Data” window opens.

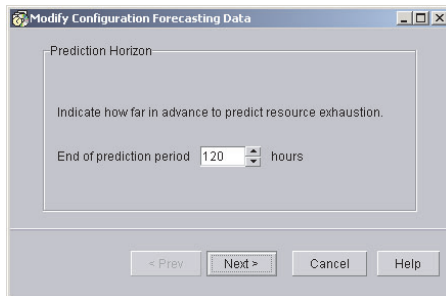


Figure 139. Prediction Configuration wizard: “Modify Configuration Forecasting Data” window

4. 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 be exhausted between the current time and the prediction horizon, a notification (alert) and, optionally, a rejuvenation schedule are generated. Note that prediction horizons less than 24 hours might cause high microprocessor utilization on slower managed systems.
 5. Click **Next**. The “Modify Configuration Notification and Scheduling” window opens.
 6. Select the parameters that control alerts and rejuvenation schedules.
 - Select whether you want both a notification (alert) and a rejuvenation schedule to be generated, or whether you want a notification only.
 - Specify how software rejuvenation handles the case in which an automatically generated rejuvenation schedule conflicts with a day that has been marked previously as restricted for rejuvenations.
 - Select **Honor Restricted Day settings** if you want the restricted-day setting to block the rejuvenation schedule.
 - Select **Ignore Restricted Day settings** if you want the rejuvenation schedule to override the restricted-day designation. Note that an alert will be sent and the system will be 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 must not exceed the prediction horizon.
 7. Click **Next**. The “Modify Configuration Action Plan” window opens.
 8. Create a simple event action plan that is run when a resource exhaustion is predicted.
 - Select **Console** if you want a message to be displayed in IBM Director Console. Type the message that you want to display, the user names of the individuals who will receive the message, and the delivery criteria for the message.
 - Select **Ticker Tape** if you want a message to run in the ticker tape of IBM Director Console. Type the message that you want to display and the user names of the individuals who will 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. For more information, see “Creating an event filter for software-rejuvenation events” on page 265.
9. Click **Finish** to complete the configuration.

When you complete the 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 left pane of the “Software Rejuvenation” window.

Starting prediction with default settings

You can quickly start resource-exhaustion prediction with default settings. The default settings are:

- **Prediction Horizon:** 120 hours
- **Resource Exhaustion Notification:** Notify and Schedule Rejuvenation
- **Options for Automatic Scheduling:** Honor Restricted Day Settings
- **Grace Time:** 0 hours
- **Action Plan:** None (no Message, User, or Delivery Criteria)

Complete the following steps to configure a managed system or systems for prediction with the default settings:

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 or systems.
3. Click **Tools** → **Prediction** → **Start with defaults** to start the configuration wizard.

Ending prediction

To end prediction on a managed system or systems, 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 “Predicting resource exhaustion” on page 263 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 systems. The “Software Rejuvenation” window opens.
2. In the left pane, click a managed system or systems.
3. Click **Tools** → **Trend Viewer**. The “Trend Viewer” window opens.
4. From the **Resource** list, select the resource that you want to view. The selected resource is displayed.

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 are only for 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 Chapter 4, “Managing and monitoring systems with event action plans,” on page 55.

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 listed events.
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.

To be notified of a software-rejuvenation event, you must create a new event action plan, customize an event action, and then associate the filter that you just created with the event action and the event action plan. See “Building an event action plan” on page 59 for more information about how to do this.

Using keyboard shortcuts

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

Ctrl+C

After selecting a highlighted object or a day in the calendar that contains a rejuvenation schedule icon, use this shortcut to save a copy of it for pasting.

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 in which there are multiple schedules, a menu is displayed in which you can select which schedule to delete.

Ctrl+H

Use this shortcut to highlight all of the days that are associated with a rejuvenation schedule.

Ctrl+V After copying a highlighted object or a day in the calendar that contains a rejuvenation schedule icon, select a day in the calendar and use this shortcut to paste the copy onto the selected day.

Chapter 28. System Accounts

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

Adding a group

Complete the following steps to add a group:

1. Drag the **System Accounts** task onto a managed system or group that supports System Accounts. The “System Accounts” window opens.

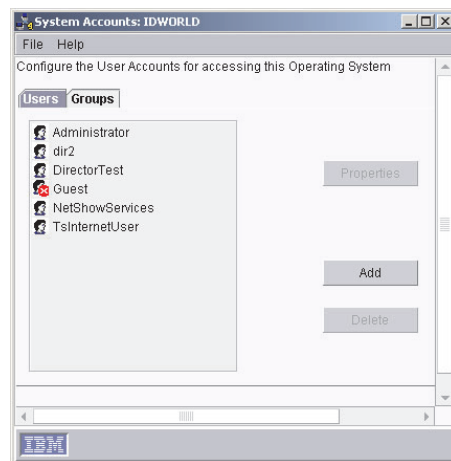


Figure 140. “System Accounts” window

2. Click the **Groups** tab.
3. Click **Add**. The “Group Configuration” page opens.
4. In the **Name** field, type the group name.
5. (Optional) In the **Description** field, type a description.
6. Click **Accept**.
7. Click **Apply**.

Deleting a user

Complete the following steps to delete a user:

1. Drag the **System Accounts** task onto a managed system or group that supports System Accounts. The “System Accounts” window opens.
2. Click the **Users** tab.
3. In the **Users** field, select a user name.
4. Click **Delete**. A window opens that displays the following message:
Note: User not deleted until the apply button is clicked!
5. Click **Close** to close the window.
6. Click **Apply**.

Editing group membership

Complete the following steps to add a user to a group or to remove a user from a group:

1. Drag the **System Accounts** task onto a managed system or group that supports System Accounts. The “System Accounts” window opens.
2. Click the **Groups** tab.
3. In the **Users** field, select **Administrators**.
4. Click **Properties**. The “Group Configuration” page opens.
5. If you are adding a user to the group, complete the following steps:
 - a. In the **Non-members** field, select a user name.
 - b. Click < to move the selected non-member to the **Members** field.If you are removing a user from a group, complete the following steps:
 - a. In the **Members** field, select a user name.
 - b. Click > to move the selected member to the **Non-members** field.
6. Click **Accept**.
7. Click **Apply**.

Chapter 29. System Availability

You can use the System Availability task, which is 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 that you specify as being problematic are flagged as such. You can run the System Availability task on a managed system or group immediately or schedule a System Availability task using the Scheduler task (see “Scheduler” on page 40 for more information on how to schedule tasks).

Notes:

1. To use the function that identifies a managed system as problematic, the managed system must have the IBM Director (version 4.1 or later) System Availability Agent installed.
2. (Windows only) The System Availability task uses information from the system log file; a damaged, missing, or full system log file affects this task. If you clear the system log file, all system-availability information is lost.
3. (Linux only) The System Availability task uses information from the `/var/log/messages` file.
4. IBM Director Server stores system-availability reports in the `IBM\Director\Reports\System Availability` directory. You can change the location where IBM Director Server stores system-availability reports in the “Settings” window. See “Changing the settings criteria” on page 272.

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.

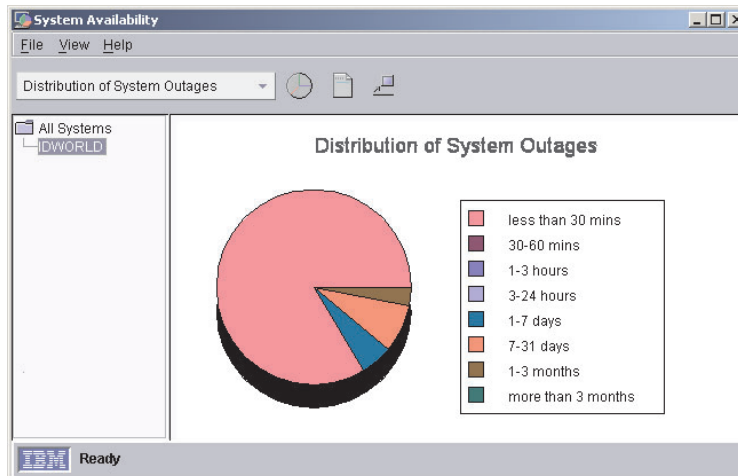


Figure 141. “System Availability” window

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.

To see the value of a specific pie chart or bar chart section, move the cursor over the section.

Notes:

1. (Windows operating systems that support IBM Director and are configured to adjust automatically for daylight saving time only) The event times that are specified in the system-availability report might vary by 1 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 managed systems where compression of message logs is the default, turn off compression of message logs to view system-availability reports.
3. System Availability reads the message logs only if the message logs are in their default directory.
4. System Availability should run as or more often than the message logs are archived to avoid losing availability information.

You can view the availability report, which is an overall statistical summary of event and problematic details, 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. Systems identified as problematic are listed in the detail section and are flagged with a red X.

For a more detailed view of the availability report, right-click the graph and click **Detailed List of Record**. The “System Downtime” window opens and displays a detailed report.

System N...	Stop Time	Restart Time	Duration Time	Event Type
IDWORLD	Monday, April 19, 2004 ...	Monday, April 19, 200...	0 day(s) 00:04:...	Unplanned Out...
IDWORLD	Monday, April 19, 2004 ...	Monday, April 19, 200...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Tuesday, April 20, 2004...	Tuesday, April 20, 200...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Tuesday, April 20, 2004...	Tuesday, April 20, 200...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Tuesday, April 20, 2004...	Tuesday, April 20, 200...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Tuesday, April 20, 2004...	Tuesday, April 20, 200...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Tuesday, April 20, 2004...	Tuesday, April 20, 200...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Tuesday, April 20, 2004...	Tuesday, April 20, 200...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Friday, April 30, 2004 2:...	Friday, April 30, 2004 ...	0 day(s) 00:02:...	Planned Outage
IDWORLD	Monday, May 3, 2004 6:...	Monday, May 3, 2004 ...	0 day(s) 00:02:...	Planned Outage

Figure 142. “System Downtime” window

In the “System Availability” window, you can detach the current view to compare and contrast different system-availability views and time frames. Click **View → Detach View**. The current view is separated as an independent window that does not reflect subsequent changes to the report. Closing the System Availability task closes any detached view windows.

With the exception of a detached view and the “System Downtime” window, you can print any window that is 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 “Customization of Graph Dates” window opens.

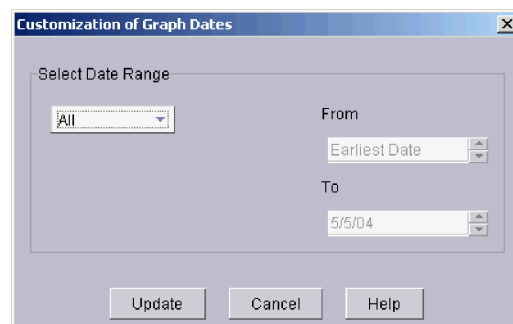


Figure 143. “Customization of Graph Dates” window

2. In the **Select Date Range** field, select one of the following time ranges for which you want to view data.

All Select this range to display system-availability data from the time that System Availability was loaded on the target system up to the present day. This selection is the default.

1 week Select this range to display system-availability data from one previous week up to midnight of the present day.

1 month Select this range to display system-availability data from one previous month up to midnight of the present day.

3 months Select this range to display system-availability data from three previous months up to midnight of the present day.

1 year Select this range to display system-availability data from one previous year up to midnight of the present day.

Customize Select this option to customize the range of time for which to display system-availability data.

Note: (Optional) If you select **Customize**, type the From and To dates in the applicable fields.

3. Click **Update**.

Note: These customized settings apply only to the currently open System Availability report and are not global settings applicable to all System Availability reports.

Changing the settings criteria

System Availability scans for problematic systems within a range of time. 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 time frame 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 in which the managed system has unplanned outages, instead of a specific number of outages, by selecting the **Percentage** check box.

1. To specify the settings criteria, click **File** → **Settings**. The “Settings” window opens.

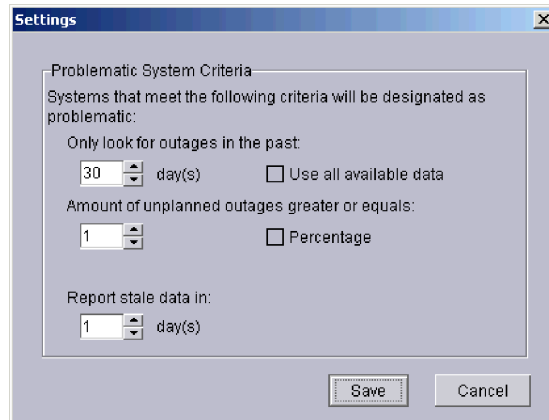


Figure 144. “Settings” window

2. Change any of the criteria; then, click **Save**.

Note: Select **Use all available data** to evaluate all persistent data available in the IBM Director Server database.

All system-availability reports that are run after you click **Save** use the new settings.

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. You also can save the current report in XML format.

Complete the following steps to export a report in HTML format:

1. Follow the steps in “Starting the System Availability task” on page 269 to generate a system-availability report.
2. After the report is generated, click **File** → **Export Availability Report** → **Export HTML 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 that you specified.
5. (Windows only) In the “Open saved file” window, in the **File name** field, type a file name; then, click **Select** to save the report to the specified location.
6. (Windows only) Click **Yes** to open the exported report in a Web browser immediately.

Complete the following steps to export a report in XML format:

1. Follow the steps in “Starting the System Availability task” on page 269 to generate a system-availability report.
2. After the report is generated, click **File** → **Export Availability Report** → **Export XML 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 that you specified.

Part 3. IBM Director features for accessing IBM Director components

Chapter 30. Working with management servers using the command-line interface (DIRCMD).....	277
Chapter 31. Working with managed systems using Web-based Access (Windows only).....	305

Chapter 30. 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). DIRCMD is the command-line interface for IBM Director Server. You can use a command-line prompt to access, control, and gather information from IBM Director Server. You can use DIRCMD in a script to perform a task automatically and confirm the task status through the use of exit codes.

Installing and accessing DIRCMD

DIRCMD is automatically installed with IBM Director Server, IBM Director Agent, and IBM Director Console. It is available on all operating systems that support IBM Director 4.1 or later, except Novell NetWare.

The system from which you invoke 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 Sockets Layer (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 more than one command, 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 that you want to invoke, for example:
 - server (server management)
 - native (managed system)
 - event (event management)
 - monitor (resource monitor)
 - procmon (process monitor)
 - snmp (SNMP device)
 - MPA (Management Processor Assistant)
 - bladecenterconfiguration (BladeCenter configuration)
 - bladecenterchassis (BladeCenter chassis)
 - chassis
- *command* specifies the command of the bundle.

- *arguments* specifies options for the specified command.

Management

Table 22 describes the management commands. All of these commands are required.

Table 22. DIRCMD management commands

Command	What it does	Syntax
server	Specifies the management server.	-s <i>server</i> where <i>server</i> is one of the following parameters: <ul style="list-style-type: none"> • The DNS-resolvable host name of the management server • The TCP/IP address of the management server
userID	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.
password	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. Note: A null or empty password can be used.

Example

To begin a DIRCMD session, you 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 that is associated with the InfoDeveloper account.

Options

Table 23 describes the DIRCMD options. All of these commands are optional.

Table 23. DIRCMD options

Command	What it does	Syntax
bundle	Lists all of the DIRCMD bundles.	-b Notes: <ol style="list-style-type: none"> 1. When this command is issued, no other commands can be issued. 2. The list of DIRCMD bundles is provided from the management server, not the DIRCMD client.
help	Provides help about DIRCMD usage and syntax.	-h Notes: <ol style="list-style-type: none"> 1. When this command is issued, no other commands can be issued. 2. The help is provided from the management server, not the DIRCMD client.

Table 23. DIRCMD options (continued)

log	<p>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.</p>	<p>-l [clear / size=<i>n</i>]</p> <p>where</p> <ul style="list-style-type: none"> • clear resets the DIRCMD log. • <i>n</i> is the maximum number of entries in the DIRCMD log. By default, this is set to 100. <p>Notes:</p> <ol style="list-style-type: none"> 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 issued.
filename	<p>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 that are supplied at the command prompt.</p> <p>Unlike when the pipe option is issued, the file contents are treated as a single value. Use the -f option only with specific tasks that require large amounts of input such as creating BladeCenter Deployment wizard configuration profiles.</p>	<p>-f <i>filename</i></p> <p>where <i>filename</i> is the path and name of the file.</p>
pipe	<p>Directs the DIRCMD client to receive command-argument data from an input pipe. The data is read <i>after</i> any command arguments that are 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.</p>	<p>-r</p>
k	<p>Directs the DIRCMD client to override the default TCP/IP data link connection class, com.tivoli.twg.libs.TWGTCPILink.</p>	<p>-k <i>datalink</i></p> <p>where <i>datalink</i> is the data link connection class. Use -k com.tivoli.twg.libs.TWGSSLLink to use the SSL data link connection class.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If this command is used, you might have to specify data link parameters to successfully configure the data link. 2. To use SSL, IBM Director Server must be configured to listen for the secure connection request.
o	<p>Specifies data link parameters. The default TCP/IP data link parameter is 2034, which sets the socket port for com.tivoli.twg.libs.TWGTCPILink. For SSL, the data link parameter is 2035, which sets the socket port for com.tivoli.twg.libs.TWGSSLLink.</p>	<p>-o <i>datalinkparms</i></p> <p>where <i>datalinkparms</i> are valid data link parameters.</p> <p>See the <i>IBM Director 4.20 Installation and Configuration Guide</i> for details of SSL setup and data link parameters.</p>

Examples

The following examples show how to use the DIRCMD options to:

- Pipe data from one command into another
- Override the default TCP/IP data link connection class

Piping data from one command into another: Use the pipe command to pipe data from one command into another. For example, type the following text at a command prompt:

```
dircmd -s IDWorld -u InfoDeveloper -p passwd server listgroupmembers -t 17D  
| dircmd -r -s IDWorld -u InfoDeveloper -p passwd 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 passwd. 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 (using the optional -r parameter) pipes the object IDs that are 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. For more information about the server-management and event-management bundle, see “Server-management bundle” on page 281 and “Event-management bundle” on page 292.

Overriding the default TCP/IP data link connection class: Use the -k command to override the default TCP/IP data link connection class. For example, type the following text at a command prompt:

```
dircmd -s IDWorld -u InfoDeveloper -p passwd -k com.tivoli.twg.libs.TWGSSLLink  
-o 2035 server AccessObjects myUser myPassw0rd 16B
```

In this example, an IBM Director super-user connects to IBM Director Server with the host name IDWorld, using the user ID InfoDeveloper and the password passwd, using the data link connection class com.tivoli.twg.libs.TWGSSLLink and secure socket port 2035. The user types the user ID myUser and the password myPassw0rd with the AccessObjects function of the server-management bundle to request access to the managed system with the object ID 16B using a secure connection between the DIRCMD client and IBM Director Server.

Exit codes

DIRCMD returns exit codes to indicate the status of the command. Table 24 contains information about the DIRCMD exit codes, their meanings and values.

Table 24. DIRCMD exit codes

Exit code	Meaning	Value
OK	Successful completion	0
USAGE	Errors due to missing or improper arguments	1
NOT_FOUND	Command or bundle not found	2
SECURITY_FAILURE	Security failure due to unauthorized client	3
COMMAND_EXCEPTION	Command implementation threw an exception	4
FAIL	General request of action failed	5

Note: Additional exit codes can be defined in specific bundle implementations for more specific conditions. Additional exit codes should have positive unique values.

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

Table 25 contains information about the syntax for invoking the server-management bundle.

Table 25. Server-management bundle syntax

Function	What it does	Command arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
DiscoverAll	Discovers all managed objects. This is equivalent to the Discover All Managed Systems function in IBM Director Console.	discoverall
ListObjects	Lists all objects (systems, SNMP devices, and others) managed by IBM Director.	listobjects [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> -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. -t, or -terse, displays the object ID. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the object ID and object name.
ListObjectAttributes	Lists the managed object attributes. Lists data that can be used as parameters for the ListObjectsByAttribute function.	listobjectattributes [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> -r, or -report, lists the name, data type, and value range for each managed object attribute. -t, or -terse, lists the name for each managed object attribute. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the name and type of each of the following attributes: name (String) By default, the attribute value is copied from the computer name in the operating system that is running on the managed system. You can edit and customize this value in IBM Director.

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<p>ListObjectAttributes (continued)</p>		<p>type (Integer) Reports the state of IBM Director Agent on the managed system.</p> <p>0 unknown 1 indeterminate 2 offline error 3 offline 4 online error 5 online</p> <p>hasLicense (Boolean) Indicates whether the managed system has an IBM Director license. This is equivalent to Granted License in the “Display System Attributes” window in IBM Director Console.</p> <p>securedsupport (Boolean) Indicates whether IBM Director can secure the system. A padlock icon is displayed next to secured managed systems in IBM Director Console.</p> <p>unsecureclient (Boolean) If unsecureclient is set to true, access is granted automatically upon discovery of the managed system. If it is set to false, you must type the password to access the system. This is equivalent to Agent Unsecured in the “Display System Attributes” window in IBM Director Console.</p> <p>accessdenied (Boolean) If unsecureclient is set to true for a discovered system, the accessdenied value for that system is set to false. This attribute is set to true on discovery of a secured managed system. If you provide a password and gain access to that system, accessdenied is set to false.</p> <p>encryptionenabled (Boolean) If encryptionenabled is set to true, the managed system is encryption-enabled. An encryption-enabled management server can connect to a nonencryption-enabled managed system. However, an encryption-enabled managed system cannot connect to a nonencryption-enabled management server.</p> <p>IPADDRS (TCP/IP address in xxx.xxx.xxx.xxx format) This attribute can store multiple IP addresses.</p> <p>IPHOSTS (String) This attribute can store multiple DNS host names, such as a system with four NICs.</p> <p>OPSYS (String) The operating system that is installed on the managed system.</p> <p>OPSYSMAJVER (Integer) The version of the operating system that is installed on the managed system. For example, the OpSysMajVer value for Red Hat Linux 7.3 is 7.</p>

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<p>ListObjectAttributes (continued)</p>		<p>OpSysMinVer (Integer) An incremental version number for the operating system. For example, the OpSysMinVer value for Red Hat Linux 7.3 is 3.</p> <p>AgentType (String) Indicates the IBM Director component that is installed on the managed system. The possible values are: Director_Server, Director_Agent, and Director_Console.</p> <p>AgentVer (String) The version of IBM Director that is installed on the managed system.</p> <p>UUID (Hexadecimal) The system identifier in the managed system BIOS.</p> <p>MACAddress (Hexadecimal) A deprecated MAC address attribute. This attribute is no longer used.</p> <p>MACAddrList (Hexadecimal) Stores the MAC address attribute of the NIC. If the managed system has multiple NICs, this attribute can store multiple MAC addresses.</p> <p>ComputerName (String) The computer name in the operating system that is installed on the managed system. IBM Director uses it as the default name attribute value.</p> <p>MachineTypeModel (String) Machine type and model combination.</p> <p>SerialNumber (String) Machine serial number.</p> <p>NativeMO.UniqueID (Hexadecimal) A value generated by IBM Director to identify the managed system.</p>
<p>ListObjectsByAttribute</p>	<p>Lists information about managed objects that meet the specified criteria.</p>	<p>listobjectsbyattribute [-r/-report/-t/-terse] {<i>attribute=value</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • -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. • -t, or -terse, displays the object ID. • <i>attribute</i> is the name of the managed-object attribute. • <i>value</i> is the value of the managed-object attribute. (The attribute value is case-sensitive.) <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the object name and object ID.</p> <p>Note: You can determine valid managed-object attributes and the range of possible values by using the ListObjectAttributes function.</p>

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
AccessObjects	Requests access to managed objects.	<p>accessobjects <i>userid password {systemID}</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>userid</i> is an IBM Director user ID that is authorized to access the managed object. • <i>password</i> is the password for the IBM Director user account that is authorized to access the managed object. • <i>systemID</i> is the unique object ID for the managed object.
PingObjects	Performs a presence check on the specified managed objects.	<p>pingobjects <i>{systemID}</i></p> <p>where <i>systemID</i> is the unique object ID for the managed object.</p>
DeleteObjects	Deletes the managed object from the IBM Director Server environment. This is equivalent to deleting a managed object from IBM Director Console.	<p>deleteobjects <i>{systemID}</i></p> <p>where <i>systemID</i> is the unique object ID for the managed object.</p>
RenameObject	Renames the managed object in the IBM Director Server environment. This is equivalent to the Rename function in IBM Director Console.	<p>renameobject <i>{NewName} {systemID}</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>NewName</i> is the new name of the managed object by which the object will be referred to in the IBM Director environment. • <i>systemID</i> is the unique object ID for the managed object.
ListGroups	<p>Lists the IBM Director groups. This is equivalent to viewing the Groups pane in IBM Director Console.</p> <p>For more information about groups, see “Groups” on page 34.</p>	<p>listgroups [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • -r, or -report, lists the group name, group ID, type (static or dynamic), and criteria for each group. • -t, or -terse, lists the group ID for each group. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the group name and group ID for each group. You can use a returned value from this function as input to the CreateDynamicGroup function.</p>
ListGroupAttributes	<p>Lists the attributes of the IBM Director groups.</p> <p>Lists data that can be used as parameters for the ListGroupByAttribute function.</p> <p>For more information about groups, see “Groups” on page 34.</p>	<p>listgroupattributes [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • -r, or -report, lists the name, data type, and value range for each attribute. • -t, or -terse, lists the name for each attribute. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the type and name for each attribute:</p> <p>name (String) The name of the group in IBM Director.</p>

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<p>ListGroupAttributes (continued)</p>		<p>type (Integer) The type of group.</p> <ul style="list-style-type: none"> 0 dynamic 1 static 2 managed-object class, such as a blade server or cluster 3 task <p>id (String) A group identifier. This attribute is set by IBM Director and is different from the hexadecimal group ID value. This attribute cannot be edited.</p> <p>readonly (Boolean) IBM Director sets this attribute when creating some groups during installation. This attribute cannot be edited.</p> <p>isdefault (Boolean) IBM Director sets this attribute to true when creating some groups by default. This attribute cannot be edited.</p> <p>isdeletable (Boolean) If isdeletable is set to false, the group cannot be deleted. This attribute is set to true for all groups that are created by a user or administrator. This attribute is set to false for some default groups. A user or administrator cannot edit this attribute.</p> <p>ishidden (Boolean) If ishidden is set to true, the group is hidden. This attribute is set to true for most default groups. A user or administrator cannot edit this attribute.</p>
<p>ListGroupsByAttribute</p>	<p>Lists the IBM Director groups that meet the specified criteria.</p> <p>For more information about groups, see “Groups” on page 34.</p>	<p>listgroupsbyattribute [-r/-report/-t/-terse] {<i>attribute=value</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • -r, or -report, lists the name, ID, type, and criteria for each group that meets the specified conditions. • -t, or -terse, lists the ID for each group that meets the conditions specified. • <i>attribute</i> is the name of the attribute. • <i>value</i> is the value of the attribute. <p>Do not include both the report and terse parameters in a command. 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>Note: You can determine valid group attributes and the range of possible values by using the ListGroupAttributes function.</p>

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<p>ListGroupMembers</p>	<p>Lists the members of specified groups. This is equivalent to viewing the Group Contents pane in IBM Director Console.</p> <p>Note: Managed objects are displayed only once, even if they are members of multiple specified groups.</p> <p>For more information about groups, see “Groups” on page 34.</p>	<p>listgroupmembers [-r/-report/-t/-terse] {<i>groupID</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • -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. • -t, or -terse, lists the object ID of the each member of the specified group. • <i>groupID</i> is the unique group ID. <p>Do not include both the report and terse parameters in a command. 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>
<p>ListDynamicGroupCriteria</p>	<p>Lists the criteria that are available for creating dynamic groups. The criteria are based on database inventory.</p> <p>For more information about dynamic groups, see “Dynamic groups” on page 34.</p>	<p>listdynamicgroupcriteria [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • -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. • -t or terse lists the identifier. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the identifier, database, table, and column. You can use the returned value of this function as input to the CreateDynamicGroup function.</p> <p>The identifiers are returned in the following format: <i>DatabaseToken.TableToken.ColumnToken.</i></p>
<p>ListInventoryValues</p>	<p>Lists the database inventory value for the specified identifiers.</p>	<p>listinventoryvalues [-r/-report/-t/-terse] {<i>identifier</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • -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. • -t, or -terse, displays the identifier and inventory value. • <i>identifier</i> is the unique inventory identifier. It must be in the form <i>DatabaseToken.TableToken.ColumnToken</i> <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the identifier, database, table, column, and the inventory value.</p>

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
<p>CreateDynamicGroup</p>	<p>Creates a dynamic group. This is equivalent to creating a dynamic group in IBM Director Console.</p> <p>For more information about dynamic groups, see “Dynamic groups” on page 34.</p> <p>Use the ListInventoryValues and ListDynamicGroupCriteria commands to provide the input values for this function.</p>	<p>createdynamicgroup [-f] <i>groupname groupcriteria</i></p> <p>where:</p> <ul style="list-style-type: none"> • -f forces an equality relationship with a value that cannot be verified with the current database. • <i>groupname</i> is the name of the dynamic group. • <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"> – <i>identifier "symbol " value</i> – {<i>identifier "symbol " value relationship identifier "symbol " value</i>} <p>where:</p> <ul style="list-style-type: none"> – <i>identifier</i> is the unique inventory identifier. It must be in the following form: <i>DatabaseToken.TableToken.ColumnToken</i>. – <i>symbol</i> is one of the following symbols: =, !=, <, <=, >, >=. – <i>value</i> is an inventory value of the same type as the unique inventory identifier. It must be an existing inventory data, or, if the optional -f command is issued, an unknown value can be used. – <i>relationship</i> is one of the following parameters: <ul style="list-style-type: none"> - AND (all true) - OR (any true) - ALL (all true for the same row) - EACH (at least one true)
<p>CreateStaticGroup</p>	<p>Creates a new static group. This is equivalent to creating a static group in IBM Director Console.</p> <p>For more information about static groups, see “Static groups” on page 36.</p>	<p>createstaticgroup <i>staticgroupname</i></p> <p>where <i>staticgroupname</i> is the name of the new static group.</p>

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
AddToStaticGroup	<p>Adds one or more managed objects to a static group. This is equivalent to adding managed objects to a static group in IBM Director Console.</p> <p>Use the ListGroups function to determine valid staticgroupIDs. Use the ListObjects function to determine valid systemIDs.</p> <p>For more information about static groups, see “Static groups” on page 36.</p>	<p>addstaticgroup <i>staticgroupID</i> {<i>systemID</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>staticgroupID</i> is the object ID of the static group. • <i>systemID</i> is the unique object ID of the managed object.
RemoveFromStaticGroup	<p>Removes one or more managed objects from a static group. This is equivalent to removing a static group in IBM Director Console.</p> <p>For more information about static groups, see “Static groups” on page 36.</p>	<p>removefromstaticgroup <i>staticgroupID</i> {<i>systemID</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>staticgroupID</i> is the object ID of the static group. • <i>systemID</i> is the unique object ID of the managed object.
DeleteGroups	<p>Deletes one or more groups from the IBM Director environment. This is equivalent to deleting a group in IBM Director Console.</p> <p>For more information about groups, see “Groups” on page 34.</p>	<p>deletegroups {<i>groupID</i>}</p> <p>where <i>groupID</i> is the unique group ID.</p>
ListNoninteractiveTasks	<p>Returns a list of noninteractive tasks. The list includes the job name, the task category (if known), and the job ID.</p>	<p>listnoninteractivetasks</p>
RunTask	<p>Immediately runs a noninteractive task against one or more managed objects.</p> <p>Use the ListNoninteractiveTasks function to determine valid job IDs.</p>	<p>runtask <i>jobID</i> {<i>systemID</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>jobID</i> is the job ID. • <i>systemID</i> is the unique object ID of the managed object. You can specify one or more objects by separating object IDs with a space. <p>The returned value is the TWGJob activation ID. Use this value as input for the ListTaskActivationStatus function.</p>

Table 25. Server-management bundle syntax (continued)

Function	What it does	Command arguments
ListTaskActivationStatus	<p>Returns the activation and execution status of noninteractive IBM Director tasks. You must have started these tasks using the RunTask function in the server-management bundle.</p> <p>Use the ListNoninteractiveTasks function to determine valid job IDs.</p>	<p>listtaskactivationstatus <i>jobID activationID</i> [<i>systemID(1)</i>]...[<i>systemID(N)</i>]</p> <p>where:</p> <ul style="list-style-type: none"> • <i>jobID</i> is the job ID of the task. This value is returned by the function ListNoninteractiveTasks and is a command argument for the function RunTask. • <i>activationID</i> is the TWGJob activation ID that is returned by the RunTask function. This value is required. • <i>systemID</i> is the unique object ID of the managed object. You can specify one or more objects by separating object IDs with a space. This function returns the status for each specified object. <p>If you specify only one object, the returned value is the status of the specified object execution. If you do not specify a object, the output for this function is:</p> <ul style="list-style-type: none"> • The overall execution status • The execution status of each target for which you ran the RunTask function

Examples

The following examples show how to use server-management bundle functions to:

- List managed objects
- List managed objects attributes
- Delete groups
- Run noninteractive tasks
- Create a dynamic group

Listing managed objects: In the following 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. When the user invokes the ListObjects function of the server bundle, the following command returns a list of all managed objects.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd server listobjects
```

Listing managed objects attributes: In the following example, the user invokes the ListObjectsByAttribute function to generate an expanded list of all managed objects running IBM Director Agent 4.20.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd server listobjectsbyattribute -r AgentVer=4.20
```

In this example, the user invokes the ListObjectsByAttribute function to list all managed systems that are installed with IBM Director Server.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd server listobjectsbyattribute AgentType=Director_Server
```

Deleting groups: In the following example, the user invokes the ListGroups function to generate a list of group IDs (a hexadecimal value) and group names. Two groups might have identical names, but the group ID is unique to each group.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd server listgroups
```

Next, the user invokes the DeleteGroups function to delete the group with group ID 24D.

```
dircmd -s IDWorld -u InfoDeveloper -p password server deletegroups 24D
```

In this example, the user invokes the DeleteGroups function to delete the groups with group IDs 24D, 256, 1E9.

```
dircmd -s IDWorld -u InfoDeveloper -p password server deletegroups 24D 256 1E9
```

Running noninteractive tasks: In the following example, the user runs noninteractive tasks on managed systems:

1. Invoke the ListNonInteractiveTasks function to generate a list of the activation and execution status of noninteractive tasks for all managed systems.

```
dircmd -s IDWorld -u InfoDeveloper -p password server listnoninteractivetasks
```

The returned list of noninteractive tasks includes the following task:

```
job-id=10 [Miscellaneous System Tasks][Power Down]
```

2. Invoke the RunTask function using job ID 10 to run a noninteractive task on the server with system ID 230.

```
dircmd -s IDworld -u InfoDeveloper -p password server runtask 10 230
```

The function returns the activation ID 3.

3. Invoke the ListTaskActivationStatus function to determine the status of noninteractive tasks with job ID 10 and activation ID 3 running on any system.

```
dircmd -s IDworld -u InfoDeveloper -p password server listtaskactivationstatus 10 3
```

The function returns the status of each task and a summary status.

4. Invoke the ListTaskActivationStatus function to determine the status of noninteractive tasks with job ID 10 and activation ID 3 running on the servers with system IDs 230, 234, and 241.

```
dircmd -s IDworld -u InfoDeveloper -p password server listtaskactivationstatus 10 3 230 234 241
```

The function returns the status of each task for each server.

Creating a dynamic group: In this example, the user creates a dynamic group to sort managed objects by microprocessor speed:

1. Invoke the ListDynamicGroupCriteria function to list the attributes of the managed systems in the dynamic group. Then, pipe the attributes to the grep program, which searches for and lists identifiers that contain the word *speed*.

```
dircmd -s IDworld -u InfoDeveloper -p password server listdynamicgroupcriteria | grep -i "speed"
```

2. Invoke the ListInventoryValues function to list current inventory values for the identifier PC_INV.TWG_PROCESSOR.CURRENT_SPEED. This step is similar to using the “Dynamic Group Editor” window in IBM Director Console where the user expands the tree by clicking **Inventory (PC) → Processor → Current Speed Of Processor (MHz)** to view a list of inventory values that can be used to create the group.

```
dircmd -s IDworld -u InfoDeveloper -p password server listinventoryvalues PC_INV.TWG_PROCESSOR.CURRENT_SPEED
```

The output for this command is 733, 2200, 2400.

3. Invoke the CreateDynamicGroup function to create a dynamic group called Fast Servers consisting of managed systems with a microprocessor speed greater than 2200 MHz.

Note: If an argument contains the greater-than symbol, you must enclose it in quotation marks. Otherwise, DIRCMD will interpret the greater-than symbol as a redirect command.

```
dircmd -s IDworld -u InfoDeveloper -p password server createdynamicgroup
"Fast Servers" "PC_INV.TWG_PROCESSOR.CURRENT_SPEED>2200"
```

4. Invoke the CreateDynamicGroup function to create a dynamic group called Slow Servers consisting of managed systems with a microprocessor speed less than 1000 MHz. The inventory list that is returned in step 2 on page 290 does not include the value 1000. DIRCMD provides the force option (-f) to force a value that is not in the inventory. IBM Director Console does not have an equivalent to the force option.

```
dircmd -s IDworld -u InfoDeveloper -p password server createdynamicgroup
-f "Slow Servers" "PC_INV.TWG_PROCESSOR.CURRENT_SPEED=1000"
```

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 to the management server.

Note: All managed-system functions must be preceded by the **native** command.

Syntax

Table 26 contains information about the syntax for invoking the managed-system bundle.

Table 26. Managed-system bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
StartDiscovery	Discovers managed systems.	startdiscovery
ListSystems	Lists all managed systems.	listsystems [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> • -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. • -t, or -terse, displays the object ID of each managed system. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the system name and object ID for each managed system.
AddSystem	Creates a managed-system object on the management server. This is equivalent to right-clicking the Group Contents pane of IBM Director Console and then clicking New → IBM Director Systems .	addsystem <i>systemname protocol netaddress</i> where: <ul style="list-style-type: none"> • <i>systemname</i> is the name of the new managed system. • <i>protocol</i> is the network protocol. • <i>netaddress</i> is a DNS resolvable host name or a TCP/IP address.

Examples

In the following 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.

When the user invokes the ListSystems function of the managed-system bundle, the following command returns a list of all managed systems.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd native listsystems
```

In the following example, the user from the previous example invokes the AddSystem function to add a managed-system object to the IBM Director environment. The new managed system is displayed in IBM Director Console as TechWriter2 with TCP/IP as the network protocol and has an IP address of 160.0.0.27.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd native addsystem TechWriter2  
TCPIP 160.0.0.27
```

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

Table 27 contains information about the syntax for invoking the event-management bundle.

Table 27. Event-management bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
ListFilters	Lists all event filters.	listfilters [-r/-report/-t/-terse] where: <ul style="list-style-type: none">• -r, or -report, lists the names, keys, and read-only Boolean status of the event filters.• -t, or -terse, displays the names of the event filters. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the keys and names of the event filters.
ListEventTypes	Lists the published event list.	listeventtypes

Table 27. Event-management bundle syntax (continued)

Function	What it does	Arguments
ListEvents	<p>Lists the contents of the event log.</p> <p>Use the ListFilters function to determine valid filter names. Use the ListObjectsfunction to determine valid system IDs.</p>	<p>listevents [-r/-report/-t/-terse] [-f <i>filtername</i>] [-h <i>hours</i>] [{<i>systemID</i>}]</p> <p>where:</p> <ul style="list-style-type: none"> • -r, or -report, lists event type, event date and time, event system, severity, category, sending system, and associated text description. • -t, or -terse, lists the event and system. • <i>filtername</i> is a specific event filter. • <i>hours</i> specifies a time frame for the events. • <i>systemID</i> is the unique system ID for the managed object. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the event type, event date and time, event system, severity, and category.</p> <p>Issuing this function without arguments will generate a list of <i>all</i> managed system events that occurred during the preceding 24 hours.</p>
ListEventActions	<p>Lists all event actions.</p>	<p>listeventactions [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • -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. • -t, or -terse lists the event action names. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the names and keys of the event actions.</p>
ListEventActionPlans	<p>Lists all event action plans.</p>	<p>listeventactionplans [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • -r, or -report, lists the name, key, and read-only value of the event action plan. • -t, or -terse, lists the name of the event action plan. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the name and key of the event action plan.</p>
CreateEventActionPlan	<p>Creates an event action plan.</p> <p>Use the ListFilters function to determine valid filter names. Use the ListEventActions function to determine valid action names.</p>	<p>createeventactionplan <i>planname</i> {-f {<i>filtername</i>} {<i>actionname</i>} }</p> <p>where:</p> <ul style="list-style-type: none"> • <i>planname</i> is the unique event action plan name. It is user-chosen. • <i>filtername</i> is an event filter. • <i>actionname</i> specifies the action plan name.

Table 27. Event-management bundle syntax (continued)

Function	What it does	Arguments
ApplyEventActionPlan	Applies an event action plan to a managed object or group.	<code>applyeventactionplan <i>planname</i> [-s {<i>systemID</i>} -g {<i>groupID</i>}]</code> where: <ul style="list-style-type: none"> • <i>planname</i> is an event action plan name. • <i>systemID</i> is an object ID • <i>groupID</i> is a group ID.

Examples

In the following 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. When the user invokes the ListEvents function of the events-management bundle, the following command returns a list of all fatal events that occurred in the previous 8 hours.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd event listevents -f "Fatal Events" -h 8
```

In the following example, the user from the previous example invokes the ListEventTypes function in combination with a grep command to list all IBM Director event types that are associated with security.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd event listeventtypes | grep -i "security"
```

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

Table 28 contains information about invoking the resource-monitor bundle.

Table 28. Resource-monitor bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
ListThresholds	Lists all the resource-monitor threshold tasks.	<code>listthresholds [-r/-report/-t/-terse]</code> where: <ul style="list-style-type: none"> • -r, or -report, displays the name and object ID of the threshold tasks in a tabular report form. • -t, or -terse, lists the object ID for the threshold tasks. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the threshold name and task object ID.

Table 28. Resource-monitor bundle syntax (continued)

Function	What it does	Arguments
ApplyThreshold	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"> • <i>taskID</i> is the object ID of the resource-monitor threshold task. • <i>systemID</i> is the object ID of the managed object. • <i>groupID</i> is object ID of the group.

Examples

In the following 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. When the user invokes the ListThresholds function, the following command lists all previously-created threshold tasks.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd monitor listthresholds -r
```

In the following example, the user from the previous example invokes the ApplyThreshold function to apply the threshold task that is associated with OID 196 ("CPU utilization," in this case) to group 191 ("Systems with Windows 2000," in this case).

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd monitor applythreshold 196 -g 191
```

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 to create and apply a process-monitor task.

All process-monitor functions must be preceded by the **procmon** command.

Syntax

Table 29 contains information about the syntax of the process-monitor bundle.

Table 29. Process-monitor bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
ListPMtasks	Lists all the process-monitor tasks.	listpmtasks [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> • -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. • -t, or -terse, lists the object ID of the process monitor task. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the name and object ID of the process monitor task.

Table 29. Process-monitor bundle syntax (continued)

Function	What it does	Arguments
CreatePMTask	Creates a process-monitor task for a program.	createpmtask <i>taskname</i> { <i>programname</i> [+S][+E][+Fn] } where: <ul style="list-style-type: none"> • <i>taskname</i> specifies a name for the task. • <i>programname</i> specifies the path and name of the application, for example, c:\windows\notepad.exe. • +S generates an event when the program begins. • +E generates an event when the program ends. • +Fn generates an event when the program does not start correctly or fails after <i>n</i> seconds.
ApplyPMTask	Applies a process-monitor task to a managed system. Use the ListPMTasks function to determine valid taskIDs. Use the ListObjects function to determine valid systemIDs.	applypmtask <i>taskID</i> { <i>systemID</i> } where: <ul style="list-style-type: none"> • <i>taskID</i> is the object ID of the process-monitor task. • <i>systemID</i> is the object ID for the managed system.

Examples

In the following 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. When the user invokes the CreatePMTask function, the following 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.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd procmon createPMTask
"Notepad monitor" c:\winnt\notepad.exe+s+f5
```

In the following example, the user from the previous example invokes the ListPMTasks function to list all process-monitor tasks.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd procmon listPMTasks
```

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

Table 30 contains information about the syntax for invoking the SNMP-device bundle.

Table 30. SNMP-device bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
StartDiscovery	Discovers all SNMP devices.	startdiscovery

Table 30. SNMP-device bundle syntax (continued)

Function	What it does	Arguments
ListSystems	Lists all SNMP devices.	<p>listsystems [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • -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. • -t, or -terse, displays the object ID of each SNMP device. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, the function returns the object ID and system name for each SNMP device.</p>
AddSystem	<p>Creates an SNMP device on the management server.</p> <p>This is equivalent to right-clicking the Group Contents pane in IBM Director Console and then clicking New → SNMP Devices.</p>	<p>addsystem <i>IPAddress</i> <i>version</i> [<i>communityname</i> <i>profilename</i>] <i>seed</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>IPAddress</i> is the IP address of the SNMP device. • <i>version</i> is the version of SNMP to use. Valid values are 1, 2, and 3. • <i>communityname</i> is the SNMPv1 or SNMPv2 community name of the SNMP device. • <i>profilename</i> is the SNMPv3 profile name of the SNMP device. • <i>seed</i> is one of the following parameters: <ul style="list-style-type: none"> – true if you want the SNMP device to be a seed for SNMP discovery. – false if you do not want the SNMP device to be a seed for SNMP discovery.
Get	Performs an SNMP Get request against the SNMP device.	<p>get <i>systemOID</i> {<i>objectIdentifier</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>systemOID</i> is the managed object ID of the SNMP device. • <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.1.0 for sysDescr.
GetNext	Performs an SNMP Get Next request against the SNMP device.	<p>getnext <i>systemOID</i> {<i>objectIdentifier</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>systemOID</i> is the managed object ID of the SNMP device. • <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.1.0 for sysDescr.

Table 30. SNMP-device bundle syntax (continued)

Function	What it does	Arguments
Set	Performs an SNMP Set request against the SNMP device.	<p>set <i>systemOID</i> {<i>objectIdentifier</i> <i>type</i> <i>value</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>systemOID</i> is the managed object ID of the SNMP device. • <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact. • <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. • <i>value</i> is the value to which you want to set the object identifier, for example, administrator.
GetBulk	Performs an SNMP Get Bulk request against the SNMP device.	<p>getbulk <i>max non-repeaters systemOID</i> {<i>objectIdentifier</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>max</i> is the maximum number of repetitions. • <i>non-repeaters</i> is the number of nonrepeaters. • <i>systemOID</i> is the managed object ID of the SNMP device. • <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.1.0 for sysDescr.
Inform	Performs an SNMP Inform request against the SNMP device.	<p>inform <i>systemOID</i> {<i>objectIdentifier</i> <i>type</i> <i>value</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>systemOID</i> is the managed object ID of the SNMP device. • <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact. • <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. • <i>value</i> is the value of the object identifier.
Trap 1	Sends an SNMPv1 trap to the SNMP device.	<p>trap 1 <i>systemOID uptime IPAddress type enterpriseOID</i> {<i>objectIdentifier</i> <i>type</i> <i>value</i>}</p> <p>where:</p> <ul style="list-style-type: none"> • <i>systemOID</i> is the managed object ID of the SNMP device. • <i>uptime</i> is the system uptime of the trap sender. • <i>IPAddress</i> is the IP address of the trap destination. • <i>type</i> is the type of the trap being sent. It is one of the following values: <ul style="list-style-type: none"> – 0 = coldStart – 1 = warmStart – 2 = linkDown – 3 = linkUp – 4 = authenticationFailure – 5 = egpNeighborLoss – 6 = <i>specificNumber</i>, where <i>specificNumber</i> is the specific number for the trap.

Table 30. SNMP-device bundle syntax (continued)

Function	What it does	Arguments
Trap 1 (continued)		<ul style="list-style-type: none"> • <i>enterpriseOID</i> is the enterprise object ID of the trap. • <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact. • <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. • <i>value</i> is the value of the object identifier.
Trap 2	Sends an SNMPv2 trap to the SNMP device.	trap 2 <i>systemOID</i> { <i>objectIdentifier</i> <i>type</i> <i>value</i> } where: <ul style="list-style-type: none"> • <i>systemOID</i> is the managed object ID of the SNMP device. • <i>objectIdentifier</i> is an object identifier, for example, 1.3.6.1.2.1.1.4.0 for sysContact. • <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. • <i>value</i> is the value of the object identifier.
Walk	Performs an SNMP walk on a branch of the MIB tree of the SNMP device.	walk <i>systemOID</i> <i>oid</i> where: <ul style="list-style-type: none"> • <i>systemOID</i> is the managed object ID of the SNMP device. • <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.

Examples

In the following 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. When the user invokes the StartDiscovery function, the following command discovers SNMP devices.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd snmp startdiscovery
```

In this example, the user invokes the ListSystems function. Issuing this command lists all discovered SNMP devices.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd snmp listsystems
```

In this example, the user invokes the Get function to request an SNMP sysDescr (1.3.6.1.2.1.1.0) request from object 21B.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd snmp get 21B 1.3.6.1.2.1.1.0
```

The output from this command is similar to the following output: 1.34.6.1.2.1.1.0 ,octets. = Hardware: x86 Family 15 model 1 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Multiprocessor Free)

Management Processor Assistant bundle

The following information explains how to use the Management Processor Assistant (MPA) bundle, which provides general access to Management Processor Assistant objects. You can invoke the Management Processor Assistant bundle to list managed objects, list attributes of managed objects, and list managed-object attribute values.

All Management Processor Assistant functions must be preceded by the **MPA** command.

Syntax

Table 31 contains information about the syntax for invoking the Management Processor Assistant bundle.

Table 31. Management Processor Assistant bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
ListObjectAttributes	Lists the managed-object attributes. Lists data that can be used as parameters for the ListObjectsByAttribute function.	listobjectattributes [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> • -r, or -report, lists the name, data type, and value range for each managed-object attribute. • -t, or -terse, lists the name for each managed object attribute. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the name and type of the following attribute: name (String) By default, the attribute value is copied from the computer name in the operating system that is running on the managed system. You can edit and customize this value in IBM Director.
ListObjectsByAttribute	Lists information about managed objects that meet the specified criteria.	listobjectsbyattribute [-t/-terse] {attribute=value} where: <ul style="list-style-type: none"> • -t, or -terse, displays the object ID. • <i>attribute</i> is the name of the managed-object attribute. • <i>value</i> is the value of the managed-object attribute. (The attribute value is case-sensitive.) If you do not issue the terse parameter, this function returns the object name and object ID. Note: You can determine valid managed-object attributes and the range of possible values by using the ListObjectAttributes function.

Table 31. Management Processor Assistant bundle syntax (continued)

Function	What it does	Arguments
ListObjectAttributeValues	Lists the current values of the following attributes of a specified managed system: <ul style="list-style-type: none"> • textID • assetTag • lastConnectionStatus • promptAccess • compEvents • assetType 	listobjectattributevalues { <i>systemID</i> } where <i>systemID</i> is the unique object ID for the managed system.
SetCredentials	Specifies the user ID and password for communicating with a service processor.	setcredentials -u <i>userID</i> -p <i>password</i> <i>systemOID</i> { <i>systemOID</i> } where: <ul style="list-style-type: none"> • <i>userID</i> is the userID IBM Director stores in its database to communicate with the service processor. • <i>password</i> is the password IBM Director stores in its database to communicate with the service processor. • <i>systemOID</i> is the managed object ID that contains the service processor. You must specify at least one systemOID. You can specify additional systemOIDs by separating systemOIDs with a space.

Examples

In the following 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. When the user invokes the ListObjectAttributeValues function, the following command returns the current values of MPA-related attributes for the managed system with the object ID 16B.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd mpa listobjectsbyattribute 16B
```

In the following example, the user sets the user ID madison and the password lucas to access the service processors contained in the managed objects with the object IDs 1F0, 1F1, and 1F2.

```
dircmd -s IDWorld -u InfoDeveloper -p passw0rd mpa setcredentials -u madison -p lucas 1F0 1F1 1F2 1F3
```

BladeCenter-configuration bundle

The following information explains how to use the BladeCenter-configuration bundle.

All BladeCenter-configuration functions must be preceded by the **bladecenterconfiguration** command.

Syntax

Table 32 on page 302 contains information about the syntax for invoking the BladeCenter-configuration bundle.

Table 32. BladeCenter-configuration bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
xmlfile	Creates a BladeCenter Deployment wizard profile.	-f <i>filename</i> bladecenterconfiguration xmlfile where <i>filename</i> is the path and name of an XML file that contains BladeCenter chassis configuration information. The content of the profileName element must not be the name of an existing BladeCenter Deployment wizard profile.

Example

In the following 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. When the user invokes the xmlfile function, the following command creates a BladeCenter Deployment wizard profile that has the name specified in the IDchassis.xml file.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd -f IDchassis.xml
bladecenterconfiguration xmlfile
```

Then, the user can run the profile by issuing the server-management bundle runtask command.

BladeCenter-chassis bundle

The following information explains how to use the BladeCenter-chassis bundle.

All BladeCenter-chassis functions must be preceded by the **bladecenterchassis** command.

Syntax

Table 33 contains information about the syntax for invoking the BladeCenter-chassis bundle.

Table 33. BladeCenter-chassis bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list
ListBCChassis	List all BladeCenter chassis managed objects.	listbcchassis [-r/-report/-t/-terse] where: <ul style="list-style-type: none"> • -r, or -report, lists the object ID and object name. • -t, or -terse, displays the object ID. Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the object ID and object name.

Table 33. BladeCenter-chassis bundle syntax (continued)

Function	What it does	Arguments
AddBCChassis	Add a BladeCenter chassis managed object.	addbccchassis <i>chassisname netaddress userid password</i> where: <ul style="list-style-type: none"> • <i>chassisname</i> is the name of the new BladeCenter chassis. • <i>netaddress</i> is a TCP/IP address. • <i>userid</i> is an IBM Director user ID that is authorized to access the managed object. • <i>password</i> is the password for the IBM Director user account that is authorized to access the managed object.
DiscoverBCChassis	Start a BladeCenter chassis discovery.	discoverbccchassis

Examples

In the following 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. When the user invokes the list function, the following command returns the list of commands in the BladeCenter-chassis bundle.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd bladecenterchassis list
```

When the user invokes the DiscoverBCChassis function, the following command starts the BladeCenter discovery.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd bladecenterchassis discoverbladecenterchassis
```

Chassis bundle

The following information explains how to use the Chassis bundle.

All Chassis functions must be preceded by the **chassis** command.

Syntax

Table 34 contains information about the syntax for invoking the Chassis bundle.

Table 34. Chassis bundle syntax

Function	What it does	Arguments
Help	Lists an overview of the bundle usage.	help
List	Lists the function set for the bundle.	list

Table 34. Chassis bundle syntax (continued)

Function	What it does	Arguments
ChassisList	Lists all chassis managed objects.	<p>chassislist [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • -r, or -report, lists the object ID and object name. • -t, or -terse, displays the object ID. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the object ID and object name.</p>
ChassisSubsystemTypeList	Lists supported subsystem types of a chassis managed object.	chassis subsystemtypelist
ChassisSubsystemList	List subsystems present on a chassis managed object.	<p>chassis subsystemlist <i>chassisOID</i> [-r/-report/-t/-terse]</p> <p>where:</p> <ul style="list-style-type: none"> • <i>chassisOID</i> is the managed object ID of the chassis. • -r, or -report, lists the object ID and object name. • -t, or -terse, displays the object ID. <p>Do not include both the report and terse parameters in a command. If you do not issue the report or terse parameter, this function returns the object ID and object name.</p>

Example

In the following 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. When the user invokes the help function, the following command returns the help message for the Chassis bundle.

```
dircmd -s IDworld -u InfoDeveloper -p passw0rd chassis help
```

Chapter 31. 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.

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 4.7x and 7.01 or later

Notes:

1. Your Web browser must support Java™ applets.
2. For Internet Explorer to work correctly with Web-based Access, you must use 56-bit encryption or higher.
3. A message is displayed about requiring the Java Virtual Machine (JVM). Web-based Access must have the JVM installed to function correctly. If you have a copy of the Microsoft JVM, install it; otherwise, download and install the JVM from <http://java.sun.com>.
4. Systems using a Web browser or Microsoft Management Console (MMC) to access a managed system require 64 megabytes (MB) of random access memory (RAM) to function correctly.

If the system from which you want to use Web-based Access is running Windows 2000, Windows 2003, or Windows XP, you can use the Microsoft Management Console (MMC), version 1.1 or later.

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 4.20 Upward Integration Module Installation Guide*.

Starting Web-based Access

You can start Web-based Access using either a Web browser or 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 used 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.

Note: (Windows NT 4.0 only) If your password consists of all blank characters, Web-based Access authenticates a password consisting of text also.

3. (Optional) To view a remote system, type the following address 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 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 used 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 you are accessing a Secure Sockets Layer (SSL) Web site for the first time. IBM Director Agent uses SSL to encrypt the data stream between the system running Web-based Access 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 that 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 ignore the security alert message.
7. In the “IBM Director Agent User ID and Password” window, type the operating-system user name and password that are associated with the targeted managed system.

If the managed system is a member of a domain, it is accessible using domain accounts. You can type your user name using either of the following formats:

- `domain_name\user_name`
- `user_name@domain_name`

where *domain_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 that you use to log in. If the user account is a member of the local Administrators group of the system, you have full access by default. If the user account is a member of the local Users group of the system, you have read access. Otherwise, access is denied. You can configure this access policy using applicable Windows administration tools.

A message stating that the Web browser requires Java support might be displayed.

A message stating that the Web browser requires the Java Foundation Class/Swing library (JFC/Swing) might be displayed. IBM provides 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. When the installation is complete, the “Download” window closes.
- e. Double-click the downloaded file to run the installer.
- f. (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.

Notes:

- a. (Windows XP and Windows Server 2003 only) The operating system is configured by default to deny network access to user accounts with blank passwords. You cannot access the managed system that is running Windows XP or Windows Server 2003 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 that you want to access remotely.
- b. The default Guest user account on Windows systems cannot log on to a managed system using Web-based Access. Use an account with user privileges on the local system to log on to a managed system using Web-based Access.

Depending on your user account system access, you gain read/write or read-only access to IBM Director Agent 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 are 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 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 used 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.

Note: (Windows NT 4.0 only) If your password consists of all blank characters, Web-based Access authenticates a password consisting of text also.

The Web-based Access interface

When Web-based Access has connected to a managed system, the Web-based Access program opens in your Web browser or MMC. Two panes are displayed.

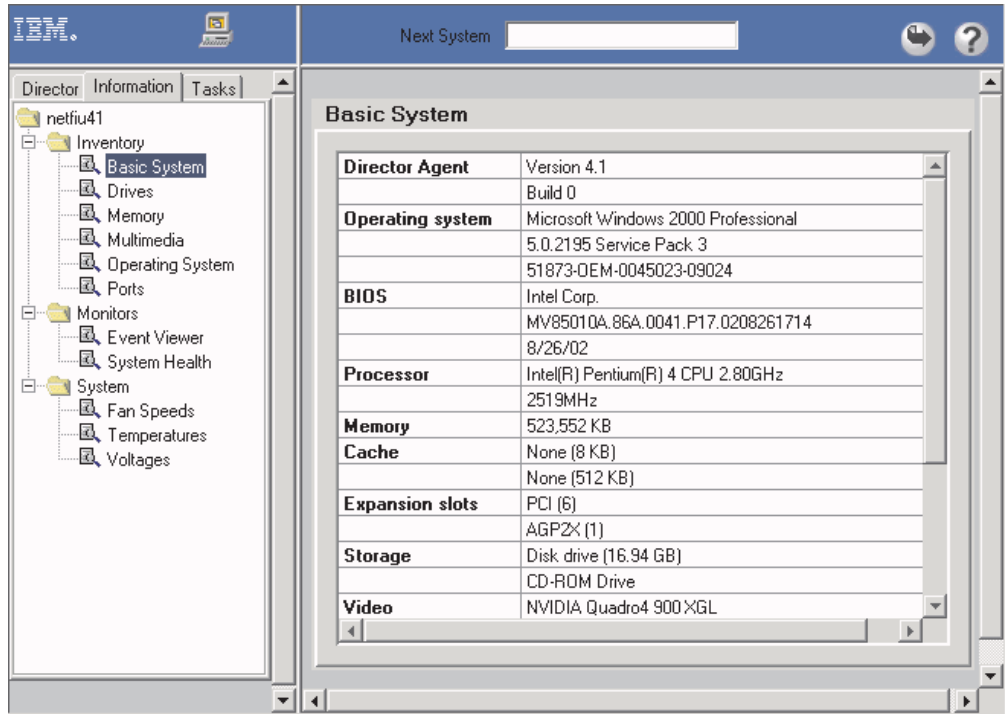


Figure 145. Web-based Access

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” on page 309.

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” on page 310.

Tasks


An expandable tree view of IBM Director Agent services that perform systems-management and system-configuration tasks on the managed system. See “Working with managed systems” on page 320.

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**.

Note: (Windows Server 2003 and Microsoft Internet Explorer only) Exporting data from a task is not supported when the Microsoft Internet Explorer Enhanced Security Configuration is enabled.

The Web-based Access online help provides definitions for the information tables and services.

Viewing hardware status

The Hardware Status service is available from the Director page when you view a management server.

Note: If you enable SSL, you cannot use Web-based Access to view hardware status information for the management server.



Figure 146. 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.

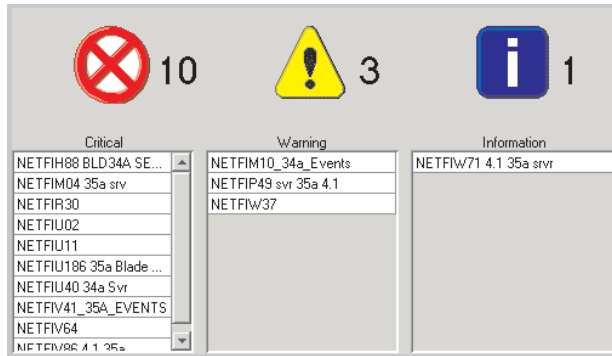





Figure 147. Hardware Status pane

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 that is being monitored, or double-click a listed system to receive data that is specific to that system.

Hardware Status monitors systems for changes in the following environments:

- Generic
- Component
- Device
- Network
- Environmental
- Security
- Other

Viewing managed-system information

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 313.

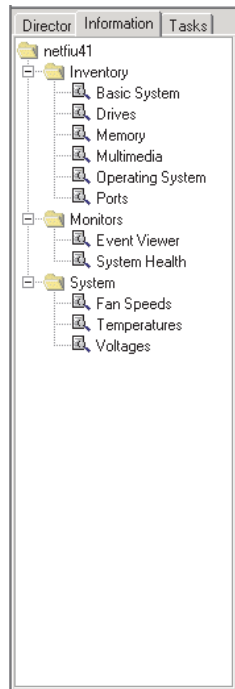


Figure 148. Information page in the left pane

The Information page might contain the following types of services:

- Inventory (see page 311)
- Monitor (see page 315)
- System (see page 318)

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 that 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 that are 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
- (Systems with a Remote Supervisor Adapter only) System board, power supplies, and PCI adapters. The availability of this information varies by the model type of the system.
- (Systems with a ServeRAID-4 adapter or later installed with ServeRAID firmware version 4.84 or later only) RAID physical drives and trays. 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 359.

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 about memory configuration is displayed.

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, if you have a system with four DIMM sockets that are currently filled with 128 MB DIMMs and 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 three DIMMs of different size, even if 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 that is 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.

Table 35 shows details that are available on the Drivers page.

Table 35. Device driver details

Item	Description
Name	The name of each device driver in the operating-system directory.
Start Mode	<p>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.</p> <p>Disabled The device driver is not added to the operating environment.</p> <p>Auto The device driver is started automatically when the operating system is started.</p> <p>Boot The device driver is initialized during the operating-system startup (boot) sequence.</p> <p>Manual The device driver is started by the user.</p> <p>System The device driver is started by the lnlInitSystem method.</p>
State	The current run state of each device driver (Running or Stopped).
Command line	The complete path to the device driver, such as c:\SystemRoot\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 that are available on this page are the same as what is 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 and contents of the Windows event log on the managed system. The following Monitor services are available:

- Event Viewer (see page 315)
- System Health (see page 316)

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 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 that 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 that you want to display. The following event-log categories are available:

Application

(Default) Displays the 30 most recent log entries that result from 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 applicable 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.

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.

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 generated output, you must use the Health service from the Tasks page. See “Health” on page 322 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. It indicates a Predictive Failure Analysis® (PFA) event from a DIMM.

Processor PFA

This is available on some servers. It indicates a Predictive Failure Analysis event from a microprocessor.

LAN Leash

This detects whether 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

If operational thresholds on the hard disk drive are exceeded, Predictive Failure Analysis events are generated. This information can be generated only for Self-Monitoring, Analysis, and Reporting Technology (SMART) drives.

Power Supply Failure

If the system power supply fails, a Critical system-health event is generated.

Redundant NIC

(Windows only) If a system has multiple network interface cards (NICs) that are configured for automatic failover and a failover or switchback event occurs, a Warning system-health event is generated.

NIC Failure

(Windows only) If a system NIC fails, a Critical system-health event is generated.

NIC Offline

(Windows only) If a system NIC is offline, a Warning system-health event is generated.

NIC Online

(Windows only) If a system NIC is online an Informational system-health event is generated.

System services

On a system that has 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, only one of the processors provides information to the System service, as follows:

- 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 system 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 that is 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 316 for more information).

The Mgmt Proc (Management Processor) Event Log service is available for Intelligent Platform Management Interface (IPMI)-based systems.

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 that are currently stored in the systems-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 they are noted as Error or Warning events.

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 power-on self test (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 that are 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 that are 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 that are 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

You 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.

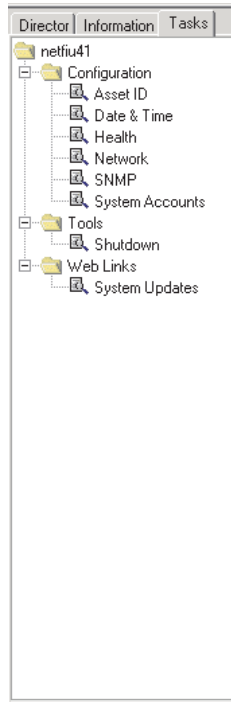


Figure 149. Task services in the left pane

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 320)
- Tools (see page 324)
- Web Links (see page 324)

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 that is 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 that 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 that 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.

Although the fields on these pages are labeled for specific information, you do not have to provide the specific information that is indicated by each label. The labels are suggestions for information that you can provide.

The Serialization page is displayed by default. The information that is 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 that is displayed includes the system name, message authentication code (MAC) address, login name (" " indicates that 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.

When you click the **Personalization** tab, a free-form window opens 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 available data space in a managed system that does not have EEPROM. You cannot type 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 the system, including duration (in months), cost, and end date. You can use the specified end date as a source for an alert. If the warranty duration expires, you can select 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 that is remaining on the managed system hard disk drives, for temperature, and to enable and disable event bindings for various event consumers.

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 that is 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**.

You can specify temperature thresholds for managed systems that have configurable thresholds for temperature sensors. Expand the thresholds tree and select the applicable temperature sensor. Specify the Warning and Critical thresholds and click **Apply**.

Use bindings to enable or disable different severities of alerts, including pop-up windows, 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, Critical, or Normal 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 that is 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. You 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 in the left pane, and nonmember groups are listed in the right pane. Clicking the < and > buttons moves user names to and from the **Member groups** and **Non-member groups** lists.

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 that is assigned to a user account that runs each time the user logs on.

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	This field contains the user's new password (32 character maximum, case sensitive).
Confirm password	This field must contain the same character string as the New Password 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: This option is available only on systems on which Advanced Power Management is supported and enabled.

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 information about 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**.

Part 4. Troubleshooting and maintenance

Chapter 32. Solving IBM Director problems	327
Chapter 33. Updating IBM Director	347
Chapter 34. Getting help and technical assistance	349

Chapter 32. Solving IBM Director problems

This chapter describes some of the problem symptoms and suggested solutions for the following procedures, components, and features in IBM Director 4.20:

- Installation, upgrades, and uninstallation (see page 327)
- IBM Director Server (see page 329)
- IBM Director Console (see page 333)
- IBM Director Agent (see page 337)
- Managed systems running Windows (see page 338)
- IBM Director tasks (see page 339)
- Software Distribution (see page 342)
- Web-based Access (see page 344)
- Systems running double-byte character set (DBCS) languages (see page 345)

Installation, upgrades, and uninstallation

This section describes problems that might occur when you install, upgrade, or uninstall IBM Director.

Installation

Table 36 describes problems that might occur when you install IBM Director.

Table 36. Installation problems

Symptom	Suggested action
(Windows only) When you install IBM Director, 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.	The monitor 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 partial installation, and reinstall IBM Director Server.
(Windows only) When an installation of IBM Director Agent is canceled, files are left in directories.	Delete the following files: <ul style="list-style-type: none">• <i>designated_drive</i>\IBM\Director\data• <i>designated_drive</i>\IBM\Director\data\map• <i>designated_drive</i>\IBM\Director\data\script• <i>designated_drive</i>\IBM\Director\data\snmp where <i>designated_drive</i> is the directory that you designated for the installation.
(Windows only) When you modify IBM Director Agent or IBM Director Console, you are prompted for the location of either the IBM Director Agent.msi file or the IBM Director Console.msi file.	Extract the files from the Web installation package that you used when you installed IBM Director Agent or IBM Director Console. When prompted for the location of the IBM Director Agent.msi file or the IBM Director Console.msi file, specify the directory where the extracted files are located.
(Windows Server 2003 only) When IBM Director Server or IBM Director Agent starts for the first time on an ASF-capable system, the event log might contain traps or exceptions.	IBM Director Server or IBM Director Agent completed installation before the system management bus (SMBus) was detected and the device driver installed. When you install IBM Director Server or IBM Director Agent, be sure that the SMBus device driver is installed before you restart the system.

Table 36. Installation problems (continued)

Symptom	Suggested action
(Windows Server 2003 only) During installation of IBM Director Agent, Windows might display the following blue screen trap: IRQL_NOT_LESS_OR_EQUAL	This problem is solved by a Microsoft update. See the Microsoft Knowledge Base Article 825236 for more information.

Upgrades

Table 37 describes problems that might occur when you upgrade IBM Director.

Table 37. Upgrade problems

Symptom	Suggested action
Error message 1306 is displayed.	Modify the settings for the IBM Director Support Program Service (TWGIPC). If Web-based Access is installed, you also must modify the settings for the IBM Director Agent Web Server (DirWbs). For both services, set the startup type to Manual . Restart (reboot) the management server, and then begin the uninstallation again.
When you upgrade from IBM Director 3.1 or 3.1.1, error message 1921 might be displayed for the UMSHTTPD service.	Stop the UMSHTTPD service.
(Japanese, Simplified and Traditional Chinese, and Korean only) After upgrading from IBM Director 3.1 to IBM Director 4.20, in the Management Processor Assistant (MPA) task, distorted characters appear in the Description field of the Alert-Forwarding Profiles.	Make a note of the Description field contents before upgrading. After installing IBM Director 4.20, you must reenter the information in English. All of the input fields that are interpreted by the service processor must be provided in US ASCII.
If you performed the following upgrades, the UM Service tree (which is displayed in the "Simple Event Filter Builder" window) is obsolete and cannot be used to filter events: 1. From version 3.1 to version 3.1.1 2. From version 3.1.1 to version 4.1 3. From version 4.1 to version 4.11 4. From version 4.11 to version 4.12 5. From version 4.12 to version 4.20	Right-click the UM Services tree and click Delete . Use the Director Agent Services tree to filter events.
(Windows only) If you performed the following upgrades and then uninstalled IBM Director Agent, certain files are not uninstalled: 1. From version 3.1 or 3.1.1 to version 4.1 2. From version 4.1 to version 4.20	You can safely delete the following files: <ul style="list-style-type: none"> • <i>d</i>:\Program Files\UMS\Director\bin\CimUrlCgi.log • <i>d</i>:\Program Files\UMS\Director\bin\UMSagent.In • <i>d</i>:\Program Files\UMS\Director\bin\verify.out • <i>d</i>:\Program Files\UMS\Director\websrv • <i>d</i>:\Program Files\UMS\endpoint\lcf_env.cm • <i>d</i>:\Program Files\UMS\endpoint\lcf_env.sh • <i>d</i>:\Program Files\UMS\httpserv\cgi-bin\CimCgi.log where <i>d</i> is the drive letter of the hard disk on which you installed IBM Director Agent.

Uninstallation

Table 38 describes problems that might occur when you uninstall IBM Director.

Table 38. Uninstallation problems

Symptom	Suggested action
(Windows only) Error message 1306 is displayed.	Modify the settings for the IBM Director Support Program Service (TWGIPC). If Web-based Access is installed, you also must modify the settings for the IBM Director Agent Web Server (DirWbs). For both services, set the startup type to Manual . Restart (reboot) the management server, and then begin the uninstallation again.
(Windows only) The following message is displayed: Apache.exe has generated errors and will be closed by Windows. You will need to restart the program.	Modify the settings for the IBM Director Support Program Service (TWGIPC) and the IBM Director Agent Web Server (DirWbs). For both services, set the startup type to Manual . Restart (reboot) the management server, and then begin the uninstallation again.
(Windows 2000 and Windows XP only) If you uninstall IBM Director Server, the following IBM Director Agent Web Server log files might be locked: <ul style="list-style-type: none"> • apache_log • date.txt • stderr.log where <i>date</i> is the date that the file was created.	If this occurs, a message is displayed stating that the file cannot be deleted. When you click Retry , the message is displayed again. This is a Windows timing issue with locked files, and it occurs very infrequently.
(Windows only) If you performed the following upgrades and then uninstalled IBM Director Agent, certain files are not uninstalled: <ol style="list-style-type: none"> 1. From version 3.1 or 3.1.1 to version 4.1 2. From version 4.1 to version 4.20 	You can safely delete the following files: <ul style="list-style-type: none"> • <i>d</i>:\Program Files\UMS\Director\bin\CimUrlCgi.log • <i>d</i>:\Program Files\UMS\Director\bin\UMSagent.In • <i>d</i>:\Program Files\UMS\Director\bin\verify.out • <i>d</i>:\Program Files\UMS\Director\websrv • <i>d</i>:\Program Files\UMS\endpoint\lcf_env.cm • <i>d</i>:\Program Files\UMS\endpoint\lcf_env.sh • <i>d</i>:\Program Files\UMS\httpserv\cgi-bin\CimCgi.log where <i>d</i> is the drive letter of the hard disk on which you installed IBM Director Agent.

IBM Director Server

Table 39 describes general problems that might occur on management servers.

Table 39. IBM Director Server problems

Symptom	Suggested action
Alerts	
If you use IBM Director 4.20 to manage a system running IBM Director Agent 3.1, you might receive frequent Remote Login alerts.	IBM Director Server communicates frequently with the service processors present in managed systems. If IBM Director Agent 3.1 is running on a server that contains a service processor, it generates an event every time the service processor is accessed.
Databases	
(Windows only) The Microsoft Jet database is full.	Migrate to a larger database such as IBM DB2 [®] , Oracle Server, or Microsoft SQL Server.

Table 39. IBM Director Server problems (continued)

Symptom	Suggested action
When an Oracle Server database is used, errors occur during the database configuration process.	Configure and start the Oracle TCP/IP listener before starting the database configuration task. If a failure occurs, check the configuration of the TCP/IP listener.
If you use Telnet from a system running Windows to access a management server running Linux, and then you run the <code>cfgdb</code> utility, messages overlay.	Before running the <code>cfgb</code> utility, set the environmental variable <code>term</code> to <code>vt100</code> . Then, maximize the Telnet window to its largest possible size.
(Linux only) If you are not logged in to IBM Director Console, typing the <code>cfgdb</code> command at a local command prompt causes an error.	Configure the database by performing one of the following procedures: <ul style="list-style-type: none"> Use Telnet to access the management server, and then run the cfgdb command. From a command prompt on the management server, issue the startx command. Then, run the cfgdb command.
(Linux only) When the IBM Director database is run locally on the management server and the management server is restarted, IBM Director Server fails to start. The <code>TWGServer.err</code> file reports a database initialization error.	<p>The TWGserver service might have started before the database service. Back up the <code>etc/init.d/TWGserver</code> script and save it to a safe location. Then, modify the <code>etc/init.d/TWGserver</code> script to make sure that the database service starts before the IBM Director service:</p> <p>For Red Hat Linux: Locate the following section in the script:</p> <pre># chkconfig: 35 90 10 # description: Starts and stops the IBM Director service.</pre> <p>90 is the start number and 10 is the stop number. Modify this section so that the TWGserver start number is greater than the start number for the database service, and the TWGserver stop number is greater than the stop number for the database service.</p> <p>For SUSE LINUX: Locate the following section in the script:</p> <pre>### BEGIN INIT INFO # Required-Start: \$network # Required-Stop: \$network # Default-Start: 3 5 # Default-Stop: 0 1 6 # Description: Starts and stops the IBM Director service. ### END INIT INFO</pre> <p>Add the database service to the Required-Start and Required-Stop lines. For example, for PostgreSQL, change the lines to read as follows:</p> <pre># Required-Start: \$network postgresql # Required-Stop: \$network postgresql</pre> <p>Save the modified script. Run the chkconfig command twice, once to remove the IBM Director service and then to add it back to the list of start and stop services.</p>
Discovery	
A BladeCenter discovery does not function correctly when multiple network interface cards (NICs) are enabled.	<p>Determine the NICs that are connected to the BladeCenter unit network. Disable all NICs except for one, which must be able to communicate with the BladeCenter management module. Perform the discovery. When the discovery is completed, reenabling the NICs that you disabled.</p> <p>Note: You must do this each time you want to discover the BladeCenter unit and its components.</p>

Table 39. IBM Director Server problems (continued)

Symptom	Suggested action
<p>After you click Discover All Systems, an RXE-100 Remote Expansion Enclosure is not discovered.</p>	<p>To solve this problem, perform one of the following procedures:</p> <ul style="list-style-type: none"> • From IBM Director Console, click Tasks → Discover Systems → Physical Platforms; then, click Discover All. • Right-click any blank space in the Group Contents pane and click New → Physical Platforms. The “Add Physical Platforms” window opens. Type the name and IP address of the Remote Supervisor Adapter that is attached to the RXE-100 Remote Expansion Enclosure; then, click OK.
<p>(Managed systems running Linux only) When no default router is configured or a nonroutable private network is used, IBM Director might not discover systems.</p>	<p>Complete one of the following procedures:</p> <ul style="list-style-type: none"> • Seed the network in the System Discovery (IP) pane. Click Options → Discovery Preferences. Then, click System Discovery (IP). • Set a default router by issuing the following command: <code>route add default gw <i>IP_address</i></code> <p>where <i>IP_address</i> is your IP address. For more information, see the man page for the route command. Setting a default router enables the discovery of systems that are accessible using the specified router.</p>
<p>IBM Director Server does not discover SNMP devices.</p>	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> • The management server is running the SNMP service. If it is not, another system on the same subnet must be running an SNMP agent. In that case, remove the management server as the seed device and add the system running the SNMP agent. • The seed devices or other devices to be discovered are running SNMP agents. • The community names that are specified in the “Discovery Preferences” window allow IBM Director to read both the following tables: <ul style="list-style-type: none"> – mib-2.system table of the devices to be discovered – mib-2.ip.ipNetToMediaTable on the seed devices • Correct network masks have been configured for all managed systems that must be discovered. • Correct addresses have been entered for the seed devices. The most effective seed devices are routers and domain name servers. To configure these devices, from IBM Director Console, click Options → Discovery Preferences. SNMP discovery does not discover all SNMP devices. If a device has not communicated with other managed systems, the device might not be discovered.
Encryption	
<p>After you use the “Encryption Administration” window to change encryption settings, certain managed systems appear accessible but cannot be managed.</p>	<p>This might be due to one of the following circumstances:</p> <ul style="list-style-type: none"> • When you request a new key or a cipher algorithm, IBM Director must perform a presence check. This presence check might not be completed immediately. During the delay, IBM Director Server cannot manage the system. • If you disable encryption on the management server, encrypted managed systems can no longer be managed. However, these systems might appear to be manageable for a certain period before they are displayed as locked. <p>To ensure that the icons displayed in IBM Director Console accurately reflect the security state of the managed system, request a presence check.</p>

Table 39. IBM Director Server problems (continued)

Symptom	Suggested action
Event actions	
After a NIC on the management server is reconfigured, certain event actions fail.	IBM Director Server has lost contact with the managed systems that were discovered before the configuration change. From IBM Director Console, click Tasks → Discover Systems → System Discovery to rediscover the managed systems.
A timeout occurs during communications between IBM Director Server and IBM Director Console.	Working with large event action plans can cause network communication errors to occur. IBM Director Server takes a long time to process large requests from IBM Director Console. During this processing period, IBM Director Console waits for a response from IBM Director Server. When no response is received after 15 seconds, a timeout error is generated. This error might occur several times for intensive operations, such as importing or exporting large event action plans. Despite the communication error, the event action plan works correctly.
i5/OS	
Shortly after IBM Director Server is started with encryption enabled using Options, Encryption Administration, IBM Director Server fails.	Make sure that IBM Java Cryptography Extension (JCE) is enabled in the /QIBM/ProdData/Java400/jdk13/lib/security/java.security file. Then, restart IBM Director Server.
IBM Director Server fails to start when SSL is enabled in the TWGServer.prop file.	Make sure that the following conditions are met; then, restart IBM Director Server: <ul style="list-style-type: none"> • A default server certificate is assigned in the Digital Certificate Manager *SYSTEM certificate store. The certificate is neither expired nor revoked. • You have installed a cumulative program temporary fix (PTF) package that includes 5722SS1 SI13495. • After installing the PTF, you enabled JCE in the /QIBM/ProdData/Java400/jdk13/lib/security/java.security file.
IBM Director Server fails to start when the Japanese coded character set identifier (CCSID) 5026 is used.	Make sure that the job CCSID and locale match and that they are supported by Qshell. Consider using CCSID 5035 and locale JA_5035. For more information, go to the iSeries Information Center at http://www.ibm.com/servers/eserver/iseries/infocenter and search on National Language Support.
Starting	
(Linux only) Shortly after IBM Director Server is started, it enters an error state and the daemon.stderr file reports the following error: Exception in thread "main"	Make sure that "localhost" is an alias for the loopback address 127.0.0.1 in the /etc/hosts file. Restart IBM Director Server.
(Windows Server 2003 only) When IBM Director Server starts for the first time on an ASF-capable system, the event log might contain traps or exceptions.	IBM Director Server completed installation before the system management bus (SMBus) was detected and the device driver installed. When you install IBM Director Server or IBM Director Agent, be sure that the SMBus device driver is installed before you restart the system.

Table 39. IBM Director Server problems (continued)

Symptom	Suggested action
You are not sure whether IBM Director Server is running.	<p>To check whether the management server is running, complete one of the following procedures:</p> <ul style="list-style-type: none"> • (i5/OS) From a Qshell command prompt, type the following command and press Enter: /QIBM/ProdData/Director/bin/twgstat <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> • (Linux) From a command prompt, type the following command and press Enter: /opt/IBM/director/bin/twgstat -r <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> • (Windows) Determine which of the following icons is displayed in the task bar in the lower-right corner of the screen. <ul style="list-style-type: none"> – A green circle indicates that IBM Director Server is running. – A green triangle icon indicates that IBM Director Server is in the process of starting. – A red diamond icon indicates that IBM Director Server is not responding. <p>Do not attempt to start IBM Director Console until a green circle is displayed in the task bar.</p>

IBM Director Console

Table 40 describes general problems that might occur on the management console.

Table 40. IBM Director Console problems

Symptom	Suggested action
BladeCenter unit	
After a blade server is installed in a BladeCenter chassis, a physical platform managed object (PPMO) associated with the blade server is not displayed in IBM Director Console.	Run the Inventory task on the BladeCenter chassis.
After a physical platform managed object is deleted, it reappears in IBM Director Console.	Delete the managed system or systems that are associated with the physical platform managed object.
Databases	
(Linux only) If you are not logged in to IBM Director Console, typing the cfgdb command at a local command prompt causes an error.	<p>Configure the database by performing one of the following procedures:</p> <ul style="list-style-type: none"> • Use Telnet to access the management server, and then run the cfgdb command. • From a command prompt on the management server, issue the startx command. Then, run the cfgdb command.
Data displayed in windows	
Some IBM Director Console windows display tables of data. The columns within these tables might not display the entire contents contained in them when the window opens.	To widen a column, drag the column border to resize it, or resize the entire window. The changes to the columns are not saved, and the next time the window is opened, you might have to resize the columns again.

Table 40. IBM Director Console problems (continued)

Symptom	Suggested action
Dynamic groups criteria	
When a dynamic group is created using certain criteria (such as the not-equal-to operator as part of the selected criteria), not all of the managed systems that meet those criteria are returned.	<p>Make sure that you use the correct criteria when you create the dynamic group. Each criterion searches only the rows in the inventory database with which it is associated.</p> <p>For example, when you select the following criterion: Inventory (PC)/SCSI Device/Device Type=TAPE</p> <p>IBM Director searches the inventory database for managed systems that have entries in the SCSI_DEVICE table. Then, IBM Director returns only the managed systems that have a value of TAPE in the DEVICE_TYPE column.</p> <p>When you select the following criterion: Inventory (PC)/SCSI Device/Device Type ^= TAPE</p> <p>IBM Director searches the inventory database for managed systems that have entries in the SCSI_DEVICE table. Then, IBM Director returns only the managed systems that do not have a value of TAPE in the DEVICE_TYPE column.</p> <p>Selecting the second criterion does not return all managed systems that do not have SCSI tape drives. It returns all managed systems that contain non-tape SCSI devices.</p>
Event action plans	
An event action plan is not displayed.	<p>When you apply an event action plan to a group, the event action plan is associated with <i>all</i> existing systems in the group. However, this group event action plan is not displayed as associated with each individual managed system that is part of the group. The event action plan is displayed as being applied to the group <i>only</i>.</p> <p>Complete the following steps to view the event action plans associated with the groups of managed systems:</p> <ol style="list-style-type: none"> 1. In IBM Director Console, click Associations → Event Action Plans. 2. In the Groups pane, click All Groups. 3. In the Group Category Contents pane, expand each group that has an event action plan applied to it and view the event action plans that are applied to the group.
Java Runtime Environment (JRE) Exceptions	
Intermittent JRE exceptions occur.	<p>Make sure that the management console has sufficient memory. Intermittent JRE exceptions might occur when you run IBM Director Console on systems that have insufficient memory. Sun Microsystems has acknowledged this problem. For more information about memory requirements, see the <i>IBM Director 4.20 Installation and Configuration Guide</i>.</p>
Managed system	
A question mark is displayed with the managed system icon.	<p>Reestablish communication between IBM Director Server and IBM Director Agent on the managed system. Click Tasks → Discover Systems → System Discovery to rediscover the managed system.</p>

Table 40. IBM Director Console problems (continued)

Symptom	Suggested action
Managed systems are not displayed in IBM Director Console.	<p>Make sure that the system is turned on, IBM Director Agent is running, and the network connection is reliable.</p> <p>Increase the network timeout value for both IBM Director Server and IBM Director Agent:</p> <ul style="list-style-type: none"> • Windows: Run twgipccf.exe. • Linux: Using an ASCII text editor, open the <code>ServiceNodeLocal.properties</code> file (located in the <code>/opt/IBM/director/data</code> directory), and modify the value of <code>ipc.timeouts</code>. By default, it is set to 15 seconds. <p>Stop and restart IBM Director Agent to ensure that the new network timeout takes effect.</p>
A request for access fails and the managed system remains locked.	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> • You are using the correct user ID and password. • If the managed system accepts encrypted communications only, make sure that the management server has encryption enabled also. • If the managed system is running Linux, the password encryption is set to either Message Digest 5 (MD5) or Data Encryption Standard (DES).
When you request access to a managed system running Linux, access is not granted.	<p>If the operating-system password encryption method is set to MD5 (Message Digest 5) when you install IBM Director Agent, salt values that contain only two characters might be generated. IBM Director requires that the salt values be eight characters in length. Use the passwd command to reset the password for the account that is used to access the managed system.</p>
<p>After using imaging to deploy a system, duplicate managed systems are displayed in IBM Director Console.</p> <p>When using imaging, make sure that the instance of IBM Director Agent that is being cloned has never been started.</p>	<p>Perform one of the following procedures on the duplicate managed system:</p> <p>Linux: Complete the following steps:</p> <ol style="list-style-type: none"> 1. Using an ASCII text editor, open the <code>ServiceNodeLocal.properties</code> file (located in the <code>/opt/IBM/director/data</code> directory), and delete the line that begins with the following string: <code>ipc.UID=</code> 2. Delete the <code>TWGagent.uid</code> file, which is located in the <code>/etc/TWAgent</code> directory. <p>Windows: Complete the following steps:</p> <ol style="list-style-type: none"> 1. Remove the following registry key: <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName\TWGMachineID</code> 2. Delete the <code>twgmach.id</code> file. If you installed IBM Director Agent in the default location, this file is in the <code>\\Program Files\IBM\data</code> directory.

Table 40. IBM Director Console problems (continued)

Symptom	Suggested action
<p>(Linux only) When no default router is configured or a nonroutable private network is used, IBM Director might not add discovered systems on these networks to the IBM Director Console Group Contents pane.</p>	<p>Complete one of the following procedures to ensure that the managed systems are displayed in IBM Director Console:</p> <ul style="list-style-type: none"> Seed the network in the System Discovery (IP) pane. Click Options → Discovery Preferences. Then, click System Discovery (IP). Set a default router by issuing the following command: <pre>route add default gw IP_address</pre> <p>where <i>IP_address</i> is your IP address. For more information, see the man page for the route command. Setting a default router enables the discovery of systems that are accessible using the specified router.</p>
<p>After you use the “Encryption Administration” window to change encryption settings, certain managed systems appear accessible but cannot be managed.</p>	<p>This might be due to one of the following circumstances:</p> <ul style="list-style-type: none"> When a new key or a new cipher algorithm is requested, a presence check is forced by IBM Director. This presence check might not be completed immediately. During this delay, IBM Director Server cannot manage the system. When encryption is disabled on the management server, encrypted managed systems can no longer be managed. However, these systems might appear to be manageable for a certain period before they are displayed as locked. <p>To ensure that the icons displayed in IBM Director Console accurately reflect the security state of the managed system, request a presence check.</p>
Starting	
<p>When you try to start IBM Director Console, the following error message is displayed:</p> <p>An IO error occurred while connecting to the IBM Director Server.</p>	<p>Before you start IBM Director Console, make sure that IBM Director Server is running.</p> <ul style="list-style-type: none"> (i5/OS) From a Qshell command prompt, type the following command and press Enter: <pre>/QIBM/ProdData/Director/bin/twgstat</pre> <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> (Linux) From a command prompt, type the following command and press Enter: <pre>/opt/IBM/director/bin/twgstat -r</pre> <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> (Windows) Determine which of the following icons is displayed in the task bar in the lower-right corner of the screen. <ul style="list-style-type: none"> – A green circle indicates that IBM Director Server is running. – A green triangle icon indicates that IBM Director Server is in the process of starting. – A red diamond icon indicates that IBM Director Server is not responding. <p>Do not attempt to start IBM Director Console until a green circle is displayed in the task bar.</p>

Table 40. IBM Director Console problems (continued)

Symptom	Suggested action
Errors occur during attempts to log on to the management server using IBM Director Console.	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> • Both the management server and IBM Director Server are running. • The management server name, user ID, and password are valid. (For systems running Windows, you must qualify the user ID with either the domain or the local computer name of the management server.) • You have a connection from the management console to TCP port 2033 on the management server. • IBM Director Console and IBM Director Server are the same version. • (If SSL is used) Both the management console and the management server are using compatible data link connection classes and parameters in the TWGConsole.prop and TWGServer.prop files. • (If SSL is used) The certification chain of the certificate authority that issued the server certificate is trusted in the keystore that is used by the management console.
Time zone	
The wrong time zone is displayed.	When the time zone setting is changed on the managed system, the time that is shown in the event viewer is not adjusted. Restart the managed system to ensure that the correct time zone is displayed.

IBM Director Agent

Table 41 describes symptoms of problems that might occur on managed systems.

Table 41. IBM Director Agent problems

Symptom	Suggested action
(Linux only) Shortly after IBM Director Agent starts, it enters an error state and the daemon.stderr file reports the following error: Exception in thread "main"	Make sure that "localhost" is an alias for the loopback address 127.0.0.1 in the /etc/hosts file. Restart IBM Director Agent.
(Windows Server 2003 only) When IBM Agent starts for the first time on an ASF-capable system, the event log might contain traps or exceptions.	<p>IBM Director Agent completed installation before the system management bus (SMBus) was detected and the device driver installed.</p> <p>When you install IBM Director Server or IBM Director Agent, be sure that the SMBus device driver is installed before you restart the system.</p>
When you request access to a managed system running Linux, access is not granted.	If the operating-system password encryption method is set to MD5 (message digest 5) when you install IBM Director Agent, salt values that contain only two characters might be generated. IBM Director requires that the salt values be eight characters in length. Use the passwd command to reset the password for the account that is used to access the managed system.

Table 41. IBM Director Agent problems (continued)

Symptom	Suggested action
(Red Hat Linux only) On rare occasions, when the Inventory task attempts to collect data on Red Hat Package Manager (RPM) packages, IBM Director Agent times out and fails.	<p>Stop and restart IBM Director Agent.</p> <p>If you do not need the RPM package data, clear the check box in the Inventory pane of the “Server Preferences” window; then, run the Inventory task again.</p> <p>If you do need the RPM package data, you must create a symbolic link. From the command prompt on the managed system, using an account with root privileges, type the following commands:</p> <pre>ln -s /usr/lib/librpm-x.so /usr/lib/librpm-4.0.3.so ln -s /usr/lib/librpmio-x.so /usr/lib/librpmio-4.0.3.so ln -s /usr/lib/librpmdb-x.so /usr/lib/librpmdb-4.0.3.so</pre> <p>where x is the version of the files on the managed system.</p>

Managed systems running Windows

Table 42 describes symptoms of Windows-specific problems that might occur on managed systems running Windows.

Table 42. Managed systems running Windows problems

Symptom	Suggested action
The Remote Access Connection Manager service fails to start and the following error message is displayed: The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.	This problem is solved by a Microsoft update. See Microsoft Knowledge Base article 830459 for more information.
(Windows 2000 only) After cluster failover, cluster failback, or disk drive unplug operations, a managed system returns invalid resource-monitor information for Windows Performance Monitors or Logical Disks.	Install Microsoft Windows 2000 Service Pack 4.
A managed system returns invalid data values for the following: <ul style="list-style-type: none"> • Windows Performance Monitors • Logical Disk or Windows Performance Monitors • Physical Disk 	This problem is solved by a Microsoft update. See Microsoft Knowledge Base article 827439 for more information.
(Windows 2000 only) The event log is full. This problem occurs on servers when NetBIOS is enabled and IBM Director is installed. Errors are generated until the event log is full.	Uninstall and then reinstall the device driver for the NIC.

Table 42. Managed systems running Windows problems (continued)

Symptom	Suggested action
(Windows 2000 Server only) After IBM Director Server is installed, the following error is displayed in the event log when the server is restarted: The open procedure for service PerfDisk in the DLL C:\WINNT\System32\perfdisk.dll has taken longer than the established wait time to be completed.	Use the regedit command to modify the following key entry and change the decimal value to 30000: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance key "Open Timeout" This gives the system enough time to complete the startup task before starting the PERF counters.
(Windows 2000 with Internet Information Services (IIS) installed) An event ID 2003 warning message appears in the application event log when you start System Monitor and add counters.	Microsoft has identified this as a problem. For more information, see Microsoft Knowledge Base Article 267831.
The following report is generated: Win32_DiskDrive.Size is less than Win32_DiskPartition.Size for a removable medium that has been formatted as a single partition.	The following hard disk drives are not supported by Windows: <ul style="list-style-type: none"> • Optical • Iomega • Jaz Microsoft identified this as a Windows Management Instrumentation (WMI) problem.
A PCI adapter with logical disks cannot be stopped using the "Unplug or Eject Hardware" window.	Install Microsoft Windows 2000 Service Pack 4.

IBM Director tasks

Table 43 describes symptoms of problems that might occur when you are using IBM Director tasks other than Software Distribution.

Table 43. IBM Director task problems

Symptom	Suggested action
Active PCI Manager	
The Active PCI Manager task appears to be available after you upgrade to IBM Director 4.20, but its subtasks are not working.	Complete the following steps to solve this problem: <ol style="list-style-type: none"> 1. From Add/Remove Programs, remove all previous versions of Active PCI Manager. 2. Reinstall IBM Director 4.20. Be sure to install the Active PCI Manager component from the Server Plus Pack.
BladeCenter Assistant	
(IBM @server BladeCenter HS40 only) In the BladeCenter Assistant task, if you click VRM to view the voltage regulator module (VRM) information, two rows of information are displayed.	Ignore the second VRM row that contains a value of 0.0; that VRM does not exist. This error does not generate an event or cause any functional problems.
Common Information Model (CIM) Browser	
When you attempt to enumerate a system running Windows, large amounts of CIM data are returned, causing errors in the CIM Browser.	Do not attempt to enumerate the instances of the following classes: <ul style="list-style-type: none"> • root/cimv2:CIM_DirectoryContainsFile • root/cim2:Win32_Subdirectory Those CIM classes have instances for every file and directory on every disk in your server. If you attempt to enumerate these classes, the managed system or management server might run out of memory.

Table 43. IBM Director task problems (continued)

Symptom	Suggested action
Inventory	
Field-replaceable unit (FRU) information does not appear when inventory is collected.	<p>If a system is not connected to the Internet when IBM Director Agent is installed, the FRU inventory might be empty. To populate the FRU inventory, run the GETFRU command. For more information, see Appendix B, "Obtaining FRU data files using the GETFRU command," on page 359, in the <i>IBM Director 4.20 Systems Management Guide</i>.</p> <p>In addition, make sure that the GETFRU command can reach the IBM Support FTP site through your firewall. For the GETFRU command to run successfully, the managed system must have firewall access through a standard FTP port.</p>
The Inventory task times out when it is run against a server that contains a Remote Supervisor Adapter II.	Make sure that the Remote Supervisor Adapter II device driver is installed on the managed system.
The ServeRAID inventory tables are missing information.	<p>When IBM Director Server collects inventory from a managed system running IBM Director Agent 3.1 and either Windows NT 4.0 or Windows 2000, the following inventory is not collected:</p> <ul style="list-style-type: none"> • ServeRAID Controllers • ServeRAID Disk Drives • ServeRAID Enclosures • ServeRAID Logical Drives <p>Consider upgrading to IBM Director Agent 4.20.</p>
(Red Hat Linux only) On rare occasions, when the Inventory task attempts to collect data on Red Hat Package Manager (RPM) packages, IBM Director Agent times out and fails.	<p>Stop and restart IBM Director Agent.</p> <p>If you do not need the RPM package data, clear the check box in the Inventory pane of the "Server Preferences" window; then, run the Inventory task again.</p> <p>If you do need the RPM package data, you must create a symbolic link. From the command prompt on the managed system, using an account with root privileges, type the following commands:</p> <pre>ln -s /usr/lib/librpm-x.so /usr/lib/librpm-4.0.3.so ln -s /usr/lib/librpmio-x.so /usr/lib/librpmio-4.0.3.so ln -s /usr/lib/librpmdb-x.so /usr/lib/librpmdb-4.0.3.so</pre> <p>where x is the version of the files on the managed system.</p>
Management Processor Assistant	
When you use the Communications configuration subtask, connection information is not displayed.	<p>Complete one of the following procedures:</p> <ul style="list-style-type: none"> • Exit Management Processor Assistant and wait a few minutes. Start the Management Processor Assistant task and try again. • Click Communications configuration. In the left pane, click Global settings to refresh the Communications configuration subtask for each selected system.
<p>(Japanese, Korean, Simplified Chinese, and Traditional Chinese only)</p> <p>In the Management Processor Assistant (MPA) task, distorted characters appear in the Description field of the Alert-Forwarding Profiles. This problem occurs after you have upgraded from IBM Director 3.1 to IBM Director 4.20.</p>	Make a note of the Description field contents before upgrading. After installing IBM Director 4.20, you must reenter the information in English. All of the input fields that are interpreted by the service processor must be provided in US ASCII.

Table 43. IBM Director task problems (continued)

Symptom	Suggested action
Mass Configuration	
When you use the Mass Configuration task to configure Asset ID™, the configuration fails.	The managed system does not have sufficient data space. When the size of the configuration is larger than that of the remaining data space, the configuration fails (although there is no indication that a failure has occurred). This is a limitation of the data save area. Make sure that, for each byte of data, the managed system has the same amount of space in the data save area.
Network Configuration	
When you use the Network Configuration task to change the computer name of a managed system, the computer name is not displayed correctly.	Be sure to restart the managed system.
(Managed system running Windows Server 2003) When you run the Network Configuration task and view the WINS pane, the IP addresses for the primary and secondary Windows Internet Naming Service (WINS) servers are reversed.	This is caused by a Microsoft implementation of a CIM class. The correct IP addresses are assigned in the system Network Properties.
Remote Control	
When you use a non-English-language keyboard during a remote-control session, some of the keys might not work.	Make sure that the inventory has been collected before you use the Remote Control task.
The Remote Control task fails when both the following conditions are true: <ul style="list-style-type: none"> You are running the task against a managed system that is behind a firewall. You are simultaneously distributing a software package to that managed system. 	The Remote Control and Software Distribution tasks 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: <pre>SESSION_SUPPORT=0</pre> <p>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.</p>
Resource Monitors	
(Windows only) When you run the Resource Monitors tasks against multiple managed systems, incorrect attribute names might be displayed for the network adapters.	The incorrect attribute names are displayed in the Available Resources pane of the "Resource Monitors" window, when you click Director Agent → TCP/IP Monitors . <p>To view the correct attribute names for the network adapters, click Director Agent → Windows Performance Monitors → Network Interface.</p>
SNMP Browser	
When a Management Information Base (MIB) file attribute value is set to a hexadecimal, octal, or binary value, the file fails.	Make sure that all of the values have been converted and are being added in a decimal format.

Table 43. IBM Director task problems (continued)

Symptom	Suggested action
You cannot change an attribute value for a MIB file.	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> • IBM Director uses a community name that allows write access to the MIB file. • The MIB file is writable. • The MIB file has a value that you can set to be displayed in the SNMP Browser. • The compiled MIB file is associated with the value that you want to change.
Trap destinations are missing from the SNMP agent table.	A table displays only the first trap destination in the SNMP configuration interface when multiple communities and traps are associated with each community. The IBM Director inventory stores only the first value of an array-valued property, such as the SNMP trap destination.

Software Distribution

Table 44 describes problems that might occur when you use Software Distribution.

Table 44. Software Distribution problems

Symptom	Suggested action
The software package creation fails.	Check the available disk space on the management console. Packages are created on the management console. If the management-console disk space is insufficient, the package creation fails.
<p>The Software Distribution task fails when both the following conditions are true:</p> <ul style="list-style-type: none"> • You are distributing a software package to a managed system that is behind a firewall. • You are simultaneously running a Remote Control task on that managed system. 	<p>The Remote Control and Software Distribution tasks 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:</p> <pre>SESSION_SUPPORT=0</pre> <p>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.</p>
<p>When a software package is distributed using a redirector share, the following error message is displayed:</p> <pre>I/O error, file (\\server\share) \ (package name)not found on managed system (system name)</pre>	This problem occurs if you manually delete a software package from the redirector share. To deleted packages from the share, you must use the "File Distribution Servers Manager" window. Right-click the Software Distribution task and click File Distribution Servers Manager .
<p>When you attempt to export a software distribution package to a network share, the following error message is displayed:</p> <pre>Unable to export package.</pre>	The Software Distribution task does not support exporting packages to a network share. Modify the operation to export the package to a local drive.

Table 44. Software Distribution problems (continued)

Symptom	Suggested action
(Windows only) Software packages are streamed from the management server, although a file-distribution server is configured for use by the managed systems.	<p>Make sure that one of the following conditions is met:</p> <ul style="list-style-type: none"> • The file-distribution server is a member of the same domain as the management server. • The file-distribution server has a trust relationship with the domain where the management server is located.
(Linux only) If you export a software distribution package to Software Package Bundle (SPB) format and then reimport the package, an error message is displayed.	<p>Change the permission levels. From the local command prompt, type the following command:</p> <pre>chmod 644 filename.spb</pre>
<p>(Japanese only, on managed systems running Windows) In the “Distribution Preferences” window, the Share Name field is filled in by default with the following example share name:</p> <p>¥system¥share</p> <p>However, when you press the yen key, the Share Name field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> 1. Do not overtype or delete the example share name. 2. Retain the yen symbols in the example and replace only system and share with the system name and share name that you want to use. <p>Note: If you press the yen key, do not use the backslashes; the backslashes cause redirected distribution to fail.</p> 3. Close the “Distribution Preferences” window; then, reenter this window, and retain the yen symbols in the Share Name field example.
<p>(Korean only, on managed systems running Windows) In the “Distribution Preferences” window, the Share Name field is filled in with the following example share name by default:</p> <p>₩system₩share</p> <p>where ₩ represents the won symbol.</p> <p>However, when you press the won key, the Share Name field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> 1. Do not overtype or delete the example share name. 2. Retain the won symbols in the example and replace only system and share with the system name and share name that you want to use. <p>Note: If you press the won key, do not use the backslashes; the backslashes cause redirected distribution to fail.</p> 3. Close the “Distribution Preferences” window; then, reenter this window, and retain the won symbols in the Share Name field example.
(File-distribution server running i5/OS only) Redirected software distribution using an FTP share fails.	<p>To use an FTP-based share for redirected software distribution, the FTP configuration on the file-distribution server might need to be modified. Use the Change FTP Attributes command (CHGFTPA) to set the initial name format to *PATH and specify the initial directory. Stop and restart the FTP server. This changes the default FTP settings for all managed systems that use the file-distribution server.</p>
After you upgrade to Software Distribution (Premium Edition), you cannot export a package that was created with Director Update Assistant.	<p>Delete the software package that was created with Software Distribution (Standard Edition). Re-import the package using Director Update Assistant in Software Distribution (Premium Edition).</p>

Web-based Access

Table 45 describes symptoms of problems that might occur when you use Web-based Access.

Table 45. Web-based Access problems

Symptom	Suggested action
(Windows XP or Windows Server 2003 only) A message is displayed stating that Java Virtual Machine (JVM) is needed.	Install a Java Virtual Machine (JVM) from Sun Microsystems.
After repeated installations, there are problems logging in to the managed system using Netscape Navigator.	When you uninstall IBM Director Agent, be sure to save the configuration data. This saves the old Secure Sockets Layer (SSL) certificate and allows the login to the IBM Director Agent Web Server to successfully complete after IBM Director Agent is reinstalled.
After you log in to Microsoft Internet Explorer, a Java security warning is displayed.	If you are using Microsoft Internet Explorer with the Sun Java Plug-in, additional prompts appear when you log in to a managed system. After you log in to Microsoft Internet Explorer, a Java Security Warning is displayed. Select Grant this session . The Java Plug-in requires authentication information. Type the same information that you used for the Microsoft Internet Explorer login.
When you install Web-based Access on a managed system that is running Apache Web Server, Web-based Access is unavailable. An error message is displayed indicating that the page cannot be found.	Web-based Access and Apache Web Server use the same default connector ports. You must modify the Web-based Access configuration files. If you installed IBM Director Agent in the default location, these files are located in the Program Files\IBM\Director\websrv\conf directory. Complete the following steps to resolve this problem: <ol style="list-style-type: none"> 1. Stop the IBM Director Agent Web Server service. 2. Modify the server.xml file: <ul style="list-style-type: none"> • Change the server port to a port that is not already in use by another application. By default, the server port is set to 8005. • Change the connector port to a port that is not already in use by another application. By default, it is set to 8009. 3. Modify the workers.properties file. Change the connector port to a port that is not already in use by another application. By default, it is set to 8009. 4. Modify the tomcat.conf file. Change the connector port to a port that is not already in use by another application. By default, it is set to 8009. 5. Restart the IBM Director Agent Web Server service.
(Traditional and Simplified Chinese only) When you open Web-based Access in a Netscape Web browser, the Chinese characters might be displayed as boxes.	Complete the following steps to ensure that Chinese characters are displayed properly: <ol style="list-style-type: none"> 1. Install the Java Plug-in 1.4.1 that is available from Sun Microsystems. 2. Check the Windows Display Properties settings to make sure that they are set correctly for Chinese language display.
When you use event bindings, events are not delivered correctly.	If you use the Health service (a Configuration task on the Tasks page) to add event bindings, the system from which you access Web-based Access must have its regional settings set to English. If the regional settings are not set to English, the event filter strings are in the non-English language, and events are not delivered correctly.

Systems running double-byte character set languages

Table 46 describes symptoms of problems that might occur when you are running IBM Director on systems using the following double-byte character set languages: Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Table 46. Systems running double-byte character set languages problems

Symptom	Suggested action
<p>(Japanese, Simplified and Traditional Chinese, and Korean only)</p> <p>After upgrading from IBM Director 3.1 to IBM Director 4.20, in the Management Processor Assistant (MPA) task, distorted characters appear in the Description field of the Alert-Forwarding Profiles.</p>	<p>Make a note of the Description field contents before upgrading. After installing IBM Director 4.20, you must reenter the information in English. All of the input fields that are interpreted by the service processor must be provided in US ASCII.</p>
<p>(i5/OS) IBM Director Server fails to start when the Japanese coded character set identifier (CCSID) 5026 is used.</p>	<p>Make sure that the job CCSID and locale match and that they are supported by Qshell. Consider using CCSID 5035 and locale JA_5035.</p> <p>For more information, go to the iSeries Information Center at http://www.ibm.com/servers/eserver/series/infocenter and search on National Language Support.</p>
<p>(Japanese only, on managed systems running Windows) In the “Distribution Preferences” window, the Share Name field is filled in by default with the following example share name: ¥system¥share</p> <p>However, when you press the yen key, the Share Name field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> 1. Do not overwrite or delete the example share name. 2. Retain the yen symbols in the example and replace only system and share with the system name and share name that you want to use. Note: If you press the yen key, do not use the backslashes; the backslashes cause redirected distribution to fail. 3. Close the “Distribution Preferences” window; then, reenter this window, and retain the yen symbols in the Share Name field example.
<p>(Korean only, on managed systems running Windows) In the “Distribution Preferences” window, the Share Name field is filled in with the following example share name by default: ₩system₩share</p> <p>where ₩ represents the won symbol.</p> <p>However, when you press the won key, the Share Name field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> 1. Do not overwrite or delete the example share name. 2. Retain the won symbols in the example and replace only system and share with the system name and share name that you want to use. Note: If you press the won key, do not use the backslashes; the backslashes cause redirected distribution to fail. 3. Close the “Distribution Preferences” window; then, reenter this window, and retain the won symbols in the Share Name field example.
<p>(Traditional and Simplified Chinese only)</p> <p>When you open Web-based Access in a Netscape Web browser, the Chinese characters might be displayed as boxes.</p>	<p>Complete the following steps to ensure that Chinese characters are displayed properly:</p> <ol style="list-style-type: none"> 1. Install the Java Plug-in 1.4.1 that is available from Sun Microsystems. 2. Check the Windows Display Properties settings to make sure that they are set correctly for Chinese language display.

Chapter 33. Updating IBM Director

IBM might offer new releases or updates to this version of IBM Director. If you purchased IBM Director Multiplatform, see the IBM @server Information Center at <http://www.ibm.com/servers/library/infocenter> for information about new releases.

If you received IBM Director with your IBM @server BladeCenter product or xSeries server, see your hardware documentation for information about updating IBM Director. Also, the IBM @server xSeries Subscription Services is available for you to receive updates automatically. For more information about this service, see your IBM representative.

Chapter 34. 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. Information about diagnostic tools is in the *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *xSeries Documentation* CD or in the *IntelliStation Hardware Maintenance Manual* at the IBM Support Web site.
- 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 or to submit a request for information.

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).

Part 5. Appendixes

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 Table 47 to identify the resource-monitor attributes that you want to monitor if you are planning your IBM Director installation or configuration or 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.

Notes:

- (Windows only) The attributes for the following resource monitors can vary depending on the features and functions that you have configured on the managed system:
 - CIM monitors
 - DMI monitors
 - Device, performance, and service monitors
 - Registry monitors
- (Linux and UNIX only) The attributes for CIM monitors can vary depending on the features and functions that you have configured on the managed system.

To view the resource-monitor attributes that are available for a managed system or device, see “Viewing all resource-monitor thresholds” on page 220.

When referring to Table 47, be sure to select the applicable column for the operating system that is installed on the managed system. For more information about resource monitors, see Chapter 23, “Resource Monitors,” on page 217.

Table 47. Resource-monitor attributes

Attribute	Windows	Linux	UNIX	NetWare	i5/OS	AIX
CPU monitor						
CPU utilization	X	X	X	X		X
CPU 'x' utilization (on SMP devices)	X			X		
Process count	X	X	X	X		X
Thread count				X		
Disk monitor						
Notes:						
1. The disk drive monitor attributes are repeated for each local nonremoveable logical drive that is 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 that is detected.						
Disk 1 workload	X					
Drive C: % space used	X					
Drive C: Space remaining	X					
Drive C: Space used	X					
Blocks available		X	X			X

Table 47. Resource-monitor attributes (continued)

Attribute	Windows	Linux	UNIX	NetWare	i5/OS	AIX
Blocks used		X	X			X
Inodes available		X	X			X
Inodes used		X	X			X
Percentage blocks available		X	X			X
Percentage blocks used		X	X			X
Percentage Inodes available		X	X			X
Percentage Inodes used		X	X			X
Percentage space available		X	X			X
Percentage space used		X	X			X
Space available (MB)		X	X			X
Space used (MB)		X	X			X
Volume SYS: space remaining		X	X	X		
Volume SYS: space used		X	X	X		
File monitor						
File-monitor attributes can be files or directories. See the rows for the applicable file-monitor attributes.						
Notes:						
1. For compatible file-system types, the “Directory exists” or “File exists” attribute (depending on which is applicable) is always valid data.						
2. (Linux, UNIX, and i5/OS only) If there are additional directories, additional subelements are displayed.						
3. (Linux, UNIX, and i5/OS only) A directory can contain hundreds of subelements. If it does, a directory might take 5 seconds or longer to open.						
4. (i5/OS only) QSYS.LIB can contain thousands of subelements. If a timeout occurs, reopening the directory after a timeout increases the timeout value, and may increase the timeout value sufficiently for the operation to complete.						
Directory						
Directory exists	X	X	X	X	X	X
Last modified	X	X	X	X	X	X
Directory attributes		X	X		X	X
Directory owner		X	X		X	X
Directory size (bytes)		X	X		X	X
Object type		X	X		X	X
File						
Checksum	X	X	X	X	X	X
File exists	X	X	X	X	X	X
Last modified	X	X	X	X	X	X
File attributes		X	X		X	X
File owner		X	X		X	X
File size (bytes)	X	X	X	X	X	X
Object type		X	X		X	X
File system monitor						
Note: (UNIX, Linux, and i5/OS only) The file system monitor attributes for specific directories are provided for typical UNIX, Linux, and i5/OS directories. If one of these directories does not exist, the attribute is not displayed.						

Table 47. Resource-monitor attributes (continued)

Attribute	Windows	Linux	UNIX	NetWare	i5/OS	AIX
/		X	X		X	
/bin		X	X		X	
/dev		X	X		X	
/etc		X	X		X	
/home		X	X		X	
/lib		X	X		X	
/lost+found		X	X			
/sbin		X	X			
/tmp		X	X		X	
/usr		X	X		X	
/var		X	X		X	
List of directory contents						
Directory attributes		X	X		X	
Directory exists		X	X		X	
Directory owner		X	X		X	
Directory size (bytes)		X	X		X	
Last modified		X	X		X	
Object type		X	X		X	
Memory monitor						
Locked memory	X					
Memory usage	X					
Available (bytes)		X	X			X
Used (bytes)		X	X			X
Cache blocks in use				X		
Percent of cache in use				X		
Total memory		X				X
Unused non-cached (MBytes)		X				
TCP/IP monitor						
Interface <i>x</i> - Broadcast packets received	X					
Interface <i>x</i> - Broadcast packets sent	X					
Interface <i>x</i> - Bytes received	X					
Interface <i>x</i> - Bytes sent	X					
Interface <i>x</i> - Unicast packets received	X					
Interface <i>x</i> - Unicast packets sent	X					
IP packets received	X					
IP packets received with errors	X					
IP packets sent	X					
TCP connections	X					

Table 47. Resource-monitor attributes (continued)

Attribute	Windows	Linux	UNIX	NetWare	i5/OS	AIX
UDP datagrams received	X					
UDP datagrams sent	X					
Process monitor						
Note: The number of applications or executable files that a process monitor checks can vary. The IBM Director user configures the processes that are 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	X
Maximum running at once	X	X	X	X	X	X
Maximum running yesterday	X	X	X	X	X	X
New executions counted	X	X	X	X	X	X
Times failed to start	X	X	X	X	X	X
Time started	X	X	X	X	X	X
Time stopped	X	X	X	X	X	X
Total execution time	X	X	X	X	X	X
Yesterday's execution time	X	X	X	X	X	X
Yesterday's new executions	X	X	X	X	X	X
UNIX system monitors						
CPU monitors		X	X			X
Disk monitors		X	X			X
Disk performance monitors		X	X			
Memory monitors		X	X			X
Network monitors		X	X			
CIM monitors						
Namespaces	X	X	X			
Classes	X	X	X			
Instances	X	X	X			
Properties	X	X	X			
I/O processors						
Auxiliary IOP Use %					X	
IOP All Comm. Use %					X	
IOP Disk Use %					X	
IOP LAN Use %					X	
IOP Memory Free (KB)					X	
IOP Operational Status					X	
IOP Optical Use %					X	
IOP SDLC Use %					X	
IOP System Function Use %					X	
IOP Tape Use %					X	
IOP Twinaxial Use %					X	
IOP X.25 Use %					X	
Primary IOP Use %					X	

Table 47. Resource-monitor attributes (continued)

Attribute	Windows	Linux	UNIX	NetWare	i5/OS	AIX
Job queues						
Job Queue Status					X	
Jobs in Queue					X	
Job statistics						
Batch Jobs Ended, Output Waiting					X	
Batch Jobs Ending					X	
Batch Jobs Held on Job Queue					X	
Batch Jobs Held while Running					X	
Batch Jobs on Held Job Queue					X	
Batch Jobs on Unassigned Job Queue					X	
Batch Jobs Running					X	
Batch Jobs Waiting for Messages					X	
Batch Jobs Waiting to Run					X	
Jobs on System					X	
NetServer statistics						
Average Response Time (Milliseconds)					X	
File Opens/Minute					X	
Kbytes Received per Minute					X	
Kbytes Sent per Minute					X	
Password Violations					X	
Print Jobs Queued/Minute					X	
Session Starts/Minute					X	
Physical disks						
Disk Arm Utilization %					X	
Disk Average Queue Length					X	
Disk Mirroring Status					X	
Disk Operational Status					X	
Disk Processor Utilization %					X	
Disk Read Commands/Minute					X	
Disk Read Kbytes/Minute					X	
Disk Space Free (MB)					X	
Disk Space Used %					X	
Disk Write Commands/Minute					X	
Disk Write Kbytes/Minute					X	
Storage pools						
Active to Ineligible (Transitions/Minute)					X	
Active to Wait (Transitions/Minute)					X	
Database Faults per Second					X	

Table 47. Resource-monitor attributes (continued)

Attribute	Windows	Linux	UNIX	NetWare	i5/OS	AIX
Database Pages per Second					X	
Non-database Faults per Second					X	
Non-database Pages per Second					X	
Wait to Ineligible (Transitions/Minute)					X	
Subsystems						
Subsystem % of Job Limit					X	
Subsystem Active Jobs					X	
Subsystem Status					X	
System statistics						
CPU Utilization %					X	
Current Temp Storage Used (MB)					X	
Max Temp Storage Used (MB)					X	
Permanent Addresses Used %					X	
System ASP Used %					X	
Temporary Addresses Used %					X	
User statistics						
Users Disconnected					X	
Users Signed Off, Output Waiting					X	
Users Signed On					X	
Users Suspended by Group Jobs					X	
Users Suspended by System Request					X	

Appendix B. Obtaining FRU data files using the GETFRU command

You can obtain information about the field-replaceable unit (FRU) components that are installed on a managed system by 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.

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.software.ibm.com/pc/pccbbs/bp_server` on FTP port 21.

Notes:

1. (Managed systems running Linux only) IBM Director attempts to copy the FRU data file from the IBM Support FTP site during the IBM Director Agent installation on the managed system.
2. (Managed systems running Windows only) After you install IBM Director Agent, IBM Director attempts to copy the FRU data file from the IBM Support FTP site when you restart the managed system.

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, complete the following steps to copy the FRU files to your network from the IBM Support FTP site:

1. Access the IBM Support FTP site (`ftp.software.ibm.com`) using the FTP protocol. This FTP site uses an anonymous login.
2. Change to the directory `/pc/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 file name. These file names use the following syntax:

`machine_type_numberums.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, use 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 an 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 “Viewing and working with processes, services, and device-services information” on page 197 for more information.

Appendix C. Terminology summary and abbreviation list

This appendix provides a summary of IBM Director terminology and a list of abbreviations that are 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.

Extensions are tools for advanced server management that extend the functionality of IBM Director. Such tools include the IBM Server Plus Pack, Software Distribution (Premium Edition), Remote Deployment Manager, and others.

(Management servers running Windows only) The *IBM Director service account* is an operating-system user account on the management server. This is the account under which the IBM Director Service runs.

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

The system from which you invoke DIRCMD, the IBM Director command-line interface, is a *DIRCMD client*.

Abbreviations

The following table lists abbreviations that are used in the IBM Director 4.20 documentation.

Table 48. Abbreviations used in IBM Director

Abbreviation	Definition
A	
ACPI	Advanced Configuration and Power Interface
ASCII	American Standard Code for Information Interchange
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI adapter

Table 48. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
ASM processor	Advanced System Management processor
B	
BIOS	basic input/output system
C	
CCSID	coded character set identifier
CIM	Common Information Model
CIMOM	CIM Object Manager
CPW	commercial processing workload
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management
CSV	comma-separated value
D	
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DMI	Desktop Management Interface
DMTF	Distributed Management Task Force
DNS	Domain Name System
DSA	Digital Signature Algorithm
E	
EEPROM	electrically erasable programmable read-only memory
F	
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	File Transfer Protocol
G	
GB	gigabyte
Gb	gigabit
GMT	Greenwich mean time
GUI	graphical user interface
GUID	globally unique identifier
H	
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I	
IETF	Internet Engineering Task Force
IFS	integrated file system
IIS	Microsoft Internet Information Services
I/O	input/output

Table 48. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
IP	Internet Protocol
IPC	interprocess communication
IPMI	Intelligent Platform Management Interface
IPX	Internetwork Packet Exchange
ISDN	integrated services digital network
ISMP	integrated system management processor
J	
JCE	IBM Java Cryptography Extension
JDBC	Java Database Connectivity
JDK	Java Development Kit
JFC	Java Foundation Classes
JRE	Java Runtime Environment
JVM	Java Virtual Machine
K	
KB	kilobyte
KBps	kilobytes per second
Kb	kilobits
Kbps	kilobits per second
KVM	keyboard/video/mouse
L	
LAN	local area network
LED	light-emitting diode
M	
MAC	media access control
MB	megabyte
MBps	megabytes per second
Mb	megabit
Mbps	megabits per second
MD5	message digest 5
MDAC	Microsoft Data Access Control
MHz	megahertz
MIB	Management Information Base
MIF	Management Information Format
MMC	Microsoft Management Console
MPA	Management Processor Assistant
MPCLI	Management Processor Command-Line Interface
MSCS	Microsoft Cluster Server
MSDE	Microsoft Data Engine
MST	Microsoft software transformation
MTU	maximum transmission unit

Table 48. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
N	
NAS	network attached storage
NetBIOS	Network Basic Input/Output System
NIC	network interface card
NNTP	Network News Transfer Protocol
NTFS	Windows NT 4.0 file system
NVRAM	nonvolatile random access memory
O	
ODBC	Open Database Connectivity
OID	object ID
P	
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PET	Platform Event Trap
PFA	Predictive Failure Analysis
PIN	personal identification number
POST	power-on self-test
PPMO	physical platform managed object
PPP	Point-to-Point Protocol
PTF	program temporary fix
R	
RAID	redundant array of independent disks
RAM	random access memory
RDM	IBM Remote Deployment Manager
RPM	(1) Red Hat Package Manager (2) revolutions per minute
S	
SCSI	small computer system interface
SHA	Secure Hash Algorithm
SID	(1) security identifier (2) Oracle system identifier
SLP	Service Location Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SMBIOS	System Management BIOS
SMBus	system management bus
SMI	System Management Information
SMS	Microsoft Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture

Table 48. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
SNMP	Simple Network Management Protocol
SPB	software package bundle
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	IBM Scalable Systems Manager
T	
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
U	
UDP	User Datagram Protocol
UID	unique ID
UIM	upward integration module
UNC	universal naming convention
USB	Universal Serial Bus
UUID	universal unique identifier
V	
VMM	IBM Virtual Machine Manager
VPD	vital product data
VRM	voltage regulator module
W	
WAN	wide area network
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
X	
XML	Extensible Markup Language

Appendix D. Notices

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

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

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

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

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

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

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

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

Edition notice

© Copyright International Business Machines Corporation 2004. All rights reserved.

U.S. Government Users Restricted Rights — Use, duplication, or disclosure restricted by 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	OS/400
AIX	PowerPC
Asset ID	Predictive Failure Analysis
BladeCenter	pSeries
DB2	Redbooks
DB2 Universal Database	ServeRAID
e-business logo	ServerProven
@server	SurePOS
IBM	ThinkCentre
IBM i5/OS	ThinkPad
IBM Virtualization Engine	Tivoli
IntelliStation	Tivoli Enterprise
iSeries	Tivoli Enterprise Console
Netfinity	TotalStorage
NetView	Wake on LAN
NetVista	xSeries

Intel and Pentium are trademarks 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 trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

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).

Advanced System Management (ASM) interconnect. A feature of IBM service processors. It enables you 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. 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 that is built into the system board of Netfinity 7000 M10 and 8500R servers. It also was available as an option that could be installed in a server that contained an ASM processor. When an ASM PCI adapter is used 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 a gateway service processor, 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; an ASM PCI adapter, a Remote Supervisor Adapter, or a Remote Supervisor II must serve as the gateway service processor.

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 remote alerts for the service processor 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 system in an environment that does not have an operating system.

anonymous command execution. Execution of 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.

ASM interconnect gateway. See gateway service processor.

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

basic input/output system (BIOS). The personal computer code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard. The Configuration/Setup Utility program is a menu-driven utility that is part of the BIOS code that comes with a server. You can start it with F1 during a specific point in the server startup (by watching the screen for a message about it).

BIOS. See basic input/output system.

blade server. An IBM @server BladeCenter 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 unit 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 chassis detect-and-deploy 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 diagnose problems in the components that are present 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.

chassis detect-and-deploy profile. A profile that IBM Director automatically applies to all new BladeCenter chassis when they are discovered. The profile settings include management module name, network protocols, and static IP addresses. If Remote Deployment Manager is installed on the management server, the chassis detect-and-deploy profile also can include deployment policies.

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 systems-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.

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

D

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

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

DES. See data encryption standard.

deployment policy. A policy that associates a specific bay in a BladeCenter chassis with an RDM noninteractive task. When a blade server is added to or replaced in the bay, IBM Director automatically runs the RDM task.

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. It is mappable to existing management protocols such as Simple Network Management Protocol (SNMP).

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 and managed system.

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. A Windows operating-system group that is 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 super-user group to use a command-line prompt to access, control, and gather information from IBM Director Server.

DIRCMD client. The system from which a system administrator invokes DIRCMD.

DirSuper. A Windows operating-system group that is 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 condition relating to a specific managed object. There are two types of events: alert and resolution. An *alert* is the occurrence of a problem relating to a managed object. A *resolution* is the occurrence of a correction or solution to a problem.

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 comprises 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 a simple event action plan.

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-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.

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

forecast. In the Capacity Manager task, a function 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

gateway service processor. A service processor that relays alerts from service processors on an ASM interconnect network to IBM Director Server.

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 managed-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 the IBM Director Console interface. 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) that you can use 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 Windows operating-system account associated with the IBM Director Server service.

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 system 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. 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. The gateway service processor must be a Remote Supervisor Adapter or a Remote Supervisor Adapter II.

interprocess communication (IPC). A method by which threads and processes can transfer data and messages among themselves. Interprocess communication is used to transfer data and messages between IBM Director Server and IBM Director Agent, as well as IBM Director Agent and service processors. It also is 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 software installed on managed systems 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 installed on a managed system.

IPC. See interprocess communication.

IPMI. See Intelligent Platform Management Interface.

IPMI baseboard management controller. Definition

ISMP. See integrated system 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 lit to indicate that a specific component or subsystem needs to be replaced.

M

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

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

managed object. An item managed by IBM Director. In IBM Director Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or scalable system, 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 I/O 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 NetWare.

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.

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

Microsoft Cluster Browser task. An IBM Director task that can be used to perform the following operations:

- Display the structure, nodes, and resources associated with a Microsoft Cluster Server (MSCS) cluster
- Determine the status of a cluster resource
- 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

nonvolatile random-access memory (NVRAM). Random access memory (storage) that retains its contents after the electrical power to the computer is shut off.

notification. See alert.

NVRAM. See nonvolatile random-access memory.

O

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

P

partition. See scalable partition.

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. 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).

plug-in. See IBM Director extension.

POST. See power-on self-test.

power-on self-test. A diagnostic testing sequence that is run by the BIOS when a system is turned on. The POST determines whether the RAM, disk drives, peripheral devices, and other hardware components are properly working.

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 access by management servers.

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

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 I/O enclosure. An IBM Director managed object that represents an expansion enclosure of PCI-X slots, for example, an RXE-100 Remote Expansion Enclosure. The enclosure consists of one or two expansion kits. Each expansion kit contains six hot-swap Active PCI-X adapter slots.

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 a gateway service

processor, 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. It 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.

RXE Expansion Port. The dedicated high-speed port used to connect a remote I/O expansion unit, such as the RXE-100 Remote Expansion Enclosure, to a server.

S

scalable node. A physical platform that has at least one SMP Expansion Module. Additional attributes are assigned to a physical platform when it is a scalable node. These additional attributes record the number of SMP Expansion Modules, SMP Expansion Ports, and RXE Expansion ports on the physical chassis.

scalable object. An IBM Director managed object that is used with Scalable Systems Manager. Scalable objects include scalable nodes, scalable systems, scalable partitions, and remote I/O enclosures that are attached to scalable nodes.

scalable partition. An IBM Director managed object that defines the scalable nodes that can run a single image of the operating system. A scalable partition has a single, continuous memory space and access to all associated adapters. A scalable partition is the logical equivalent of a physical platform. When Scalable Systems Manager is installed, you can power-on and power-off a supported scalable partition through IBM Director Console. IBM Director manages a scalable partition through the service processor on the primary scalable node of that scalable partition. Scalable partitions are associated with scalable systems and comprise only the scalable nodes from their associated scalable systems.

scalable system. An IBM Director managed object that consists of scalable nodes and the scalable partitions that are made from the scalable nodes in the scalable system. When a scalable system contains two or more scalable nodes, the servers that they represent must be interconnected through their SMP Expansion Modules to make a multinode configuration, for example, a 16-way xSeries 455 server made from four scalable nodes. When a scalable node is unlocked, IBM Director automatically creates a scalable system and scalable partition containing that scalable node based on the information stored in NVRAM of the service processor.

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 445 and xSeries 455 servers.

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 Cable. The cable used to connect two SMP Expansion Ports.

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 server is the first hardware platform that uses SMP Expansion Modules.

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

SNMP Access and Trap Forwarding. An IBM Director Agent feature that enables SNMP as a protocol for accessing managed-system data. When installed on a managed system, this feature 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).

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.

SSM. See Scalable Systems Manager.

static group. See group, static.

static partition. A view-only scalable partition.

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 provides active monitoring of critical system functions, including system temperatures, voltages, and fan speeds. It also handles in-band alert notification for managed systems running Windows and some managed systems running Linux.

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 Wired for Management (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 scalable nodes, scalable partitions, scalable systems, 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 enable 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 Systems Manager Server (SMS), to interpret and display data provided by IBM Director Agent. A module also can provide enhancements that you can use 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 numbers, component FRU number, serial number, manufacturer ID, and slot numbers; 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 you 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 enables you to remotely turn on a server. After the server is started, it 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, enables you to use a Web browser or Microsoft Management Console (MMC) to view real-time asset and health information about the managed system.

Index

A

- abbreviations 361
- abcwizard.dtd file 126
- access objects (DIRCMD) 284
- actions
 - See event actions
- activations 40
- Active PCI Manager
 - Common Information Model 79
 - Fault Tolerant Management Interface 79
 - CIM events 83
 - CIM queries 82
 - failover operation 82
 - fault-tolerant groups 79
 - FTMI operations 81
 - interface 80
 - overview 8
 - starting 80
 - hardware, supported 8
 - operating systems, supported 26
 - overview 8
 - Slot Manager
 - adding adapters 90
 - analyzing PCI performance 88
 - defining adapter attributes 91
 - event filtering 92
 - icons 87
 - interface 84
 - optimization solutions 89
 - overview 8, 83
 - performance issues 88
 - reports 90
 - setting adapter and slot characteristics 91
 - starting 84
 - viewing slots and adapters 84, 85
 - working with slots and buses 87
 - subtasks 8
 - troubleshooting 339
- add BladeCenter chassis (DIRCMD) 303
- Add Physical Platforms window 331
- add systems (DIRCMD) 291, 297
- add to static group (DIRCMD) 288
- Advanced Power Management 324
- Advanced Systems Management PCI adapter
 - See ASM PCI adapter
- Advanced Systems Management processor
 - See ASM processor
- Agent
 - See IBM Director Agent
- AIX
 - Custom Package Editor 245
 - InstallP Package wizard 242
 - RPM Package wizard 241
- alert-forwarding profile
 - configuring 98, 179
 - deleting 99
 - troubleshooting 328, 340
- alerts
 - definition 55
 - displaying hardware status 32
 - filtering 65
 - Remote Login 329
 - resource exhaustion 263
 - sending a test 180
 - ServeRAID Manager 226
 - settings 97, 179
 - viewing hardware status 207
- all events filter 61
- All Groups, viewing by event action plans 74
- All Systems and Devices, viewing
 - event action plans 74
 - managed systems 74
- anonymous command execution, restricting 204
- Apache Web Server, troubleshooting 344
- applications
 - See also process monitors
 - closing a process 198, 199
 - importing and exporting 233
 - running 201
- apply event action plan (DIRCMD) 294
- apply PM task (DIRCMD) 296
- apply threshold (DIRCMD) 295
- arrays, viewing information 226
- ASF
 - changing 305
 - configuring 147
 - generating events 56
 - monitoring power states 147
 - operating systems, supported 17
 - secure power management 147
- ASM interconnect 175
- ASM PCI adapter
 - Management Processor Assistant Agent 6
 - Management Processor Assistant task 175
 - Web-based Access System services 318
- ASM processor
 - accessing through IBM Director Console 32
 - managed object 33
 - Management Processor Assistant 175
 - Management Processor Assistant Agent 6
 - Web-based Access System services 318
- Asset ID
 - EEPROM 93
 - operating systems, supported 17
 - service 320
 - starting 93
 - troubleshooting 341
 - viewing information 93
- asset.dat file 93
- associations
 - example 40
 - menu 40
 - system names in blue 40
 - types of 39

associations (*continued*)

viewing

event action plans 73

groups 39

attributes, resource monitors 353

authentication keys 148

B

Basic System services 311

BFP files 249

bindings, enabling and disabling 322

blade servers

bay

local power-control button 109

USB assignment 109

BladeCenter chassis associations 40

blue indicator light 107

boot sequence 111

deployment policies 111

information 97

installing operating systems 120

KVM assignment 108

physical platform 33

powering on and off 108

problem 107

restarting 108

setting new owner 109

total BladeCenter units 29

viewing

in a BladeCenter chassis 40

information 106

start (boot) sequence 109

BladeCenter

chassis

blade servers associations 40

configuring 110

configuring automatically 95

managed object 33, 303

viewing information 106

component data 107

deployment infrastructure, multiple NICS 330

diagnostics 107

documentation xvi

event types 64

events 64

hardware

-specific events 64

status 107

I/O modules 109, 110

management module, changing settings 99

products, supported tasks 29

remote access 104

troubleshooting 330, 333

BladeCenter Assistant

See also BladeCenter Deployment wizard

changing subtasks 96

Configuration subtask

alert-forwarding profile 98, 99

configuring remote-alert settings 97

login profiles 104

BladeCenter Assistant (*continued*)

Configuration subtask (*continued*)

management module 99

network settings 99

overview 97

service processors 99, 104

SNMP settings 103

starting 95

viewing service processor data 97

configuring multiple servers 97

Deployment wizard subtask 110

establishing communication 96

interface 96

management module

changing settings 99

establishing communication 96

Management subtask

blade server 108

blade server start (boot) options 109

changing 108, 109

configuring 109

starting 95

viewing 106, 107, 110

managing BladeCenter units 95

overview 95

saving changes 97

selecting servers 96

service processor 96

Show/hide server tree 96

sorting information 97

Switch Management launch pad subtask 126

troubleshooting 339

viewing blade server information 97

XML file 110

BladeCenter chassis command (DIRCMD) 302

BladeCenter configuration command (DIRCMD) 301

BladeCenter Deployment wizard 110

chassis detect-and-deploy profile

creating 110, 122

overwriting 122

configuring

chassis 110

IP settings 117

deploying operating systems 120

deployment policies 111

management module

logging in to 113

network protocols, configuring 116

properties, configuring 95, 115

profiles

changing name of 122

creating (DIRCMD) 302

displayed in IBM Director Console

(illustration) 123

modifying 123

overview 110

switch modules

external ports, configuring 119

network protocols, configuring 119

user name and password, changing 118

- blue-indicator light
 - blade server problem 107
 - server problem 190
- books xvi
- bottlenecks
 - See also* Capacity Manager
 - See also* event action plans
 - automatic notification 129
 - creating
 - event action plan 130
 - event filter 130
 - event 128
 - identifying 127, 128
 - latent 129
 - performance analysis
 - function 129
 - icons 136
 - report 137
 - scheduling 129
 - types 128
- browser
 - See also* Microsoft Internet Explorer
 - See also* Netscape Navigator
 - Web-based Access 305
- building an event action plan 59

C

- caching software packages 234
- Caldera Open UNIX 197
- calendar pages, Scheduler 46
- Capacity Manager
 - See also* Resource Monitors
 - activating monitors 128
 - bottlenecks
 - adjusting thresholds 142
 - automatic notification 129
 - creating an event filter 130
 - detecting 129
 - identifying 128
 - types 128
 - determining potential solutions 129
 - diagnosing problems 129
 - discovery 127
 - forecasting performance 139
 - HTML 137
 - latent bottlenecks 129
 - monitors
 - types 127
 - viewing and activating 127
 - noninteractive tasks 40
 - operating systems, supported 26
 - overview 8, 127
 - performance forecast graph, viewing 139
 - reports
 - bottlenecks 129
 - changing settings 140
 - creating definitions 131
 - customizing 131
 - generating 131, 135
 - predefined definitions 131
- Capacity Manager (*continued*)
 - reports (*continued*)
 - reduced sampling frequency 132
 - saving and printing 137
 - setting graph display options 140
 - setting Report window display options 141
 - viewing details 137
 - viewing previously generated 138
 - Scheduler 129
- Category Editor 37
- CCSID 5026, troubleshooting 332
- cfgdb utility, troubleshooting 330, 333
- changing job properties, Scheduler 48
- chassis
 - configuring 110
 - detect-and-deploy profile
 - creating 110
 - definition 111
 - overwriting 122
 - intrusion, system-health information 317
 - troubleshooting managed objects 111
- chassis (DIRCMD) 303
- chassis command (DIRCMD) 303
- chassis list (DIRCMD) 304
- Chassis Membership association 39
- chassis subsystem list (DIRCMD) 304
- chassis subsystem type list (DIRCMD) 304
- Chinese characters incorrectly displayed 344
- Chinese-language systems, troubleshooting 345
- CIM Browser
 - CIM class instance
 - executing a method for 144
 - setting a property value for 144
 - operating systems, supported 17
 - shortcuts for classes and methods 145
 - starting 143
 - troubleshooting 339
 - viewing
 - CIM structure 143
 - information 144
- client, DIRCMD 277
- Cluster Membership association 39
- Cluster Systems Management 10
- clusters, viewing resources 193
- command-line
 - interface 277
 - programs 201, 215
- Common Information Model (CIM)
 - See also* CIM Browser
 - events 83, 316
 - queries 82
- community strings 323
- compatibility documents xvii
- Compatibility Documents for IBM Director 4.20 11, 13
- component
 - association, Rack Manager 208
 - service processor data 190
- computer name displayed incorrectly 341
- configuration
 - Asset ID service 320
 - changing 305, 320

- configuration (*continued*)
 - Date and Time service 322
 - Health service 322
 - Network service 322
 - remote 322
 - SNMP service 323
 - System Accounts service 323
- Configure Alert Standard Format
 - See ASF
- Configure SNMP Agent
 - See SNMP devices
- Console
 - See IBM Director Console
- CPU
 - See microprocessor
- create dynamic group (DIRCMD) 287
- create event action plan (DIRCMD) 293
- create PM task (DIRCMD) 296
- create static group (DIRCMD) 287
- criteria, creating groups 34, 36
- critical
 - events 61
 - events filter 61
 - threshold values 322
- CSV files
 - event-log events 158
 - inventory-query results 170
 - resource-monitor recording 222
 - Web-based Access 309
- Custom Package Editor 245
- customer support xvii
- customizing action types 67

D

- daemon.stderr file 332, 337
- data
 - importing 233
 - transmission 277
- database
 - configuration, troubleshooting 330, 333
 - files 309
 - function of 5
 - initialization error 330
 - troubleshooting
 - cfgdb utility 330
 - Oracle Server 330
- Date and Time service 322
- date and time, setting 322
- DBCS languages, troubleshooting 345
- default router, setting 331, 336
- defunct disk drives, locating 226
- delete groups (DIRCMD) 288
- delete objects (DIRCMD) 284
- deployment policies 111
- Deployment wizard
 - See BladeCenter Deployment wizard
- design strategies, event action plan 57
- Desktop Management Interface (DMI)
 - Asset ID 93
 - DMI Browser 153

- detect-and-deploy profile
 - creating 110
 - overwriting 122
- device
 - driver
 - Remote Supervisor Adapter II 340
 - SMBus, detection of (Windows) 327, 332, 337
 - drivers 314, 324
 - services
 - starting and stopping 198
 - viewing 197
- DHCP server 100, 181
- DIRCMD
 - access objects 284
 - add BC chassis 303
 - add systems 291, 297
 - add to static group 288
 - apply event action plan 294
 - apply PM task 296
 - apply threshold 295
 - BladeCenter chassis 302
 - BladeCenter chassis command 302
 - BladeCenter configuration 301
 - BladeCenter configuration command 301
 - BladeCenter Deployment wizard 110
 - bundle 278
 - chassis 303
 - chassis command 303
 - chassis list 304
 - chassis subsystem list 304
 - chassis subsystem type list 304
 - client 277
 - create dynamic group 287
 - create event action plan 293
 - create PM task 296
 - create static group 287
 - delete groups 288
 - delete objects 284
 - discover all 281
 - discover BC chassis 303
 - event command 292
 - event management 292
 - example 278, 280, 289, 290, 292, 294, 295, 296, 299, 301, 302, 303, 304
 - exit codes 280
 - filename 279
 - get 297
 - get bulk 298
 - get next 297
 - help 278, 281, 291, 292, 294, 295, 296, 300, 302, 303
 - inform 298
 - installing and accessing 277
 - k 279
 - list 281, 291, 292, 294, 295, 296, 300, 302, 303
 - list BC chassis 302
 - list dynamic group criteria 286
 - list event action plans 293
 - list event actions 293
 - list event types 292
 - list events 293

- DIRCMD (*continued*)
 - list filters 292
 - list group attributes 284
 - list group by attribute 285
 - list group members 286
 - list groups 284
 - list inventory values 286
 - list noninteractive tasks 288
 - list object attribute values 301
 - list object attributes 281, 282, 283, 300
 - list objects 281
 - list objects by attribute 300
 - list objects by attributes 283
 - list PM tasks 295
 - list systems 291, 297
 - list task activation status 289
 - list thresholds 294
 - log 279
 - managed system 291
 - management commands 278
 - Management Processor Assistant command 300
 - monitor command 294
 - native command 291
 - o 279
 - ping objects 284
 - pipe 279
 - process monitor 295
 - procmon command 295
 - remove from static group 288
 - rename objects 284
 - resource monitor 294
 - run task 288
 - server command 281
 - server management 281
 - set 298
 - set credentials 301
 - snmp command 296
 - snmp device 296
 - start discovery 291, 296
 - syntax conventions 277
 - trap 1 298, 299
 - trap 2 299
 - walk 299
 - xml file 302
 - XML file 110
 - DirWbs service 328, 329
 - disable encryption 50
 - discover all (DIRCMD) 281
 - discover BladeCenter chassis (DIRCMD) 303
 - discovery
 - default router, setting 331, 336
 - inventory 167
 - managed systems 32, 281, 291
 - parameters for SNMP devices 227
 - performance-analysis monitors 127
 - physical platforms 331
 - RXE-100 331
 - SNMP devices 227, 296
 - troubleshooting 330, 331
 - Discovery Preferences window 331
 - disk
 - bottleneck 128
 - monitoring usage 127
 - resource monitor 217
 - display requirements 327
 - distorted characters, troubleshooting 340
 - distribution
 - redirected
 - definition 234
 - exceeding available space 234
 - software 233
 - streamed, definition 233
 - Distribution Preferences window, troubleshooting 343
 - DMI Browser
 - creating a group class shortcut 154
 - operating systems, supported 17
 - setting attribute value 154
 - starting 153
 - viewing component information 153
 - documentation xvi
 - Domains/Workgroups association 39
 - downloading xviii
 - compatibility documents xvii
 - hardware compatibility information xviii
 - IBM Director code xviii
 - IBM Director publications xviii
 - systems-management software xviii
 - downtime, system 269
 - dragging, in IBM Director Console 32
 - Drives services 311
 - duplication event filter 62
 - dynamic groups
 - creating 34, 287
 - criteria, troubleshooting 334
 - definition 34
 - listing criteria 286
- ## E
- e-mail notification 70
 - EEPROM 93, 321
 - Electronic Service Agent 10
 - encryption
 - Administration 50
 - changing algorithm 50
 - enabling or disabling 50
 - keys 50
 - troubleshooting 331, 336
 - Web-based Access 306
 - environment
 - Director Information page 311
 - operating system variables 314
 - rack 207
 - server hardware status 309
 - small 305
 - environment (illustration) 4
 - environmental
 - data
 - BladeCenter 107
 - service processor 190
 - sensor events filter 61

- error message
 - 1306 328
 - 1722 327
 - 1921 328
 - an IO error occurred 336
 - event ID 2003 339
 - exception in thread "main" 337
 - IRQL_NOT_LESS_OR_EQUAL 328
- event
 - actions,
 - See event actions
 - application
 - changes state 197
 - viewing issues 315
 - availability 59
 - bottleneck 128
 - definition 55
 - filters,
 - See event filters
 - hardware issues, viewing 315
 - hardware status 164
 - hourly bottleneck 130
 - how they work 55
 - i5/OS-specific 56, 61, 64
 - IBM Director Server 57
 - Log All Events 56
 - management 55
 - management server 57
 - Message Browser 48
 - overview 55
 - PCI slot manager 92
 - process monitor 197, 200
 - processing
 - i5/OS-specific events 56
 - Windows-specific events 56
 - publishing 59
 - resource exhaustion 257
 - security problems, viewing 315
 - software issues, viewing 315
 - software rejuvenation 265
 - sources that generate 55
 - system issues, viewing 315
 - types
 - alert 55
 - availability 59
 - BladeCenter Assistant-specific events 64
 - BladeCenter hardware-specific events 64
 - i5/OS-specific events 56
 - resolution 55
 - resource monitor 217
 - viewing by 315
 - Windows-specific events 56
 - viewing details 155
 - Windows-specific 56, 61, 64
- event action plans
 - See *also* event management
 - alerts and resolutions, filtering 65
 - All Systems and Devices 74
 - applying to managed object 40, 294
 - association 40, 73
 - backing up 74
 - event action plans (*continued*)
 - Builder
 - building a new event action plan 60
 - customizing action types 67
 - IBM Director Console toolbar 32
 - icon 32
 - interface 60
 - building 59
 - category, filtering 65
 - creating 59, 293
 - date and time of events, filtering 65
 - design strategies 57
 - DIRCMD 294
 - displayed in IBM Director Console 334
 - event text, filtering 65
 - example 58
 - exporting
 - from IBM Director Server 74
 - to Archive 74
 - to HTML 74
 - to XML 74
 - extended attributes, filtering 65
 - grouping systems 58
 - how events work 55
 - importing to IBM Director Server 75
 - listing 293
 - Log All Events 56
 - managed group 72
 - managed systems
 - applying to 72
 - filtering 65
 - modifying 72
 - moving to another management server 74
 - naming conventions 55
 - overview 55
 - planning and designing 57
 - qualify filtering criteria 65
 - resource-monitor events 217
 - restricting 74
 - software rejuvenation 265
 - sources of events, filtering 64
 - structuring 58
 - successful implementation 55
 - system variables 65
 - systems 72
 - tree 72
 - troubleshooting 332, 334
 - urgency of events, filtering 64
 - user-defined variables, filtering 65
 - viewing
 - associations 73
 - groups 74
 - managed systems by association 40
 - managed systems by event action plan 40
 - wizard 60
 - See IBM Director 4.20 Installation and Configuration Guide
- event actions
 - adding 73
 - customizing 66, 69
 - deleting 73

- event actions *(continued)*
 - dragging 69
 - event data substitution variables 68
 - example 70, 71
 - history, enabling and viewing 73
 - listing 293
 - locating 69
 - Message Browser 48
 - modifying 73
 - testing 69
 - troubleshooting 332
 - types
 - available 66
 - customizing 67
 - listing 61
- event category 65
- event command (DIRCMD) 292
- event data substitution
 - definition 67
 - variables 68
- Event Filter Builder category 63
- event filters
 - adding 73
 - creating 63
 - definition 61
 - deleting 73
 - displaying new 66
 - dragging 66
 - duplication event filter 62
 - event action plan 65
 - event log 155
 - exclusion event filter 62
 - Hardware Predictive Failure events 61
 - listing 292
 - listing types 60
 - modifying 73
 - preconfigured types 60
 - qualify filtering criteria 65
 - severity levels 64
 - simple event filter 61
 - slot-manager event 92
 - software-rejuvenation events 265
 - structuring 59
 - system variables 65
 - threshold
 - event 62
 - event filter 62
- event log
 - BladeCenter management module 107
 - changing display options 155
 - changing settings 157
 - exporting events from 158
 - filtering events 155
 - full 338
 - listing contents of 293
 - Management Processor 190
 - operating systems, supported 17
 - service processor 190
 - status and VPD 107, 190
 - tasks 63
 - troubleshooting 327, 332, 337
- event log *(continued)*
 - viewing
 - entries 316
 - event details 155
 - filtering 315
 - event subscription, definition 56
 - event text 65
 - Event Viewer service 315
 - event-management bundle (DIRCMD) 292
 - examples
 - DIRCMD
 - BladeCenter chassis bundle 303
 - BladeCenter-configuration bundle 302
 - chassis bundle 304
 - creating a dynamic group 290
 - deleting groups 289
 - event-management bundle 294
 - listing managed objects 289
 - listing managed objects attributes 289
 - managed-system bundle 292
 - Management Processor Assistant bundle 301
 - overriding the default TCP/IP data link connection classes 280
 - piping data from one command to another 280
 - process-monitor bundle 296
 - resource-monitor bundle 295
 - running noninteractive tasks 290
 - snmp-device bundle 299
 - starting a session 278
 - event action
 - creating a pager notification 70
 - creating a phone notification 70
 - creating a pop-up message notification 71
 - creating an e-mail notification 70
 - event action plan 58
 - testing and tracking network resources 73
 - ticker-tape messages 67
- exclusion event filter 62
- execution history
 - jobs 46, 47
 - limiting number of job executions 45
 - process tasks 203
- exit codes, DIRCMD 280
- export
 - event action plans 74
 - event log events 158
 - groups 38
 - inventory-query results 170
 - resource-monitor recording 222
 - Software Distribution 233
 - software packages 233
 - threshold tasks 222
- extended attributes
 - event action plan 65
 - event filters 65
- extensions 10
 - Cluster Systems Management 10
 - definition 7
 - Electronic Service Agent 10
 - publishing events 59
 - Real Time Diagnostics 10

extensions (*continued*)
Remote Deployment Manager 9
Scalable Systems Manager 10
Server Plus Pack 8
Software Distribution (Premium Edition) 9, 233
Virtual Machine Manager 10

F

failover operation 82
fan
BladeCenter speed readings 107
failure, system-health information 317
service processor speed readings 190
viewing speed information 319
Fan Speeds service 319
fatal events filter 61
Fault Tolerant Management Interface (FTMI)
See Active PCI Manager
File Distribution Servers Manager window 342
File Transfer
disabling TCP/IP support 161
operating systems, supported 18
starting 159
synchronizing 160
target system, changing 160
transferring
between managed systems 160
files 159
UDP 161
file-distribution server
troubleshooting 343
viewing details about 254
files
abcwizard.dtd 126
asset.dat 93
BFP 249
CSV 158, 170, 222, 309
daemon.stderr 332, 337
HTML 137, 158, 170, 222, 273
IBM Director Agent.msi 327
ISS 237
MIB 229
MST 239
response 237
server.xml 344
ServiceNodeLocal.properties 335
SNMPServer.properties 228
software distribution update 235
SPB 249
tcpip.ini 341, 342
text 222
THRSHPLAN 222
tomcat.conf 344
transform 239
TWGagent.uid 335
TWGConsole.prop 337
twgmach.id 335
TWGServer.err 330
TWGServer.prop 332, 337
UpdateXpress 235

files (*continued*)
workers.properties 344
XML 110, 124, 158, 170, 222, 235, 236, 273
filtering events, troubleshooting 328
filters
See event filters
firewall access, troubleshooting 341, 342
FRU
data files 359
information, troubleshooting 340
Numbers services 312
viewing information 312
FTMI
See Active PCI Manager
FTP
alternative 159
IBM Support site 359
share
Software Distribution 234
troubleshooting (i5/OS) 343

G

Get (DIRCMD) 297
Get Bulk request (DIRCMD) 298
Get Next (DIRCMD) 297
GETFRU command 340, 359
glossary 369
group security profiles 267
grouping
managed objects 31
managed systems 58
groups
attributes 284
category-based 37
creating 321
definition 34
deleting 288
DIRCMD 35
distributing software packages 250
dragging a task 45
dynamic 286
creating 34, 287
overview 34
wildcard 35
example 34
exporting 38
fault tolerant 79
IBM Director Console interface 31
importing 38
interface 34
listing 284
monitoring resources 222
predicting resource exhaustion 263
removing static 288
security 323
static 288
creating 36, 287
overview 36
task-based 35
types 34

groups (*continued*)
 using criteria not in database 35
 viewing by event action plan 74

H

hard disk drive predictive failure alert, system-health information 317

hardware

 alerts, supported operating systems 18
 data 167
 information, viewing 320
 predictive failure events 61
 predictive failure events filter 61

hardware compatibility xviii

Hardware Status

 alert display 32
 critical event 310
 information event 310
 operating systems, supported 18
 service

 Director page 309
 pane 310
 tree view 308
 viewing 309

 summary 107, 190

 task 163

 icons 163
 viewing events 164

 viewing rack alerts 207

 warning event 310

harmless events filter 61

Health service

 alerts displayed 322
 configuring System Health output 316
 using 322

help (DIRCMD) 281, 291, 292, 294, 295, 296, 300, 302, 303

help files, Web-based Access 7, 309

help, IBM Director resources xvii

history, event action 73

hot-spare drives, viewing information 226

HTML files

 event action plan 74
 event-log events 158
 inventory-query results 170
 performance-analysis report 137
 resource-monitor recording 222
 system-availability report 273

I

I/O modules

 configuring IP settings 110
 Switch Management launch pad subtask 126
 viewing and configuring 109
 viewing VPD data 110

i5/OS

 Custom Package Editor 245
 events 56, 61, 64
 groups support 34

i5/OS (*continued*)

 OS/400 Restore Library Package wizard 243

 OS/400 Restore Licensed Program Package wizard 244

 OS/400 Restore Object Package wizard 244

 software distribution, troubleshooting 343

IBM Director

 BFP files 249

 File Package wizard 249

 software package block files 249

 Update Assistant 235

 updating 347

 user IDs 50

IBM Director Agent

BladeCenter

 chassis 29

 server 29

 browser 305

 function 5

 generating events 55

 IBM Director tasks 29

 imaging, troubleshooting 335

 installing and accessing DIRCMD 277

 license 6, 11

 Linux, compression of message logs 270

 managed objects 33

 managed systems 33

 operating systems, supported 13

 physical platform 33

 remote-access authorization 213

 secure communication with IBM Director Server 51

 troubleshooting

 installing 327, 328

 modifying an installation 327

 starting 327, 337

 uninstalling 329

 upgrading 328

IBM Director Agent features

 Management Processor Assistant Agent 6

 Remote Control Agent 7

 ServeRAID Manager 6

 SNMP Access and Trap Forwarding 7

 Web-based Access help files 7

IBM Director Agent Web Server (DirWbs) service 328, 329

IBM Director Agent.msi file 327

IBM Director Console

 actions 32

 associations, viewing 39

 authorizing users 50

 changing the view 32

 creating managed systems manually 32

 display requirements 327

 dragging 32

 Encryption Administration 50

 event action plan

 expanding 72

 exporting 74

 importing 75

 finding and viewing systems 32

 function 6

- IBM Director Console *(continued)*
 - groups 34
 - hardware-status alert display 32
 - icon indicating online or offline 31
 - installing and accessing DIRCMD 277
 - interface 31
 - license 6, 11
 - making associations 32
 - managed objects
 - grouping 31
 - overview 33
 - managed systems 33
 - marquee area 32
 - menu bar 33
 - Message Browser 48
 - modifying an installation, troubleshooting 327
 - physical platform 33
 - pop-up messages 264
 - requesting access to a managed system 31
 - right-clicking 32
 - setting
 - options 31
 - preferences 31
 - setting options 31
 - sorting managed systems 32
 - starting tasks 31
 - supported operating systems 15
 - system names in blue 40
 - ticker-tape messages 32
 - toolbar 32
 - troubleshooting
 - BladeCenter 333
 - data displayed in windows 333
 - deleted physical platform object displayed 333
 - discovered systems not displayed 331, 336
 - logon failure 337
 - managed system access denied 335, 337
 - managed system icon with question mark 334
 - managed systems not displayed 335
 - starting 336
 - time zone error 337
 - User event action 48
 - viewing
 - alerts 48
 - associations 31
 - inventory 32
 - scheduled jobs information 46
- IBM Director Console.msi file 327
- IBM Director Hardware and Software Compatibility
 - document xvii
- IBM Director Multiplatform, updating 347
- IBM Director Server
 - determining if running 333
 - DIRCMD 35, 277
 - encryption enabled, troubleshooting 332
 - events, alert messages 316
 - exporting event action plan 74
 - function 5
 - i5/OS, troubleshooting running on 332
 - importing event action plan
 - from archive export 75
- IBM Director Server *(continued)*
 - importing event action plan *(continued)*
 - management server 74
 - installing DIRCMD 277
 - license 5, 11
 - processing events 57
 - redirected distribution 234
 - secure communication with managed objects 51
 - SSL enabled, troubleshooting 332
 - supported operating systems 13
 - troubleshooting
 - database 330
 - event log error 339
 - installing 327
 - Microsoft Jet 329
 - starting 327, 332
 - Telnet 330
 - viewing event details 155
- IBM Director Support Program service (TWGIPC) 328, 329
- IBM eServer Information Center xviii
- IBM Support FTP site 312, 359
- IBM systems-management software
 - downloading xviii
 - overview xvii
- IBM Web sites
 - eServer Information Center xviii
 - Redbooks xvii
 - ServerProven xviii
 - Support xviii
 - Systems Management Software xviii
 - xSeries Systems Management xviii
- icons
 - Discover All Managed Systems 32
 - Event Action Plan Builder 32
 - hardware status 163
 - Message Browser 32
 - online or offline 31
 - padlock 31
 - performance analysis 136
 - Resource Monitors status 219
 - Scheduler 32
 - Slot Manager 87
 - User Administration 32
- illustrations
 - IBM Director environment 4
 - IBM Director software components 5
- imaging IBM Director Agent, troubleshooting 335
- import
 - applications and data 233
 - event action plans, Archive export 75
 - files for software distribution 234
 - groups 38
 - Software Distribution 233
 - threshold tasks 222
- in-band alerts, SNMP traps 7
- inform (DIRCMD) 298
- Information page 311
- Information services, Web-based Access 308, 310
- input ports information, viewing 314
- installation, troubleshooting 327

- InstallShield
 - Package wizard 237
 - Professional 237
 - unattended installation 238
 - Web site 238
- insufficient data space, troubleshooting 341
- insufficient disk space, troubleshooting 339
- insufficient memory, troubleshooting 334
- integrated SCSI controller with RAID capabilities 225
- integrated systems management processor
 - See ISMP
- interface
 - BladeCenter Assistant 96
 - Event Action Plan Builder 60
 - groups 34
 - hardware-status alert display 32
 - IBM Director Console 31
 - Management Processor Assistant 176
 - marquee area 32
 - menu bar 33
 - ticker-tape messages 32
 - Web-based Access 308
- interim fixes xvii
- invalid data values, troubleshooting 338
- Inventory 359
 - attributes, creating groups 34, 36
 - Basic System service 311
 - collecting data 167
 - Console, viewing 32
 - data
 - using 321
 - viewing 167
 - discovery 167
 - Drives service 311
 - FRU Numbers service 312
 - listing database values 286
 - Memory service 313
 - Multimedia service 313
 - Operating System service 313
 - operating systems, supported 18
 - Ports service 314
 - queries
 - creating custom 168
 - editing custom 169
 - exporting results to a file 170
 - predefined 167
 - rack data 208, 209
 - scheduling collections 167
 - software dictionary
 - adding an entry 170
 - matches 171
 - overview 167, 170
 - software inventory, viewing 170
 - troubleshooting 338, 340
- inventory errors, troubleshooting 340
- IPMI baseboard management controller
 - based systems 318
 - generating events 56
 - MPA Agent 6
- IPX Network IDs association 39
- iSeries Information Center 332

- ISMP
 - accessing through IBM Director Console 32
 - Management Processor Assistant 175
 - MPA Agent 6
 - physical platform 33
 - System services 318
- ISS files 237

J

- Japanese-language systems, troubleshooting 343, 345
- Java
 - Foundation Class/Swing library (JFC/Swing) 307
 - Web site 305
- job
 - definition 40
 - viewing managed systems 40
- JRE exceptions, troubleshooting 334

K

- key combinations, sending 214
- keyboard
 - accessing interface 33
 - Software Rejuvenation shortcuts 266
- keys, authentication 148
- Korean-language systems, troubleshooting 343, 345
- KVM 106, 108

L

- LAN adapter, bottleneck 128
- LAN Leash, system-health information 317
- latent bottleneck, definition 129
- LED
 - Blink function 87
 - slot error status 86
 - viewing 107, 190
- license
 - IBM Director Agent 6, 11
 - IBM Director Console 6, 11
 - IBM Director Server 5, 11
- light path diagnostics, viewing 107, 190
- Linux, RPM Package wizard 241
- list (DIRCMD) 281, 291, 292, 294, 295, 296, 300, 302, 303
 - list BladeCenter chassis (DIRCMD) 302
 - list dynamic group criteria (DIRCMD) 286
 - list event action plans (DIRCMD) 293
 - list event actions (DIRCMD) 293
 - list event types (DIRCMD) 292
 - list events (DIRCMD) 293
 - list filters (DIRCMD) 292
 - list group attributes (DIRCMD) 284
 - list group by attribute (DIRCMD) 285
 - list group members (DIRCMD) 286
 - list groups (DIRCMD) 284
 - list inventory values (DIRCMD) 286
 - list noninteractive tasks (DIRCMD) 288
 - list object attribute values (DIRCMD) 301
 - list object attributes (DIRCMD) 281, 282, 283, 300

- list objects (DIRCMD) 281
- list objects by attribute (DIRCMD) 300
- list objects by attributes (DIRCMD) 283
- list PM tasks (DIRCMD) 295
- list systems (DIRCMD) 291, 297
- list task activation status (DIRCMD) 289
- list thresholds (DIRCMD) 294
- Load All Events 316
- loader timeout information, viewing 319
- Lock functions 87
- locked files
 - troubleshooting 329
 - Web-based Access 329
- Log All Events 56, 60
- log files, system 269
- logical disk drives
 - troubleshooting 339
 - viewing information 226, 311
- login profiles
 - BladeCenter 104
 - dial-in 188
- logs 293
- low disk space, system-health information 317

M

- managed device
 - See also* SNMP devices
 - definition 33
- managed objects
 - creating 291
 - definition 33
 - deleting 284
 - listing 281
 - renaming 284
 - secure communication with IBM Director Server 51
- managed systems
 - access request denied 335, 337
 - additional information, viewing 40
 - behind firewall, troubleshooting 341, 342
 - bottlenecks, determining 129
 - configurations, changing 320
 - creating manually in IBM Director Console 32
 - definition 3, 33
 - DIRCMD 284
 - discovery 32
 - distributing software 233
 - dragging a task 45
 - firewall access 340
 - forecasting performance 139
 - gathering information 311
 - hardware data 167
 - information services 308, 310
 - invalid data values 338
 - issuing a command 203
 - managed object 33
 - monitoring resources 127, 222
 - performance analysis 127
 - power states 147
 - predicting resource exhaustion 263
 - real-time information 305

- managed systems (*continued*)
 - remote access 211, 215, 305
 - requesting access 31
 - resource monitor 217
 - restarting 191, 257
 - running Windows, troubleshooting 338
 - software data 167
 - software distribution 233
 - statistics 220
 - tasks services 308
 - troubleshooting 337
 - encryption 331, 336
 - resource-monitor information 338
 - time zone error 337
 - viewing
 - CIM structure 143
 - information 320
 - viewing by
 - event action plan 40, 73
 - jobs already run 40
 - resource monitors 40
 - scheduled jobs 40
- management commands (DIRCMD)
 - password 278
 - server 278
 - userID 278
- management console
 - definition 4
 - insufficient disk space 342
 - troubleshooting 333
- management module
 - changing settings 99
 - logging in to 113
 - network protocols, configuring 116
 - properties, configuring 115
- management processor
 - See also* service processors
 - definition 33
 - generating events 56
 - managed object 33
- Management Processor Assistant
 - Agent
 - installing 318
 - overview 6
 - physical platform 33
 - turning servers on and off 191
 - BladeCenter hardware-specific events 64
 - changing subtasks 176
 - Communications configuration subtask
 - configuring service processor communication 177
 - starting 175
 - viewing IP settings 178
 - Configuration subtask
 - alert-forwarding profile 179
 - configuring 181, 186
 - configuring alert settings 179
 - dial-in login profiles 188
 - PPP settings 185
 - restarting service processor 185
 - sending a test alert 180

- Management Processor Assistant *(continued)*
 - service processors 181
 - SNMP settings 184
 - starting 175
 - viewing service processor data 179
 - configuring multiple servers 177
 - distorted characters, troubleshooting 340
 - establishing communication 176
 - interface 176
 - Management subtask, viewing 189, 190, 191
 - operating systems, supported 20
 - out-of-band communication 178
 - overview 6
 - saving changes 177
 - selecting servers 176
 - Server Management subtask
 - restarting managed system 191
 - server start (boot) options 191
 - servers 191
 - starting 175
 - viewing 189, 190
 - service processor 176
 - Show/hide server tree 176
 - sorting information 177
 - starting 175
 - System Health Monitoring 191
 - troubleshooting 328, 340, 345
 - viewing service processor information 179
 - Management Processor Assistant (DIRCMD) 300
 - Management Processor Assistant command (DIRCMD) 300
 - Management Processor Event Log 319
 - Management Processor VPD 319
 - management server
 - backing up event action plans 74
 - connection to client 277
 - definition 3
 - Hardware Status service 308, 309
 - logon failure 337
 - moving event action plans 74
 - troubleshooting 329
 - managing systems running IBM Director Agent 3.1 or later 11
 - marquee area, ticker-tape messages 32
 - Mass Configuration
 - applying to a group 52
 - Asset ID 93
 - Configure ASF 147
 - creating a profile 51
 - managing profiles 52
 - Network Configuration 195
 - overview 51
 - troubleshooting 341
 - memory
 - bottleneck 128
 - DIMM information 191
 - monitoring usage 127
 - PFA, system-health information 317
 - services 313
 - upgrade options 313
 - usage resource monitor 217
 - memory *(continued)*
 - viewing information 313
 - menu bar 33
 - Message Browser
 - displaying all alerts 48
 - icon 32
 - starting 48
 - viewing alerts 48
 - message digest 5 method, troubleshooting 335, 337
 - message logs, compression 270
 - Mgmt Proc Event Log service 319
 - Mgmt Processor Vital Product Data service 319
 - MIB files
 - attribute values, troubleshooting 341, 342
 - compiling 229
 - microprocessor
 - bottleneck 128
 - monitoring utilization 127
 - Microsoft
 - Cluster Browser
 - operating systems, supported 20
 - starting 193
 - Cluster Server (MSCS) 193
 - Internet Explorer
 - troubleshooting 344
 - Web-based Access 305
 - Knowledge Base Article
 - 267831 339
 - 825236 328
 - 827439 338
 - 830459 338
 - Management Console 7, 305, 307
 - software transformation files 239
 - Windows 2000 Service Pack 4 338, 339
 - Windows Installer Package wizard 239
 - minor events filter 61
 - modem, configuring settings 186
 - Monitor
 - Event Viewer service 315
 - System Health service 316, 318
 - monitor command (DIRCMD) 294
 - MPA
 - See Management Processor Assistant
 - MST files 239
 - multi-node server, managed object 33
 - multimedia adapters information, viewing 313
 - Multimedia service 313
 - multiple NICs, troubleshooting 330
- ## N
- native command (DIRCMD) 291
 - Netscape Navigator
 - troubleshooting 344, 345
 - Web-based Access 305
 - network
 - information, viewing 322
 - preventing congestion 234
 - resources, testing and tracking 73
 - settings, configuring 99, 181

- network (*continued*)
 - shares
 - software distribution fails 234
 - troubleshooting 342
 - utilization, monitoring 127
- network adapter attribute names, troubleshooting 341
- Network Configuration 195
 - operating systems, supported 20
 - troubleshooting 341
- Network service 322
- network timeout value, modifying 335
- NIC, system-health information 317, 318
- non-English language keyboard, troubleshooting 341
- noninteractive task, definition 40
- notifications
 - definition 55, 225
 - e-mail 70
 - message window 316
 - pager 70
 - phones 70
 - pop-up message 71
 - system failure 147
 - viewing 226
- NVRAM information, viewing 319

O

- Object Type association 39
- operating system
 - compatibility xvii
 - information, viewing 313
 - resources 257
 - services information, viewing 314
 - support for tasks 15
 - supported 13
 - timeout information, viewing 319
- Operating System services 313
- optional commands (DIRCMD) 278
- options, setting 31
- Oracle Server, troubleshooting 330
- Oracle TCP/IP listener 330
- OS/400
 - See* i5/OS
- out-of-band communication 178
- outages
 - avoiding 257
 - identifying system 269
- output ports information, viewing 314

P

- padlock icon 31
- pager notification 70
- PCI adapter
 - managing 79
 - optimization solutions 89
 - performance issues 88
 - troubleshooting 339
- performance analysis
 - bottlenecks, detecting 129
 - CPU utilization 127

- performance analysis (*continued*)
 - disk usage 127
 - forecasting 139
 - forecasting trends 127
 - icon 136
 - latent bottlenecks 129
 - memory usage 127
 - network utilization 127
 - PCI
 - analyzing 88
 - bus, slots, and adapters 83
 - issues 88
 - optimizing 89
 - potential solutions, determining 129
 - problems, diagnosing 129
 - report
 - details 137
 - recommendations 137
 - resource-management planning 127
 - PET, generating events 56
 - phone notification 70
 - physical disk drives, viewing information 226, 311
 - physical platform
 - blade server 33
 - definition 33
 - deleting from IBM Director Console 34
 - discovery of 331
 - IBM Director Agent 33
 - managed object 33
 - Physical Platform - Remote I/O Enclosures
 - association 39
 - ping objects (DIRCMD) 284
 - planning and designing event action plans 57
 - platform managed object 333
 - Platform Membership association 39
 - policies, deployment 111
 - pop-up message notification 71
 - port, Web-based Access 306, 307
 - Ports service 314
 - POST timeout information, viewing 319
 - power
 - monitoring states 147
 - off 324
 - off timeout information, viewing 319
 - supply
 - viewing BladeCenter readings 107
 - viewing service processor readings 190
 - supply failure, system-health information 317
 - viewing information 319
 - Power Management
 - See also* ASF
 - operating systems, supported 22
 - Power/Restart Activity service 319
 - PPP, configuring settings 185
 - predefined components, Rack Manager 208
 - Prediction Configuration wizard 263
 - preferences, setting 31
 - presence check 284
 - problem
 - determination 143
 - solving 327

- Process Management
 - See also* process monitors
 - applying 201
 - closing an application (process) 198, 199
 - creating process monitors 200
 - device services, starting and stopping 198
 - DIRCMD 296
 - GETFRU command 360
 - issuing a command on a managed system 203
 - operating systems, supported 24
 - process monitors 197
 - process tasks
 - creating 202
 - overview 201
 - running 203
 - Remove Process Monitors 201
 - removing 201
 - restricting anonymous command execution 204
 - Scheduler 201
 - security 201, 204
 - viewing 201
 - viewing information 197
 - working with Windows services 198
- process monitors
 - See also* Process Management
 - applying 201, 296
 - creating 200, 296
 - event 55
 - noninteractive tasks 40
 - removing 201
 - viewing 201
- process, noninteractive tasks 40
- processor
 - See also* BladeCenter Assistant
 - See also* management module
 - See also* Management Processor Assistant
 - PFA, system-health information 317
 - removed, system-health information 317
 - resource monitor 217
- procmon command (DIRCMD) 295
- Profile Builder
 - See* Mass Configuration
- profiles
 - alert forwarding 98, 99, 179
 - BladeCenter Deployment wizard
 - changing name of 122
 - displayed in IBM Director Console (illustration) 123
 - overview 110
 - dial-in login 188
 - group security 267
 - login 104
 - Mass Configuration 51
 - SNMPv3 231
 - user security 267
- programs
 - See* command-line programs
- publications xvi

R

- Rack Manager
 - component association 208
 - creating and configuring a rack 209
 - existing rack, adding and removing components 209
 - interface 207
 - inventory data 208, 209
 - operating systems, supported 26
 - overview 9
 - starting 207
 - viewing information 208
- Rack Membership association 39
- rack, managed object 33
- RAID arrays, monitoring and managing 6
- Real Time Diagnostics 10
- Red Hat, RPM Package wizard 241
- Redbooks xvii
- redirected distribution
 - definition 234
 - exceeding available space 234
 - IBM Director Server 234
- redirector share, troubleshooting 342
- releases, new 347
- remote
 - See also* Remote Control
 - See also* Remote Session
 - access 104, 188, 203
 - access authorization 213
 - configuration 322
 - I/O enclosure, managed object 33
 - secure power management 147
- Remote Access Connection Manager service, troubleshooting 338
- Remote Control
 - Agent, overview 7
 - changing refresh rates 212
 - changing states 212
 - cutting and pasting 214
 - modes 211
 - operating systems, supported 24
 - playing a recorded session 213
 - preventing user access 213
 - recording a session 213
 - restricting usage 213
 - sending key combinations 214
 - starting 211
 - troubleshooting 341
- Remote Deployment Manager
 - creating a physical platform 33
 - overview 9
- remote management
 - See* ASF
- Remote Session
 - cutting and pasting 215
 - operating systems, supported 24
- Remote Supervisor Adapter
 - configuring, monitoring, and managing 175
 - device driver 340
 - documentation xvi
 - FRU information 312

- Remote Supervisor Adapter *(continued)*
 - Management Processor Assistant 6
 - physical platform 33
 - System services available 318
 - troubleshooting 340
- remove from static group (DIRCMD) 288
- rename objects (DIRCMD) 284
- reports
 - bottlenecks 129
 - frequency of outages 270
 - generating 321
 - PCI performance analysis 90
 - performance analysis
 - details 137
 - generating 131
 - recommendations 137
 - system
 - availability 270
 - outages 270
 - uptime 270
- request access 31
- resolution
 - definition 55
 - filtering 65
- resource
 - critical system 353
 - exhaustion, definition 257
 - utilization, viewing 265
- Resource Monitors
 - applied to managed systems 40
 - association 40
 - attributes 217, 353
 - Capacity Manager 127
 - DIRCMD 294, 295
 - event action plan 217
 - events 55
 - exporting a recording 222
 - monitoring on multiple systems 222
 - monitoring trends 127
 - operating systems, supported 24
 - recording 220, 221
 - setting thresholds 217
 - status icons 219
 - subtasks
 - All Available Recordings 217
 - All Available Thresholds 217
 - threshold tasks, exporting and importing 222
 - thresholds 294
 - ticker-tape messages 223
 - troubleshooting 341
 - viewing
 - available 217
 - data on the ticker tape 223
 - graph of recording 221
 - managed systems 40
 - managed systems by association 40
 - thresholds 220
- resource-monitor information, troubleshooting 338
- response file 237
- restart
 - information 319

- restart *(continued)*
 - Web-based Access 324
- right-click, in IBM Director Console 32
- RPM Package wizard 241
- RPM packages, troubleshooting 338, 340
- run task (DIRCMD) 288
- RXE-100 Remote Expansion Enclosure
 - configuring using SSM 10
 - managed object 33

S

- salt values, required lengths 335, 337
- Scalable Partitions Membership association 39
- Scalable Systems Manager
 - See SSM
- Scalable Systems Membership association 39
- schedule a task
 - dragging onto a managed system or group 45
 - specifying a date and time 42
- scheduled job
 - types 47
 - viewing information 46
- Scheduler
 - Activations association 40
 - association 40
 - changing properties 48
 - delaying execution on unavailable systems 44
 - distributing software packages 250
 - executing
 - in client time zone 45
 - on systems added to the target group 44
 - icon 32
 - inventory collection 167
 - job, definition 40
 - Jobs association 40
 - limiting number of job executions 45
 - performance analysis 129
 - process monitors 201
 - running
 - noninteractive tasks 40
 - programs and processes 201
 - saving changes not permitted 48
 - scheduling a task
 - Console 45
 - directly 41
 - Software Distribution 250
 - starting 41
 - using a group as the target 44
 - viewing
 - execution history logs 48
 - job information 47
 - job properties 48
 - job schedules 46
 - managed systems by association 40
 - scheduled job history information 48
 - scheduled job information 46
- secure remote management
 - See ASF
- Secure Sockets Layer (SSL) 277
- secured system 31

- security
 - anonymous command execution 204
 - between IBM Director Server and managed objects 51
 - events filter 61
 - file transfer 159
 - process management 201
 - profiles 267
 - remote administration 323
 - remote control 213
 - software packages 252
 - Windows NT password 306, 308
- serial ATA controllers with integrated RAID 225
- Server
 - See IBM Director Server
- server command (DIRCMD) 281
- server keys, creating new 50
- Server Plus Pack
 - Active PCI Manager 79
 - Capacity Manager 127
 - installation 8
 - operating systems, supported 26
 - overview 8
 - purchasing 8
 - Rack Manager 207
 - Software Rejuvenation 257
 - System Availability 269
- Server Preferences window 338, 340
- server status 189
- Server Timeouts service 319
- server-management bundle (DIRCMD) 281
- server.xml file 344
- ServeRAID FRU information 312
- ServeRAID inventory missing 340
- ServeRAID Manager 6
 - controllers and adapters 225
 - integrated SCSI controller with RAID capabilities 225
 - operating systems, supported 24
 - overview 6
 - starting 225
 - viewing alerts 226
- servers
 - blue-indicator light 190
 - DHCP 100, 181
 - file distribution 254
 - problem 190
 - restarting 191
 - software distribution 253, 254
 - turning on and off 191
 - viewing and changing start (boot) options 191
 - viewing information 189
- service packs xvii
- service processors
 - See also ASM processor, ASM PCI Adapter, ISMP, and Remote Supervisor Adapter
 - See also BladeCenter Assistant
 - See also Management Processor Assistant
 - communicating with Director Server
 - in-band 6
 - service processors (*continued*)
 - configuring
 - communication 177
 - network settings 99, 181
 - documentation xvi
 - generating events 56
 - hardware summary 190
 - managing 6
 - out-of-band communication 178
 - remote access 188
 - restarting 104, 185
 - viewing
 - data 97, 179, 190
 - device driver information 319
 - event log 190
 - firmware information 319
 - information 179
 - IP settings 178
 - NVRAM information 319
 - ServiceNodeLocal.properties file 335
 - services 197
 - session support, disabling 341, 342
 - set (DIRCMD) 298
 - set credentials (DIRCMD) 301
 - setting
 - date and time 322
 - rejuvenation options 262
 - threshold values 322
 - trap destination addresses 323
 - settings
 - Web-based Access 305
 - shared directories, types 234
 - shut down 324
 - Shutdown service 324
 - silent installations
 - See unattended installations
 - simple event filter
 - definition 61
 - expanding 60
 - predefined filters 61
 - Simplified-Chinese systems, troubleshooting 345
 - slot error status 86
 - Slot Manager
 - See Active PCI Manager
 - SNMP
 - configuring settings 103, 184
 - generating events 56
 - SNMP Access and Trap Forwarding
 - overview 7
 - SNMP agents 331
 - SNMP Browser
 - See SNMP devices
 - snmp command (DIRCMD) 296
 - snmp device (DIRCMD) 296
 - SNMP devices
 - compiling a MIB file 229
 - configuring
 - attributes 229
 - trap forwarding 228
 - creating 228, 297
 - definition 3

- SNMP devices (*continued*)
 - DIRCMD 296, 297
 - monitoring performance 229
 - operating systems, supported 17, 24
 - overview 227
 - setting attribute value 231
 - setting discovery parameters 227
 - SNMPv3 profile 231
 - troubleshooting 331, 341, 342
 - viewing attributes 229
- SNMP service 323, 331
- SNMP System Object ID association 39
- SNMP traps
 - alert messages 316
 - configuring forwarding 228
 - event log 227
 - troubleshooting 342
- SNMPServer.properties file 228
- software
 - aging, definition 257
 - data 167
 - distribution server 253, 254
 - package block file 249
 - transformation file 239
- software components (illustration) 5
- Software Distribution
 - AIX InstallP Package wizard 242
 - association 40
 - caching 234
 - changing server preferences 253
 - Custom Package Editor 245
 - Director Update Assistant 235
 - distribution fails on network shares 234
 - editing a software package 252
 - exceeding available space 234
 - exporting software package 252
 - file-distribution server 254
 - groups 250
 - importing files using wizards 234
 - InstallShield Package wizard 237
 - Microsoft Windows Installer Package wizard 239
 - network congestion 234
 - OS/400 Restore Library Package wizard 243
 - OS/400 Restore Licensed Program Package wizard 244
 - OS/400 Restore Object Package wizard 244
 - overview 233
 - Premium Edition
 - features 233
 - overview 9
 - troubleshooting 343
 - redirected distribution 234
 - restricting access to software package 252
 - RPM Package wizard 241
 - scheduling distributions 250
 - Software Package association 40
 - software-package details 254
 - Standard Edition features 233
 - streamed distribution 233
 - troubleshooting
 - file-distribution server 343
- Software Distribution (*continued*)
 - troubleshooting (*continued*)
 - managed system behind firewall 342
 - package creation 342
 - unattended installation 238
 - update file 235
 - UpdateXpress 235
 - viewing
 - creation and distribution status 253
 - managed systems by association 40
 - software package contents 252
 - software-distribution history 253
 - XML file 235
 - software packages
 - caching 234
 - categories
 - creating 250
 - editing 251
 - distributing 250
 - editing 252
 - exporting 252
 - importing
 - BFP files 249
 - Director File Package wizard 249
 - SPB files 249
 - importing and building
 - AIX InstallP Package wizard 242
 - Custom Package Editor 245
 - Director Update Assistant 235
 - InstallShield 237
 - ISS files 237
 - MST files 239
 - OS/400 Restore Library Package wizard 243
 - OS/400 Restore Licensed Program Package wizard 244
 - OS/400 Restore Object Package wizard 244
 - RPM Package wizard 241
 - Window Installer 239
 - XML files 236
 - inventory tracking 170
 - restricting access 252
 - SPB format, troubleshooting 343
 - types 233
 - viewing
 - contents 252
 - creation and distribution status 253
 - details 254
 - software-distribution history 253
- Software Rejuvenation
 - creating schedule filters 261
 - deleting schedules 261
 - editing schedules 261
 - keyboard shortcuts 266
 - operating systems, supported 26
 - options, setting 262
 - overview 9
 - prediction
 - configuring 263
 - ending 265
 - resource exhaustion 263
 - starting 265

- Software Rejuvenation (*continued*)
 - resource utilization, viewing 265
 - scheduling
 - managed systems 259
 - service 260
 - service rejuvenation, configuring 258
 - starting 257
- solving problems 327
- SPB files 249
- spreadsheet files 309
- SSL
 - See Secure Sockets Layer
- SSM, overview 10
- start discover (DIRCMD) 296
- start discovery (DIRCMD) 291
- starting
 - programs with event action plans 55
 - tasks, in IBM Director Console 32
 - Web-based Access 305
- static groups
 - adding to 288
 - creating 36, 287
 - definition 36
 - removing from 288
- static partition, managed object 33
- statistics, resource monitors 222
- Status association 39
- storage events filter 61
- streamed distribution, definition 233
- structure
 - event action plan 58
 - event filters 59
- subscription services 347
- Sun Web site 305
- switch modules
 - configuring IP settings 110
 - external ports, configuring 119
 - network protocols, configuring 119
 - Switch Management launch pad 126
 - user name and password, changing 118
 - viewing and configuring 109
 - viewing VPD data 110
- synchronizing files, directories, or drives 160
- System
 - Fan Speeds service 319
 - Mgmt Proc Event Log service 319
 - Mgmt Processor Vital Product Data service 319
 - Power/Restart Activity service 319
 - Server Timeouts service 319
 - Temperatures service 319
 - Voltages service 319
- System Accounts
 - adding a group 267
 - deleting a user 267
 - editing a group 268
 - operating systems, supported 24
 - service 323
 - task 267
- System Availability
 - changing
 - graph dates 271

- System Availability (*continued*)
 - changing (*continued*)
 - settings criteria 272
 - comparing and contrasting views 271
 - HTML file 273
 - operating systems, supported 26
 - overview 9
 - saving report 273
 - starting 269
 - system outages 269
 - XML file 273
- system board voltage 319
- system failure 147
- System Health Monitoring 191
- System Health service 316, 318
- System Management Server, alert messages 316
- system names in blue 40
- System Status, setting and clearing 48
- System Updates service 324
- system variables
 - changing 73
 - event action plan 65
 - event filters 65
 - viewing 73
- system-environment factors, viewing information 316, 318

T

- task bar icons (Windows) 333, 336
- Task Based Group Editor 35
- tasks
 - Active PCI Manager 79
 - Asset ID 93
 - BladeCenter Assistant 95
 - Capacity Manager 40, 127
 - CIM Browser 143
 - Configure Alert Standard Format 147
 - DMI Browser 153
 - Encryption Administration 50
 - event action plans 55
 - event log 63, 155
 - File Transfer 159
 - Hardware Status 163
 - IBM Director Console interface 31
 - Inventory 167
 - Mass Configuration 51
 - Message Browser 48
 - Microsoft Cluster Browser 193
 - Network Configuration 195
 - noninteractive
 - definition 40
 - listing 288
 - running 288
 - operating systems, supported 15
 - performing on multiple groups 34
 - Process Management 40, 197
 - process monitors 40
 - publishing events 59
 - Rack Manager 207
 - Remote Control 211

- tasks (*continued*)
 - Remote Session 215
 - Resource Monitors 217
 - Scheduler
 - Console toolbar 32
 - running noninteractive tasks 40
 - ServeRAID Manager 225
 - services, Web-based Access 308
 - SNMP Browser 229
 - Software Distribution 233
 - Software Rejuvenation 257
 - System Accounts 267
 - System Availability 269
 - System Status 48
 - User Administration 49
 - viewing managed systems by
 - event action plan 40
 - jobs already run 40
 - jobs scheduled to be run 40
 - resource monitors 40
 - Web-based Access 308, 320
- TCP/IP
 - Addresses association 39
 - data link connection 277
 - disabling support 161
 - Host Names association 39
 - Routers/DNS association 39
- tcpip.ini file 341, 342
- temperature
 - out of specification, system-health information 317
 - viewing
 - BladeCenter readings 107
 - readings 319
 - service processor readings 190
 - thresholds 319
- Temperatures service 319
- terminology 361
 - alert 55
 - event 55
 - event data substitution 67
 - event subscription 56
 - extensions 7
 - IBM Director 361
 - job 40
 - managed device 33
 - managed object 33
 - managed system 3, 33
 - management console 4
 - management server 3
 - noninteractive task 40
 - notification 55
 - redirected distribution 234
 - resolution 55
 - SNMP device 3
 - streamed distribution 233
- test and track network resources
 - example 73
- test event action 69
- text
 - files 222
 - resource-monitor recording 222
- threshold event
 - filter 62
 - simple event filter 61
- threshold values, setting 322
- thresholds
 - event action plans 55
 - performance monitors 128
 - resource monitor 217, 294
 - resource-monitor tasks, exporting and importing 222
 - temperature 319
 - voltages 319
- THRSHPLAN files 222
- ticker-tape messages
 - example 67
 - marquee area 32
 - Message Browser 48
 - resource-monitor data 223
 - Software Rejuvenation 264
- timeout, troubleshooting 332
- Tivoli Enterprise Console events, alert messages 316
- tomcat.conf file 344
- toolbar
 - Discover All Managed Systems 32
 - See IBM Director 4.20 Installation and Configuration Guide
 - Event Action Plan Builder
 - See event action plans
 - Message Browser
 - See Message Browser
 - Scheduler
 - See Scheduler
 - User Administration
 - See IBM Director 4.20 Installation and Configuration Guide
 - See User Administration
- Tools services, Shutdown 324
- trademarks 368
- Traditional-Chinese systems, troubleshooting 345
- transform file 239
- trap 1(DIRCMD) 298, 299
- trap 2 (DIRCMD) 299
- trap destination addresses, setting 323
- troubleshooting
 - Active PCI Manager 339
 - Asset ID 341
 - BladeCenter discovery 330
 - CCSID 5026 332
 - cfgdb utility 330
 - Chinese characters incorrectly displayed 344
 - CIM Browser 339
 - database configuration 330
 - database full 329
 - database initialization error 330
 - DBCS languages, troubleshooting 345
 - discovery 330, 331
 - dynamic groups criteria 334
 - encryption 331, 336
 - event action plans 332, 334
 - event actions 332
 - event ID 2003 339

- troubleshooting (*continued*)
 - event log error after restarting 339
 - event log full 338
 - FRU information 340
 - IBM Director Agent 337
 - installing 327, 328
 - modifying 327
 - starting 327, 337
 - timeouts 340
 - uninstalling 329
 - IBM Director Agent Web Server 329
 - IBM Director Console 333
 - BladeCenter object not displayed 333
 - deleted physical platform object displayed 333
 - discovered systems not displayed 331, 336
 - logon failure 337
 - managed system access request denied 335, 337
 - managed system duplicated 335
 - managed system not displayed 335
 - managed system with question mark 334
 - modifying 327
 - starting 336
 - windows 333
 - IBM Director Server 329
 - installing 327
 - starting 327, 332
 - uninstalling 329
 - imaging IBM Director Agent 335
 - installation 327
 - insufficient disk space 339
 - Internet Information Services 339
 - Inventory task 338, 340
 - Japanese-language systems 343
 - JRE exceptions 334
 - Korean-language systems 343
 - logical disk drive 339
 - managed systems
 - behind firewall 341
 - encryption 331, 336
 - invalid data values 338
 - resource-monitor information 338
 - running Windows 338
 - management console 333
 - Management Processor Assistant 328, 340, 345
 - management server 329
 - Mass Configuration task 341
 - MIB file attribute values 341, 342
 - Microsoft Internet Explorer 344
 - Microsoft Jet 329
 - Network Configuration task 341
 - network share 342
 - network timeout value, modifying 335
 - PCI adapter 339
 - redirector share 342
 - Remote Access Connection Manager service 338
 - Remote Control task 341
 - Remote Login alerts 329
 - Remote Supervisor Adapter II 340
 - Resource Monitors task 341
 - resource-monitor information 338

- troubleshooting (*continued*)
 - RPM packages 338, 340
 - RXE-100 discovery 331
 - ServeRAID inventory missing 340
 - Simple Event Filter Builder window 328
 - SNMP devices 331, 341, 342
 - SNMP traps 342
 - Software Distribution task 342
 - file-distribution server 343
 - managed system behind firewall 342
 - package creation 342
 - software package in SPB format 343
 - Telnet 330
 - time zone error 337
 - timeout associated with large event action plans 332
 - uninstalling
 - Apache error 329
 - error message 1306 329
 - upgrading
 - error message 1306 328
 - error message 1921 328
 - voltage regulator module (VRM) information 339
 - Web-based Access 344
 - Apache Web Server 344
 - event bindings 344
 - Java security warning 344
 - JVM 344
 - Netscape Navigator 344, 345
 - starting 344
 - Win32_DiskDrive.Size 339
 - won symbols 343
 - yen symbols 343
 - TWGagent.uid file 335
 - TWGConsole.prop file 337
 - twgescli.exe 56
 - TWGIIPC service 328, 329
 - twgmach.id file 335
 - TWGserver service 330
 - TWGServer.err file 330
 - TWGServer.prop file 332, 337
 - twgstat command 333, 336

U

- UDP 161, 211
- ultra320 SCSI controllers with integrated RAID 225
- UM Services tree, troubleshooting 328
- UMSHTTPD service 328
- unattended installation 238
- UNC-based share 234
- uninstalling IBM Director, troubleshooting
 - Apache error 329
 - error message 1306 329
 - locked files 329
- unknown events filter 61
- Update Assistant subtask 235
- updates, new 347
- UpdateXpress, XML file for software distribution 235
- upgrading
 - from earlier versions 11

- upgrading *(continued)*
 - troubleshooting
 - error message 1306 328, 345
 - error message 1921 328
 - Simple Event Filter Builder window 328
- uptime, system 269
- upward integration 3
 - See also* IBM Director 4.20 Upward Integration Modules Installation Guide
 - Web-based Access 305

USB

- media
 - setting blade server owner 109
 - viewing blade-server bay 109
- policy, viewing and changing 108

user

- IDs
 - Director 50
 - operating system 50
- interface 31
- profiles 49
- security 323

User Administration

- editing an existing user profile 50
- icon 32
- task 49

user security profiles 267

V

viewing

- alerts
 - IBM Director Console 48
 - Message Browser 48
- associations 31
- execution history logs 48
- job
 - history information 48
 - information, Scheduler 47
 - previously scheduled 46
 - properties 48

Virtual Machine Manager 10

voltage

- out of specification, system-health information 317
- readings, viewing 319
- regulator module (VRM) information, troubleshooting 339
- viewing
 - BladeCenter readings 107
 - service processor readings 190

Voltages service 319

VPD

- service processors 190
- vital product data 110

VRM voltage 319

W

- walk (DIRCMD) 299
- warning events filter 61
- warning threshold values 322

- Web Links services, System Updates 324
- Web site
 - IBM device drivers and updates 324
 - IBM Director resources xvii
 - IBM iSeries Information Center 332
 - IBM Redbooks xvii
 - IBM ServerProven xviii
 - IBM Support xviii
 - IBM Systems Management Software xviii
 - IBM xSeries Systems Management xviii
 - InstallShield 238
 - Java 305
 - Smart Technology Enablers 153
 - Sun 305
- Web-based Access
 - Asset ID service 320
 - Basic System service 311
 - configuration files, modifying 344
 - Date and Time service 322
 - Drives service 311
 - encryption 306
 - event bindings, troubleshooting 344
 - Event Viewer service 315
 - Fan Speeds service 319
 - FRU Numbers service 312
 - GETFRU command 359
 - Hardware Status service 308, 309
 - Health service 322
 - help 309
 - help files 7
 - information services 308, 310
 - interface 308
 - managed system information 310, 320
 - managed systems 305
 - Memory service 313
 - Mgmt Proc Event Log service 319
 - Mgmt Processor Vital Product Data service 319
 - Microsoft Internet Explorer, troubleshooting 344
 - Microsoft Management Console 305, 307
 - Multimedia service 313
 - Network service 322
 - Operating System service 313
 - port 306, 307
 - Ports service 314
 - Power/Restart Activity service 319
 - secure power management 148
 - Server Timeouts service 319
 - Shutdown service 324
 - SNMP service 323
 - starting
 - using MMC 307
 - using Web browser 305
 - System Accounts service 323
 - System Health service 316, 318
 - System Updates service 324
 - tasks services 308, 320
 - Temperatures service 319
 - troubleshooting 344
 - Java security warning 344
 - JVM 344
 - Netscape Navigator 344, 345

- Web-based Access *(continued)*
 - troubleshooting *(continued)*
 - starting 344
 - uninstalling 329
 - user interface 308
 - Voltages service 319
 - Web browsers 305
- WIN server names, troubleshooting 341
- windows
 - Add Physical Platforms 331
 - Discovery Preferences 331
 - Distribution Preferences 343
 - File Distribution Servers Manager 342
 - IBM Director Console, Discovery Preferences 331
 - Server Preferences 338, 340
- Windows
 - event log
 - events 316
 - generating events 55
 - viewing information 315
 - events 56, 61, 64
 - Installer Package wizard 239
 - InstallShield 237
 - NT limitations 15
 - NT security 306, 308
- Windows 2000, troubleshooting 338
- Windows installation
 - invalid data values 338
 - network adapter attribute names,
 - troubleshooting 341
 - Network Configuration task, troubleshooting 341
 - troubleshooting
 - event ID 2003 339
 - event log error 339
 - event log full 338
 - Win32_DiskDrive.Size 339
- Windows Management Instrumentation (WMI)
 - generating events 56
 - problem 339
- Windows Server 2003, troubleshooting 327, 328, 332, 337, 339, 341
- wizards
 - Add Card 83
 - AIX InstallP Package 242
 - BladeCenter Deployment 29, 110
 - Director File Package 249
 - Director Update Assistant 235
 - Event Action Plan 55, 60
 - InstallShield Package 237
 - Microsoft Windows Installer Package 239
 - OS/400 Restore Library Package 243
 - OS/400 Restore Licensed Program Package 244
 - OS/400 Restore Object Package 244
 - Prediction Configuration 263
 - RPM Package 241
- won symbols, troubleshooting 343
- workers.properties file 344

- XML files
 - BladeCenter Deployment wizard 110, 124
 - event action plan 74
 - event-log events 158
 - importing software packages 236
 - inventory-query results 170
 - resource-monitor recording 222
 - Software Distribution 235
 - system-availability report 273

Y

- yen symbols, troubleshooting 343

X

- xml file (DIRCMD) 302



Part Number: 90P2918

Printed in USA

(1P) P/N: 90P2918

