

IBM Director 4.11



Installation and Configuration Guide

IBM Director 4.11



Installation and Configuration Guide

Note: Before using this information and the product it supports, read the general information in Appendix C, “Notices”, on page 215.



Second Edition (September 2003)

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

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

Contents

Figures	vii
Tables	xi
About this book	xiii
How this book is organized	xiii
Notices that are used in this book	xiv
IBM Director publications	xiv
IBM Director resources on the World Wide Web	xv

Part 1. Overview of IBM Director 1

Chapter 1. Introducing IBM Director	3
IBM Director environment	3
IBM Director components	4
IBM Director Agent features	7
IBM Director extensions	8
Upgrading from previous releases of IBM Director	11
Chapter 2. Requirements for installing IBM Director	13
System requirements	13
Supported operating systems	14
Network requirements	16
Licensing	18
Database	18
Chapter 3. Planning your IBM Director installation	21
General planning considerations	21
Managing service processors	22
Setting up a BladeCenter deployment infrastructure	28
Database management	29
IBM Director security	33

Part 2. Installing IBM Director 37

Chapter 4. Installing IBM Director Server	39
Installing IBM Director Server on Windows	39
Installing IBM Director Server on Linux	51
Chapter 5. Installing IBM Director Console	55
Installing IBM Director Console on Windows	55
Installing IBM Director Console on Linux	59
Chapter 6. Installing IBM Director Agent	61
Installing IBM Director Agent on Windows	61
Installing IBM Director Agent on Red Hat Linux, SuSE Linux, or VMware ESX	68
Installing IBM Director Agent on NetWare	71
Installing IBM Director Agent on Caldera Open UNIX	74

Part 3. Configuring IBM Director 77

Chapter 7. Configuring an IBM BladeCenter chassis	79
--	----

Starting IBM Director Console	79
Discovering a BladeCenter chassis	81
Using the BladeCenter Deployment wizard.	84
Chapter 8. Configuring IBM Director	97
Using the Event Action Plan wizard	97
Discovering managed systems, devices, and objects	102
Authorizing IBM Director users	106
Configuring security settings	111
Configuring software distribution	113
Chapter 9. Installing IBM Director extensions	121
Completing the Rack Manager installation on the management server	121
Installing Software Distribution (Premium Edition).	122
Installing the Server Plus Pack extensions on managed systems	123

Part 4. Upgrading IBM Director 133

Chapter 10. Upgrading IBM Director Server	135
Upgrading IBM Director Server on Windows.	135
Upgrading IBM Director Server on Linux	142
Chapter 11. Upgrading IBM Director Console	145
Upgrading IBM Director Console on Windows	145
Upgrading IBM Director Console on Linux	149
Chapter 12. Upgrading IBM Director Agent	151
Upgrading IBM Director Agent using standard installation procedures	151
Upgrading IBM Director Agent using the Software Distribution task	165

Part 5. Maintenance and problem solving 171

Chapter 13. Modifying and uninstalling IBM Director	173
Modifying an IBM Director installation	173
Uninstalling IBM Director.	179
Chapter 14. Solving IBM Director problems	183
Installation, upgrades, and uninstallation	183
IBM Director Server.	185
IBM Director Console	188
IBM Director Agent	191
Managed systems running Windows	192
IBM Director tasks	193
Software Distribution	194
Web-based Access	195
Chapter 15. Getting help and technical assistance	199
Before you call	199
Using the documentation.	199
Getting help and information from the World Wide Web	199
Software service and support	200

Part 6. Appendixes 201

Appendix A. IBM Director Agent — IBM Director Server security	203
--	------------

How authentication works	203
Securing managed systems.	205
Changing access or security states	206
Key management	208
Appendix B. Terminology summary and abbreviation list	211
IBM Director terminology summary	211
Abbreviations	211
Appendix C. Notices	215
Edition notice	215
Trademarks.	216
Glossary	217
Index	227

Figures

1. Hardware in an IBM Director environment	4
2. Software in an IBM Director environment	5
3. Example of a BladeCenter deployment network	28
4. Installing IBM Director Server on Windows: “Server Plus Pack” window	40
5. Installing IBM Director Server on Windows: “Feature and installation directory selection” window	40
6. Installing IBM Director Server on Windows: “Features and installation directory selection” window	41
7. Installing IBM Director Server on Windows: Installing the Server Plus Pack	42
8. Installing IBM Director Server on Windows: “IBM Director service account information” window	43
9. Installing IBM Director Server on Windows: “Encryption settings” window	44
10. Installing IBM Director Server on Windows: “Software-distribution settings” window	44
11. Installing IBM Director Server on Windows: “Web-based Access information” window	45
12. Installing IBM Director Server on Windows: “Network driver configuration” window	46
13. Installing IBM Director Server: “IBM Director database configuration” window	47
14. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window	48
15. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window	48
16. Installing IBM Director Server: “IBM Director Microsoft SQL Server database configuration” window	49
17. Installing IBM Director Server: “IBM Director Oracle database configuration” window	49
18. Installing IBM Director Server: “IBM Director Oracle database configuration” window	50
19. Installing IBM Director Console: “Server Plus Pack” window	56
20. Installing IBM Director Console: “Feature and destination directory selection” window	56
21. Installing IBM Director Console: Installing ServeRAID Manager	57
22. Installing IBM Director Console: Installing the Server Plus Pack	58
23. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window	63
24. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window	64
25. Installing IBM Director Agent on Windows: “Security settings” window	64
26. Installing IBM Director Agent on Windows: “Software Distribution settings” window	65
27. Installing IBM Director Agent on Windows: “Web-based Access information” window	66
28. Installing IBM Director Agent on Windows: “Network driver configuration” window	66
29. Installing IBM Director Agent on NetWare: “Choose destination location” window	72
30. Installing IBM Director Agent on NetWare: “Select Components” window	73
31. Installing IBM Director Agent on NetWare: “InstallShield Wizard complete” window	73
32. “IBM Director Login” window	80
33. IBM Director Console	80
34. IBM Director Console: Group Contents pane	82
35. “Add BladeCenter Chassis” window	83
36. “Management Module Network Interfaces” window	84
37. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window	86
38. BladeCenter Deployment wizard: “Login to the BladeCenter management module” window	87
39. BladeCenter Deployment wizard: “Change the user name and password for the management module” window	88
40. BladeCenter Deployment wizard: “Configure the management module properties” window	89
41. BladeCenter Deployment wizard: “Configure the management module protocols” window	90
42. BladeCenter Deployment wizard: “Configure the IP settings” window	91
43. BladeCenter Deployment wizard: “Change the user name and password for switch modules” window	92
44. BladeCenter Deployment wizard: “Configure the switch module” window	93
45. BladeCenter Deployment wizard: “Deploy operating systems on the blade servers” window	94
46. BladeCenter Deployment wizard: “Configure the deployment policies” window	94
47. BladeCenter Deployment wizard: “Setup summary” window	95
48. IBM Director Console Tasks pane: Deployment Wizard profile	96
49. Event Action Plan wizard: “Welcome to the Event Action Plan wizard” window	97
50. Event Action Plan wizard: “Select the event filters” window	98

51. Event Action Plan wizard: “Select the notification” window	99
52. Event Action Plan wizard: “Apply the event action plan” window	100
53. Event Action Plan wizard: “Discover all systems and devices” window	101
54. Event Action Plan wizard: “Review your selection summary” window	102
55. “Discovery Preferences” window	104
56. “Add Management Processors” window	105
57. IBM Director Console: Group Contents pane	106
58. “User Administration” window	107
59. “User Defaults Editor” window	107
60. “User Administration” window	108
61. “User Editor” window: “User Properties” page	109
62. “User Editor” window: “Privileges” page	109
63. “User Editor” window: “Group Access” page	110
64. “User Editor” window: “Task Access” page	111
65. IBM Director Console: “Add Share Name” window	116
66. IBM Director Console: “Software Distribution” page	117
67. IBM Director Console: “Managed System Distribution Preferences” window	118
68. IBM Director Console: “Add Share Name” window	119
69. Installing Capacity Manager on NetWare: “Choose Destination Location” window	125
70. Installing Capacity Manager on NetWare: “Start Copying Files” window	126
71. Creating a software package: “Software Distribution Manager” window (Standard Edition)	127
72. Creating a software package: “Software Distribution Manager” window (Premium Edition)	127
73. Creating a software package: “Director Update Assistant” window	127
74. Creating a software package: “IBM Update Package/Root Directory Location” window	128
75. Creating a software package: “IBM Update Package/Root Directory Location” window	128
76. Creating a software package: “Director Update Assistant” window	129
77. Creating software packages: “Director Update Assistant” window	129
78. Creating software packages: “Director Update Assistant” window	129
79. All Software Distribution Packages: IBM Director Server Plus Pack	130
80. Scheduling the installation of a software package: “New Scheduled Job” window	131
81. Upgrading IBM Director Server on Windows: “Server Plus Pack” window	136
82. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window	136
83. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window	137
84. Upgrading IBM Director Server on Windows: Installing the Server Plus Pack	138
85. Upgrading IBM Director Server on Windows: “IBM Director service account information” window	139
86. Installing IBM Director Server on Windows: “Encryption settings” window	140
87. Upgrading IBM Director Server on Windows: “Software-distribution settings” window	140
88. Upgrading IBM Director Server on Windows: “Web-based Access information” window	141
89. Upgrading IBM Director Server on Windows: “Network driver configuration” window	141
90. Upgrading IBM Director Console: “Server Plus Pack” window	146
91. Upgrading IBM Director Console: “Feature and destination directory selection” window	146
92. Upgrading IBM Director Console: Installing ServeRAID Manager	147
93. Upgrading IBM Director Console: Installing the Server Plus Pack	148
94. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window	153
95. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window	154
96. Upgrading IBM Director Agent on Windows: “Security settings” window	154
97. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window	155
98. Upgrading IBM Director Agent on Windows: “Web-based Access information” window	156
99. Upgrading IBM Director Agent on Windows: “Network driver configuration” window	156
100. Upgrading IBM Director Agent on NetWare: “Select Components” window	162
101. Creating a software package: “Software Distribution Manager” window (Standard Edition)	165
102. Creating a software package: “Software Distribution Manager” window (Premium Edition)	166
103. Creating a software package: “Director Update Assistant” window	166
104. Creating a software package: “IBM Update Package/Root Directory Location” window	167
105. Creating a software package: “IBM Update Package/Root Directory Location” window	167
106. Creating a software package: “Director Update Assistant” window	168

107. Creating software packages: “Director Update Assistant” window	168
108. All Software Distribution Packages: IBM Director Agent Upgrade	169
109. Scheduling the installation of a software package: “New Scheduled Job” window	169
110. “Program Maintenance” window	174
111. Modifying IBM Director Agent on NetWare: “Choose destination location” window	177
112. Modifying IBM Director Agent on NetWare: “Select Components” window	177
113. “Request Access to Systems” window.	207

Tables

1. Minimum hardware requirements for IBM Director	13
2. Network adapter device drivers necessary to run the Fault Tolerant Management Interface	14
3. Supported operating systems for Server Plus Pack extensions installed on managed systems	15
4. Supported network protocols	16
5. Ports used by IBM Director	17
6. In-band communication between service processors and IBM Director Server	23
7. IBM Director Agent features that handle in-band communication and alerts	24
8. Out-of-band communication pathways and alert-forwarding strategies	24
9. Whether service processors connected over LAN to IBM Director Server can communicate with service processors on the ASM interconnect.	25
10. Service processors in IBM Netfinity and xSeries systems	25
11. Part numbers for Remote Supervisor Adapter firmware updates	27
12. Diruns parameters	180
13. Installation problems	183
14. Upgrade problems	184
15. Uninstallation problems	185
16. IBM Director Server problems	185
17. IBM Director Console problems	188
18. IBM Director Agent problems	191
19. Managed systems running Windows problems	192
20. IBM Director task problems	193
21. Software Distribution problems	194
22. Web-based Access problems	195
23. Abbreviations used in IBM Director	211

About this book

This book provides information about installing and configuring IBM® Director 4.11. In addition to presenting an overview of IBM Director and its requirements, it covers the following topics:

- Planning an IBM Director environment
- Installing IBM Director and IBM Director extensions
- Upgrading from IBM Director 3.x or later to IBM Director 4.11
- Configuring IBM Director

It also includes information about IBM Director security and solving problems you might encounter with IBM Director.

How this book is organized

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

Chapter 2, “Requirements for installing IBM Director”, on page 13 contains basic information about IBM Director. This includes system and network requirements, supported operating systems and database applications, information about the IBM Director service account, and an overview of IBM Director security features.

Chapter 3, “Planning your IBM Director installation”, on page 21 contains information about planning your IBM Director environment. It also includes information about working with service processors, setting up a BladeCenter™ deployment infrastructure, and configuring a database application for use with IBM Director.

Chapter 4, “Installing IBM Director Server”, on page 39 contains instructions for installing IBM Director Server.

Chapter 5, “Installing IBM Director Console”, on page 55 contains instructions for installing IBM Director Console.

Chapter 6, “Installing IBM Director Agent”, on page 61 contains instructions for installing IBM Director Agent.

Chapter 7, “Configuring an IBM BladeCenter chassis”, on page 79 contains information about starting IBM Director Console, discovering the BladeCenter chassis, and running the BladeCenter Deployment wizard.

Chapter 8, “Configuring IBM Director”, on page 97 contains information about running the Event Action Plan wizard, setting discovery preferences and creating management processor objects, authorizing IBM Director users, configuring security settings, and preparing to use software distribution.

Chapter 9, “Installing IBM Director extensions”, on page 121 contains instructions for completing the Rack Manager installation on the management server, installing IBM Director Software Distribution (Premium Edition), and installing the IBM Director Server Plus Pack extensions on managed systems.

Chapter 10, “Upgrading IBM Director Server”, on page 135 contains instructions for upgrading IBM Director Server.

Chapter 11, “Upgrading IBM Director Console”, on page 145 contains instructions for upgrading IBM Director Console.

Chapter 12, “Upgrading IBM Director Agent”, on page 151 contains instructions for upgrading IBM Director Agent.

Chapter 13, “Modifying and uninstalling IBM Director”, on page 173 contains information about modifying or uninstalling IBM Director.

Chapter 14, “Solving IBM Director problems”, on page 183 lists solutions to problems that you might encounter with IBM Director.

Chapter 15, “Getting help and technical assistance”, on page 199 contains information about accessing IBM Support Web sites for help and technical assistance.

Appendix A, “IBM Director Agent — IBM Director Server security”, on page 203 contains information about IBM Director Agent — IBM Director Server security. It includes an overview of authentication, procedures for securing managed systems, and information about key management.

Appendix B, “Terminology summary and abbreviation list”, on page 211 contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

Appendix C, “Notices”, on page 215 contains product notices and trademarks.

The “Glossary” on page 217 provides definitions for terms used in IBM Director publications.

Notices that are used in this book

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

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

IBM Director publications

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

- *IBM Director 4.11 Installation and Configuration Guide* Second Edition, September 2003 (dir411_install.pdf)
- *IBM Director 4.11 Systems Management Guide* Second Edition, September 2003 (dir411_sysmgt.pdf)
- *IBM Director 4.1 Events Reference* (dir41_events.pdf)
- *IBM Director 4.1 Upward Integration Modules Installation Guide* (dir41_uim.pdf)

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

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

- *IBM eServer BladeCenter Type 8677 Planning and Installation Guide*
- *Advanced System Management PCI Adapter, Software User's Guide*
- *Advanced System Management PCI Adapter, Installation Instructions*
- *Remote Supervisor Adapter, User's Guide*
- *Remote Supervisor Adapter, Installation Guide*
- *Remote Supervisor Adapter II, User's Guide*
- *Remote Supervisor Adapter II, Installation Guide*
- *IBM Management Processor Command-Line Interface Version 2.0 User's Guide*

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

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

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

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

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

IBM Director resources on the World Wide Web

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

IBM Systems Management Software: Download/Electronic Support page

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

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

IBM xSeries Systems Management page

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

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

IBM ServerProven® page

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

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

IBM Director Agent page

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

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

IBM Support page

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

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

Part 1. Overview of IBM Director

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. IBM Director has features that are designed expressly to work with the hardware in the following currently-marketed IBM systems and products:

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

A powerful suite of tools and utilities, IBM Director automates many of the processes 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.

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.

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

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

Figure 1 shows the hardware in an IBM Director environment.

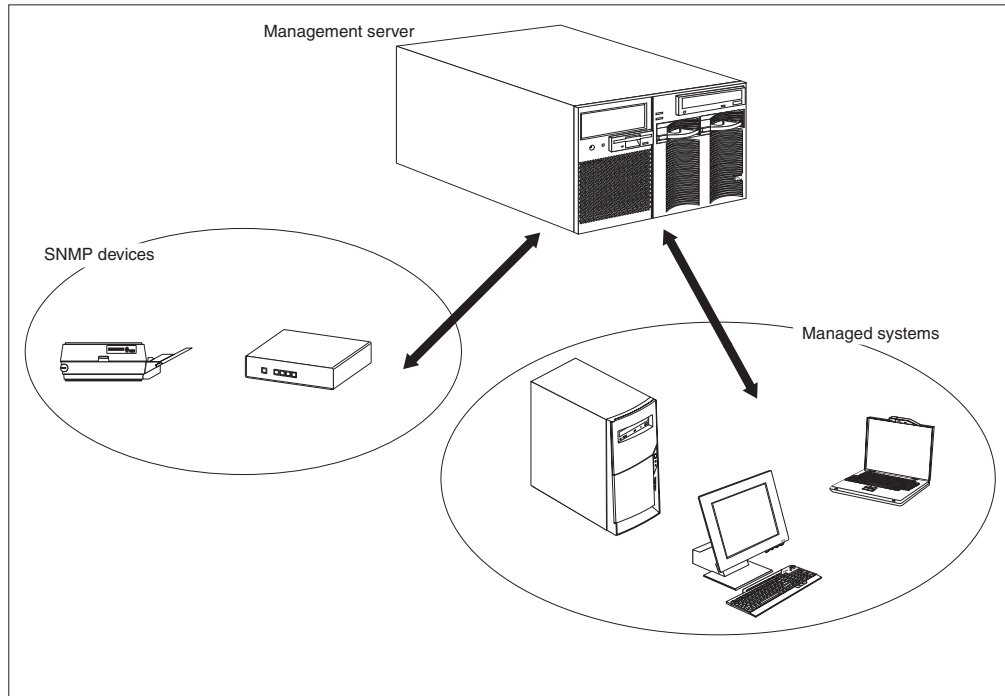


Figure 1. Hardware in an IBM Director environment

For information about IBM hardware that is supported by IBM Director, see the hardware compatibility list on the IBM ServerProven Web site at <http://www.ibm.com/pc/us/compat/index.html>.

IBM Director components

The IBM Director software has three components:

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

Each group of hardware in your IBM Director environment requires a different combination of these components.

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

Figure 2 on page 5 shows where the IBM Director software components are installed in a basic IBM Director environment.

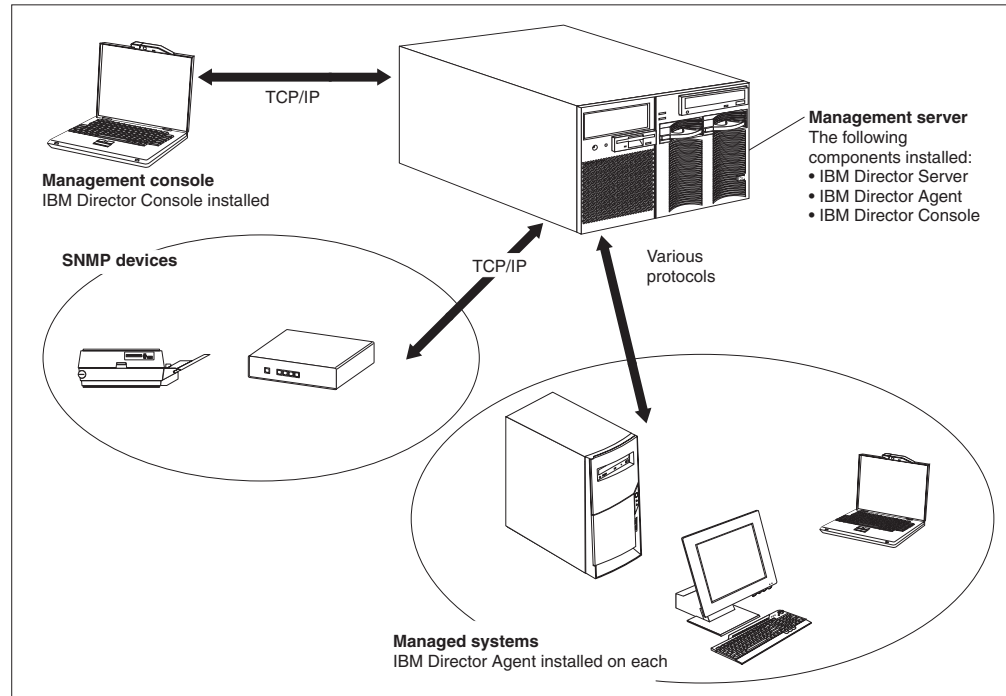


Figure 2. Software in an IBM Director environment

IBM Director Server

IBM Director Server is the main component of IBM Director; it contains the management data, the server engine, and the application logic. IBM Director Server provides basic functions such as discovery of the managed systems, persistent storage of configuration and management data, an inventory database, event listening, security and authentication, management console support, and administrative tasks.

IBM Director Server stores the inventory data in a Structured Query Language (SQL) database. You can access information that is stored in this relational database even when the managed systems are not available. You can use the Microsoft Jet 4.0 database engine, which is included in Windows® 2000. For large-scale IBM Director solutions, you must use another database application.

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

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

- Microsoft Windows 2000 Server and Advanced Server (Service Pack 3 required)
- Windows Server 2003 (Standard, Enterprise, and Web Editions)
- Red Hat Linux, version 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- SuSE Linux, version 8.0
- SuSE Linux Enterprise Server, version 8.0

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

IBM Director Agent

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

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

- Windows 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 Professional, Server, Advanced Server, and Datacenter Server (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)
- Windows Server 2003 (Standard, Enterprise, Datacenter, and Web Editions)
- Red Hat Linux, versions 7.1, 7.2, and 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- Red Hat Enterprise Linux ES and WS, version 2.1
- SuSE Linux, versions 7.2, 7.3, and 8.0
- SuSE Linux Enterprise Server, version 8.0
- Novell NetWare, version 6.0
- Caldera Open UNIX[®], version 8.0
- SCO UnixWare, version 7.1.3
- VMware ESX Server, versions 1.5.2 and 2.0

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

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

IBM Director Console

IBM Director Console is the graphical user interface (GUI) for IBM Director Server. Data is transferred between IBM Director Console and IBM Director Server through TCP/IP. Using IBM Director Console, 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.

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

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)
- Windows Server 2003 (Standard, Enterprise, and Web Editions)
- Red Hat Linux, version 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- SuSE Linux, version 8.0
- SuSE Linux Enterprise Server, version 8.0

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

IBM Director Agent features

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

ServeRAID Manager

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

Management Processor Assistant Agent

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

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

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

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

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 operating systems.

Web-based Access

You can use Web-based Access to access a managed system using either a Web browser or the Microsoft Management Console (MMC). When you install

Web-based Access on a managed system, you can access IBM Director Agent and view real-time asset and health information about the managed system. This feature is supported only on Windows 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 operating systems.

System Health Monitoring

System Health Monitoring provides active monitoring of critical system functions, including disk space availability, drive alerts, temperatures, fan functionality, and power supply voltage. It produces and relays hardware alerts to the operating-system event log, IBM Director Server, and other management environments. System Health Monitoring is supported only on Windows operating systems.

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

SNMP Access and Trap Forwarding

This feature enables SNMP as a protocol for accessing managed-system data. This 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: If you want IBM Director to poll SNMP devices and receive their alerts, verify that an SNMP Server and SNMP Trap Service are running on the management server.

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, Scalable Systems 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, 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.

Notes:

1. Active PCI Manager is supported on managed systems running Windows 2000 (Server, Advanced Server, and Datacenter Server) and Windows 2003 (Standard, Enterprise, and Web Editions) only.
2. Earlier versions of Active PCI Manager are not compatible with IBM Director. Before you install IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
3. IBM Active PCI Software for Microsoft Windows, version 5.0.2.0 or later, must be installed. You can download the software from <http://www.ibm.com/support/>. In the **Search** field in the upper-right corner of the page, type `activepci`.

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

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

IBM 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.

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 were saved in NVRAM by the BIOS Configuration/Setup Utility program
- 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.

Additional IBM Director extensions

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

Real Time Diagnostics

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

Cluster Systems Management

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

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

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

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

APC PowerChute Extension for IBM Director

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

Electronic Service Agent

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

Application Workload Management (Aurema)

Manages how multiple applications use server resources.

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

Upgrading from previous releases of IBM Director

If you are running IBM Director 3.x or later, you can upgrade to IBM Director 4.11. Earlier versions of IBM Director are not compatible with IBM Director 4.11.

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 you upgrade IBM Director Console, you must upgrade IBM Director Server also.

IBM Director Server 4.11 can manage systems running IBM Director Agent 3.x. This is useful for managed systems running operating systems that are not supported by IBM Director 4.11:

- Windows 95, 98, and Millennium Edition (Me)
- NetWare, version 5.x
- OS/2® WARP® Server for e-business
- Caldera Linux, versions 2.3.1 and 3.1
- Turbolinux, versions 6.0.5 and 6.5
- SCO UnixWare, version 7.1.1

Chapter 2. Requirements for installing IBM Director

This chapter contains information about system and network requirements, licenses, and supported database applications. It also contains an overview of the IBM Director security features.

System requirements

This section contains information about hardware requirements and supported operating systems.

Hardware requirements

The systems on which you install IBM Director Server or IBM Director Agent must meet the Wired for Management (WfM), version 2.0, specifications.

The following table lists the minimum microprocessor speed, random access memory (RAM), and disk space needed by the IBM Director components.

Table 1. Minimum hardware requirements for IBM Director

	IBM Director Server	IBM Director Agent	IBM Director Console
Microprocessor speed	Pentium® 300+ MHz	Pentium class processor	Pentium 300+ MHz
Memory (RAM)	256 MB (512 MB recommended)	128 MB	128 MB
Disk space	316 MB	109 MB	168 MB
Display	At least 256 colors	Not applicable	At least 256 colors

Because a system configured with the minimum requirements might perform poorly in a production environment, consider the following suggestions:

- The microprocessor speed, memory, and disk space minimum requirements are *in addition* to whatever resources are necessary for the software already installed on the system.
- Conduct a performance analysis to ensure that the system has sufficient capacity to handle the additional requirements of functioning as a management server or management console.

BIOS, device drivers, and firmware

SMBIOS 2.1 or later is required for all systems in an IBM Director environment.

A best practice is to upgrade all BIOS code, device drivers, and firmware to the latest versions before installing IBM Director. This ensures that the latest performance improvements and fixes have been applied.

To run the Fault Tolerant Management Interface (a subtask of Active PCI Manager) against a managed system, the managed system must have the applicable device driver installed. The following table lists the minimum version of the supported device drivers for each network adapter.

Table 2. Network adapter device drivers necessary to run the Fault Tolerant Management Interface

Manufacturer	Version
Intel	8.0
3Com	2.3
Broadcom	6.6.7

Ensure that the applicable device driver is installed and that the device driver is at the supported version or later.

Supported operating systems

This section lists the operating systems upon which IBM Director can be installed.

Note: For the most recent list of operating systems on which IBM Director can be installed, 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:

- Microsoft Windows 2000 Server and Advanced Server (Service Pack 3 required)
- Windows Server 2003 (Standard, Enterprise, and Web Editions)
- Red Hat Linux, version 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- SuSE Linux, version 8.0
- SuSE Linux Enterprise Server, version 8.0

IBM Director Agent

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

- 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 Professional, Server, Advanced Server, and Datacenter Server (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)
- Windows Server 2003 (Standard, Enterprise, Datacenter, and Web Editions)
- Red Hat Linux, versions 7.1, 7.2, and 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- Red Hat Linux Enterprise Linux ES and WS, version 2.1
- SuSE Linux, versions 7.2, 7.3, and 8.0
- SuSE Linux Enterprise Server, version 8.0
- Novell NetWare, version 6.0
- Caldera Open UNIX, version 8.0

- SCO UnixWare, version 7.1.3
- VMware ESX Server, versions 1.5.2 and 2.0

IBM Director Console

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

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)
- Windows Server 2003 (Standard, Enterprise, and Web Editions)
- Red Hat Linux, version 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- SuSE Linux, version 8.0
- SuSE Linux Enterprise Server, version 8.0

Server Plus Pack extensions

The following table lists the Server Plus Pack extensions that can be installed on managed systems and the operating systems on which they can be installed. (Rack Manager does not contain an agent component. It can be used against all managed systems, regardless of operating system.)

Table 3. Supported operating systems for Server Plus Pack extensions installed on managed systems

Operating system	IBM Director Extensions
Windows NT 4.0 Server (Standard, Enterprise, and Terminal Server Editions) and Windows NT 4.0 Server with Citrix MetaFrame Windows 2000 Professional Windows Server 2003 Datacenter Edition	<ul style="list-style-type: none"> • Capacity Manager • Software Rejuvenation • System Availability
Windows 2000 (Server, Advanced Server, and Datacenter Server) Windows Server 2003 (Standard, Enterprise, and Web Editions)	<ul style="list-style-type: none"> • Active PCI Manager • Capacity Manager • Software Rejuvenation • System Availability
Red Hat Linux, versions 7.1, 7.2, and 7.3 Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1) Red Hat Linux Enterprise Server ES and WS, version 2.1 SuSE Linux, versions 7.2, 7.3, and 8.0 SuSE Linux Enterprise Server, version 8.0	<ul style="list-style-type: none"> • Capacity Manager • Software Rejuvenation • System Availability
NetWare, version 6.0	<ul style="list-style-type: none"> • Capacity Manager
VMware ESX Server, versions 1.5.2 and 2.0	<ul style="list-style-type: none"> • Capacity Manager • System Availability

Network requirements

This section discusses supported network protocols and Web browsers, as well as ports used in an IBM Director environment.

Network protocols

IBM Director Server communicates with the IBM Director Console only through TCP/IP. You can use TCP/IP, NetBIOS, SNA, or IPX to communicate between IBM Director Server and IBM Director Agent. IBM Director Server communicates with SNMP devices only through TCP/IP.

Note: TCP/IP is the only network protocol that you can use to communicate with managed systems running Linux or UNIX.

The following table lists the supported versions of network protocols.

Table 4. Supported network protocols

Protocol	Supported version
TCP/IP	All WinSock-compatible versions of TCP/IP supported by Windows 2000, NetWare 6.0, Linux, and UNIX
NetBIOS	Native NetBIOS versions supported by Windows 2000
IPX	IPX versions supported by NetWare 6.0 and Windows 2000
SNA	Microsoft SNA 4.0 with Service Pack 1

Ports

The following table lists the ports used by IBM Director. Depending on which IBM Director services are installed (such as Web-based Access or IBM Director Remote Control Agent), IBM Director needs certain ports available for communication.

Table 5. Ports used by IBM Director

	Connection	Port	IPX ports
IBM Director	IBM Director Server → BladeCenter switch module	80 TCP 23	
	IBM Director Server → IBM Director Agent	14247 UDP and TCP 14248 UDP (Linux only)	4490 (hex) read 4491 (hex) write
	IBM Director Agent → IBM Director Server	14247 UDP and TCP	4490 (hex) read 4491 (hex) write
	IBM Director Server → IBM Director Console	Random*	
	IBM Director Console → IBM Director Server	2033 TCP*	
	IBM Director Console → IBM Director Console	a free port (For use of BladeCenter Switch Management LaunchPad)	
	SNMP access	161 UDP	
	SNMP traps	162 UDP	
	Remote session on SNMP devices	23	
	Web-based Access	IBM Director Web server (configured during installation of IBM Director Agent)	411 HTTP
423 HTTPS			
8009 (internal use)			
Service processors	IBM Director → service processor and BladeCenter management module	23 TCP	
	Service processor (using Telnet)	6090 TCP 427 UDP and TCP	
	Web-based Access	80	
	SNMP agent	161 UDP	
	SNMP traps	162 UDP	
	IBM Director over LAN alerts	13991 UDP	

* IBM Director Console opens a port in the 1024 - 65535 range. Then it connects through TCP to IBM Director Server using port 2033. When IBM Director Server responds to IBM Director Console, it communicates to the random port in the 1024 - 65535 range that IBM Director Console opened.

Web browsers

If you have installed Web-based Access on a managed system, you can use the following Web browsers to access a managed system running Microsoft Windows:

- Microsoft Internet Explorer, version 4.1 or later
- Netscape Navigator, versions 4.7 or 7.01

You also can use Microsoft Management Console (MMC), version 1.1 or later.

Your Web browser must support Java[®] applets. If you are running Internet Explorer on Windows XP, you must install Service Pack 1 for Windows XP.

If you are using Internet Explorer, you must use 56-bit encryption or higher.

Licensing

IBM Director includes the following licenses:

- One license for the installation of IBM Director Server (which automatically includes IBM Director Agent and IBM Director Console)
- 20 licenses to install IBM Director Agent on non-IBM systems
- Unlimited licenses to install IBM Director Console

Most IBM Intel-based systems come with a license for IBM Director Agent. For a complete list of systems 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.

Database

IBM Director requires a SQL database to store the system inventory data. You can use the following database applications in conjunction with IBM Director:

- Microsoft Jet 4.0 database engine, Service Pack 6, and Microsoft Data Access Control (MDAC) 2.7 (Windows only)
- Microsoft Data Engine (MSDE) 1.0, Service Pack 3, and MDAC 2.7 (Windows only)
- Microsoft SQL Server 2000 Desktop Engine, Service Pack 3, and MDAC 2.7 (Windows only)
- Microsoft SQL Server 7.00, Service Pack 3, and MDAC 2.7 (Windows only)
- Microsoft SQL Server 2000, Service Pack 3, and MDAC 2.7 (Windows only)
- IBM DB2[®] Universal Database™ 6.1, Fix Pack 11 (Windows only)
- IBM DB2 Universal Database 7.2, Fix Pack 9
- IBM DB2 Universal Database 8.1, Fix Pack 2

- Oracle Server, versions 8.1.7 and 9.0.x
- PostgreSQL, versions 7.2 and 7.3 (Linux only)

The Microsoft Jet 4.0 database engine is built into Windows 2000, Windows XP, and Windows 2003. However, the Jet database has a 2.14 GB limit. If your environment has more than 300 to 500 systems, you should *not* use Microsoft Jet 4.0.

If you plan to use a database application other than Microsoft Jet, you should install and configure the database application *before* installing IBM Director Server.

Chapter 3. Planning your IBM Director installation

This chapter contains information about planning your IBM Director environment. It also includes information about working with service processors, setting up a BladeCenter deployment infrastructure, and configuring a database application for use with IBM Director.

General planning considerations

Installation of IBM Director begins with planning. Consider the following factors:

1. Review and assess your entire network. Your network must be up and running before you begin installing IBM Director. Complete the following steps for a seamless installation and to ensure the discovery of all systems in your network.
 - Determine the physical location and network address of all servers, computers, and other devices in your network. Identify subnets and determine whether there are any remote subnets. Identify the communication method you are using; this determines the type of discovery to deploy.
 - Determine the capabilities of your network and the amount of traffic that your network can manage. If you have a wide area network (WAN) link, use a T1 line (1.5 MBps) at a minimum, for reliable network performance during installation.
 - Ensure that all servers, computers, and devices are properly installed and cabled to ensure discovery.
 - Document operating-system levels installed on the systems to be managed, and enable SNMP traps if necessary.
2. Determine the long-term growth and the rate of growth that you expect for your IBM Director environment. You can use the Microsoft Jet database engine, which has a maximum size of 2.14 GB. This provides management for approximately 300 to 500 managed systems. The Microsoft Jet database engine is not filtered. Therefore, when an inventory is performed, all managed systems, including desktop computers and mobile computers, are inventoried. The quantity of software installed and inventoried can add a significant amount of information to your database. If you use a database application other than the Microsoft Jet database engine, prepare your database application before installing IBM Director.
3. Determine the services that each managed system is providing and the information that you want to monitor and manage for each system. Determine what performance information to monitor and the event action plans to create. Often, desktop and mobile computers are monitored differently than are servers. Be sure to plan for what you want to monitor so that the performance of the managed system is not affected.
4. Ensure that all of your servers have the latest level of device driver, firmware, and BIOS code installed. You can update your IBM xSeries servers and certain Netfinity servers to the latest level of code using IBM UpdateXpress™. Be sure to check the supported servers information found on the UpdateXpress CD or Web site before using it to install updates.
5. Determine on which server you want to install IBM Director Server. You must install IBM Director Server on more than one server if you are managing more than 5000 systems. You might want to install IBM Director Server on more than one server, depending on network infrastructure or geographical location of managed systems, or if different system administrators own managed systems.

Note: Do not install IBM Director Server on a domain controller. Its high resource utilization might degrade domain controller performance. In addition, if you install IBM Director Server on a domain controller and then demote the domain controller, you no longer can access to IBM Director Console. Furthermore, unless the IBM Director service account has domain administrator privileges, you cannot restart IBM Director Server.

Use a non-blade server as the management server. This ensures that you can run the BladeCenter Deployment wizard and use the BladeCenter tasks.

6. Install IBM Director Agent on each system that you want to manage.
7. Determine the discovery method that you want to use. By default, IBM Director discovers only systems that are on the same subnet as the management server. If you have a local subnet and a remote subnet, you must configure additional discovery capabilities. To change the default settings, use the Discovery Preferences feature in IBM Director Console. Communication between the management server and the managed systems occurs through UDP port 14247. This is important to consider when you are using IBM Director in a routed environment. Typically, broadcasts are limited to local subnets; consider using relay agents for discovery on remote subnets. See “Setting discovery preferences” on page 103 for more information.

Managing service processors

To effectively use IBM Director to manage IBM Netfinity and xSeries servers, you must identify which service processors are present in your servers. Doing so enables you to accomplish the following tasks:

- Determine which IBM Director Agent features to install on managed systems
- Decide how to configure servers, optional service processors, and ASM interconnects to maximize the ability of systems to communicate with and send alerts to IBM Director Server
- Manually create management processor objects in IBM Director Console

Communication between service processors and IBM Director Server

There are several pathways along which communication between IBM Director Server and the service processors present in IBM Netfinity or xSeries servers takes place:

Interprocess communication

IBM Director Server communicates with IBM Director Agent; IBM Director Agent uses a device driver to pass data to and from the service processor. This is also called in-band communication.

Over the LAN

Data is transmitted between the service processor and IBM Director Server over the LAN. This is possible if the service processor has a network interface card (NIC).

Over the ASM interconnect

Data is passed from the service processor over an ASM interconnect network to a second service processor. The second service processor serves as a gateway between IBM Director Server and the service processors on the ASM interconnect network.

Both of the latter types of communication are known as out-of-band, because they take place independent of an operating system.

An *ASM interconnect network* is a group of service processors networked together using the ASM interconnect feature. Connected through the RS-485 ports and standard Category 5 cables, the service processors can communicate and send alerts out-of-band to IBM Director Server. Such a network eliminates the need for multiple modems, telephones, and LAN ports; it also permits service processors without network interface cards to communicate out-of-band with IBM Director Server.

An *ASM interconnect gateway* is the service processor that serves as the focal point for the ASM interconnect network. The ASM interconnect gateway controls the ASM interconnect network and receives all alerts from the service processors that are on it. You can use either a Remote Supervisor Adapter or an ASM PCI adapter as the ASM interconnect gateway. However, to ensure that ISMPs on the interconnect network are able to communicate out-of-band with IBM Director, you must use a Remote Supervisor Adapter as the ASM interconnect gateway.

Notes:

1. If you have an xSeries 360 or 440 server attached to an RXE-100 Remote Expansion Enclosure, you cannot use the on-board Remote Supervisor Adapter as an ASM interconnect gateway. The Remote Supervisor Adapter is dedicated to managing the RXE-100 Remote Expansion Enclosure.
2. For IBM Director and SSM to communicate out-of-band, the following conditions must be met:
 - Service processors must maintain consistent IP addresses. You either must assign static IP addresses or configure Dynamic Host Configuration Protocol (DHCP) to maintain consistent IP addresses for the service processors.
 - The service processor IP addresses cannot change after IBM Director has discovered the server.

In-band communication and alerts

To enable in-band communication between IBM Director Server and a managed system that contains a service processor, you must install the MPA Agent on the managed system.

Whether a service processor can communicate in-band with IBM Director Server depends on the service processor type and the operating system running on the server. Integrated system management processors (ISMPs) in servers running Novell NetWare or Caldera Open UNIX cannot communicate in-band with IBM Director.

Table 6. In-band communication between service processors and IBM Director Server

Type of service processor	Operating system on managed system			
	Windows	Linux	NetWare	Caldera Open UNIX
Advanced System Management processor (ASM processor)	Yes	Yes	Yes	Yes
Advanced System Management PCI Adapter (ASM PCI adapter)	Yes	Yes	Yes	Yes
Remote Supervisor Adapter Remote Supervisor Adapter II	Yes	Yes	Yes	Yes
Integrated system management processor (ISMP)	Yes	Yes	No	No

When in-band communication is possible, alerts are handled either by the MPA Agent or System Health Monitoring, depending on the operating system. ISMPs in servers running Linux cannot send alerts in-band, although in-band communication between the service processor and IBM Director Server is possible.

Table 7. IBM Director Agent features that handle in-band communication and alerts

Type of service processor	Operating system on managed system			
	Windows	Linux	NetWare	Caldera Open UNIX
Advanced System Management Processor (ASM processor)	System Health Monitoring	MPA Agent	MPA Agent	MPA Agent
Advanced System Management Processor PCI Adapter (ASM PCI Adapter)	System Health Monitoring	MPA Agent	MPA Agent	MPA Agent
Remote Supervisor Adapter Remote Supervisor Adapter II	System Health Monitoring	MPA Agent	MPA Agent	MPA Agent
Integrated system management processor (ISMP)	System Health Monitoring	Not applicable	Not applicable	Not applicable

Out-of-band communication and alerts

The type of service processor present in a server determines which paths out-of-band communication can take. Some service processors can communicate out-of-band directly with IBM Director Server; others must be on an ASM interconnect network that includes a service processor with the ability to communicate out-of-band with IBM Director Server.

The type of service processor and firmware levels also determines what type of alert-forwarding strategy is possible.

Table 8. Out-of-band communication pathways and alert-forwarding strategies

Type of service processor	Pathways for out-of-band communication	Possible alert-forwarding strategies
Advanced System Management processor (ASM processor)	<ul style="list-style-type: none"> Over an ASM interconnect to either an ASM PCI adapter or a Remote Supervisor Adapter 	IBM Director over LAN
Advanced System Management PCI Adapter (ASM PCI adapter)	<ul style="list-style-type: none"> LAN Over an ASM interconnect to either an ASM PCI adapter or a Remote Supervisor Adapter 	IBM Director over LAN
Remote Supervisor Adapter Remote Supervisor Adapter II	<ul style="list-style-type: none"> LAN Over an ASM interconnect to either an ASM PCI adapter or a Remote Supervisor Adapter 	IBM Director comprehensive or IBM Director over LAN, depending on the firmware present on the Remote Supervisor Adapter

Table 8. Out-of-band communication pathways and alert-forwarding strategies (continued)

Type of service processor	Pathways for out-of-band communication	Possible alert-forwarding strategies
Integrated system management processor (ISMP)	<ul style="list-style-type: none"> Over an ASM interconnect to a Remote Supervisor Adapter 	IBM Director comprehensive or IBM Director over LAN, depending on the firmware present on the Remote Supervisor Adapter

See the documentation that came with your server for information about how to configure your service processor and ASM interconnect to ensure that IBM Director Server receives alerts. The IBM Redbooks publication *Implementing Systems Management Solutions Using IBM Director* (SG24-6188-01) also contains information that might be helpful. See “IBM Director resources on the World Wide Web” on page xv for more information.

The following table details which service processors, when connected over a LAN to IBM Director Server, can communicate with service processors connected to an ASM interconnect network.

Table 9. Whether service processors connected over LAN to IBM Director Server can communicate with service processors on the ASM interconnect

Service processor connected over LAN to IBM Director Server	Systems connected to the ASM interconnect				
	ISMP	ASM processor	ASM PCI adapter	Remote Supervisor Adapter	Remote Supervisor Adapter II
ASM PCI adapter	No	Yes	Yes	No	No
Remote Supervisor Adapter	Yes	Yes	Yes	Yes	Yes
Remote Supervisor Adapter II	Yes	Yes	Yes	Yes	Yes

In general, IBM Director Server can communicate over the LAN to a service processor, which in turn can communicate with service processors on the ASM interconnect network. However, when IBM Director Server uses interprocess communication to connect to a service processor, communication with other service processors on the ASM interconnect network is not supported.

Service processors in IBM Nefinity and xSeries servers

The following table provides information about the service processors that are, or can be, installed in IBM Nefinity and xSeries servers.

Table 10. Service processors in IBM Nefinity and xSeries systems

Server	ISMP	ASM processor	ASM PCI Adapter	Remote Supervisor Adapter
Netfinity 1000	No	No	No	No
Netfinity 3000	No	No	No	No

Table 10. Service processors in IBM Netfinity and xSeries systems (continued)

Server	ISMP	ASM processor	ASM PCI Adapter	Remote Supervisor Adapter
Netfinity 3500 family (3500 /M10/M20)	No	No	No	No
Netfinity 4000R	No	No	No	No
Netfinity 4500R	No	Standard	Optional	No
Netfinity 5000	No	Standard	Optional	No
Netfinity 5100	No	Standard	Optional	No
Netfinity 5500 family (5500, M10, M20)	No	Standard	Optional	No
Netfinity 5600	No	Standard	Optional	No
Netfinity 6000R	No	Standard	Optional	No
Netfinity 7000	No	No	No	No
Netfinity 7000 M10	No	No	Standard	No
Netfinity 7100	No	Standard	Optional	No
Netfinity 7600	No	Standard	Optional	No
Netfinity 8500R	No	No	Standard	No
xSeries 130 Value Line (8672)	No	No	No	No
xSeries 130 Performance Line (8654)	No	Standard	No	No
xSeries 135 Value Line	No	No	No	No
xSeries 135 Performance Line	No	Standard	No	No
xSeries 150	No	Standard	No	No
xSeries 200	No	No	No	No
xSeries 205	No	No	No	Optional
xSeries 220	No	No	No	Optional
xSeries 225	No	No	No	Standard
xSeries 230	No	Standard	Optional	No
xSeries 232	Standard	No	No	Optional
xSeries 235	Standard	No	No	Optional
xSeries 240	No	Standard	Optional	No
xSeries 250	No	Standard	Optional	No
xSeries 255	Standard	No	No	Optional
xSeries 300	No	No	No	No
xSeries 305	No	No	No	Optional
xSeries 330 (8654)	No	Standard	Optional	Optional
xSeries 330 (8674)	No	Standard	Optional	Optional
xSeries 330 (8675)	No	Standard	Optional	Optional
xSeries 335 (8676)	Standard	No	No	Optional
xSeries 340	No	Standard	Optional	No

Table 10. Service processors in IBM Netfinity and xSeries systems (continued)

Server	ISMP	ASM processor	ASM PCI Adapter	Remote Supervisor Adapter
xSeries 342	Standard	No	No	Optional
xSeries 343	No	No	No	No
xSeries 345	Standard	No	No	Optional
xSeries 350	No	Standard	Optional	No
xSeries 360	No	No	No	Standard
xSeries 370	No	No	Standard	No
xSeries 380	No	No	No	No
xSeries 440	No	No	No	Standard
xSeries 450	No	No	No	Standard

Updating Remote Supervisor Adapter firmware

If your server has a Remote Supervisor Adapter and is one of the following systems, consider updating the service processor firmware:

- xSeries 235
- xSeries 255
- xSeries 335
- xSeries 345
- xSeries 360

Installing updated firmware will activate additional IBM Director features. Then, you can use IBM Director to perform the following tasks:

- Discover the Remote Supervisor Adapter before an operating system or IBM Director Agent is installed on the server.
- Automatically add the system from which you performed the discovery operation as an alert destination for the Remote Supervisor Adapter. All supported alerts then are sent to that system.
- Generate additional recovery alerts and more-detailed hardware alerts. For example, fan Predictive Failure Analysis[®] (PFA) alerts are detected and displayed in the Hardware Status task window as warning-level events.

To update the firmware, download the applicable update from the IBM Support Web site at <http://www.ibm.com/pc/support/>. The following table contains the part numbers for the firmware update.

Table 11. Part numbers for Remote Supervisor Adapter firmware updates

Server model	Firmware update part number	Firmware version
xSeries 235	74p4808 and 74p809	1.03 or later
xSeries 255	90p515 and 90p516	1.03 or later
xSeries 335	74p4841	1.03 or later
xSeries 345	74p4810 and 74p4811	1.05 or later
xSeries 360	90p4125 and 90p4126	1.08 or later

If a search on a firmware update part number fails, a later version of the firmware is available. Search the IBM Support Web site using your server model number; then, check for a later version of the firmware.

Setting up a BladeCenter deployment infrastructure

If you want to use IBM Director to manage the blade servers in a BladeCenter chassis, you must use a non-blade server as the management server.

Consider setting up a separate management network to configure and manage your BladeCenter chassis and blade servers. By separating the LAN segment used for production from the LAN segment to which the BladeCenter management module is connected, you can ensure that only authorized system administrators can connect to the BladeCenter chassis and switch modules.

Figure 3 shows a network that you could use to securely deploy your BladeCenter chassis and blade servers.

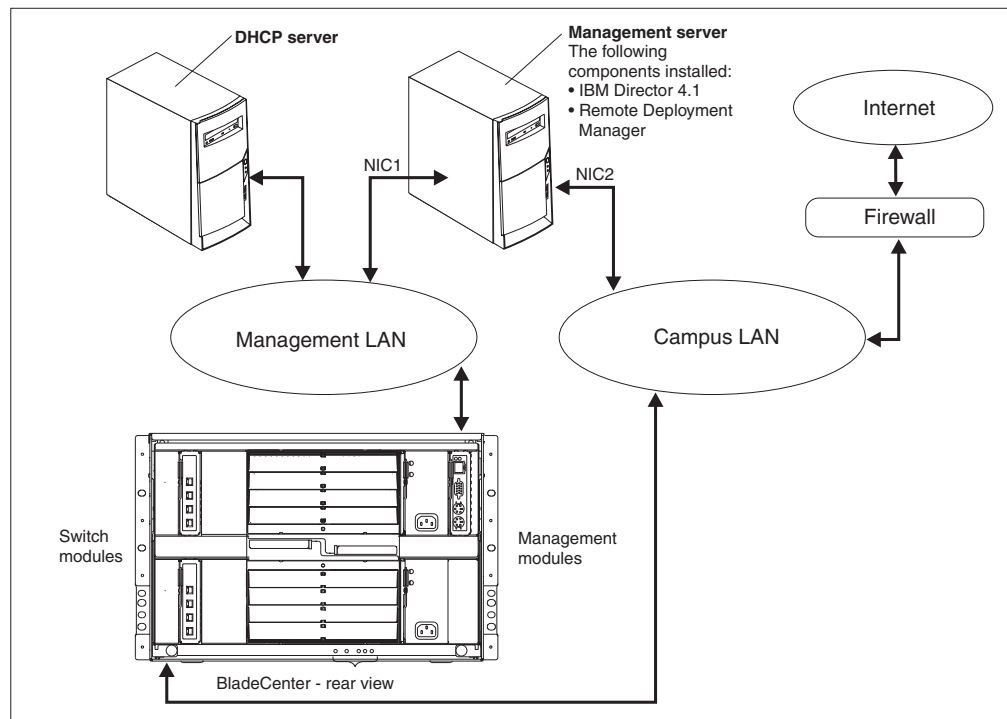


Figure 3. Example of a BladeCenter deployment network

Such a network configuration ensures that applications running on the blade servers cannot modify chassis settings, because the blade servers have no connection to either the management module or the switch module configuration ports.

Consider using a Dynamic Host Configuration Protocol (DHCP) server to assign a temporary address to the external port of the management module. When a BladeCenter management module is first started, it searches for a DHCP server. If a DHCP server is not found, the BladeCenter management module assigns a nonroutable IP address (192.168.70.125) to the external management port. Because this static IP address is the same for all management modules, IP address conflicts can occur if you do not use a DHCP server and introduce multiple BladeCenter chassis onto a network simultaneously. When you run the BladeCenter Deployment wizard and configure the BladeCenter chassis, you assign static IP addresses to the switch module and the external and internal ports of the management module.

If you intend to use Remote Deployment Manager (RDM), install RDM 4.1 on the management server also.

If you plan to use a database application other than Microsoft Jet, consider installing the database server on the management LAN also. If the database server is in a different domain, there must be a trust relationship between the two domains.

Make sure that you have installed the latest version of the management module firmware. To download the firmware, go to the IBM Support Web site at <http://www.ibm.com/pc/support/>.

Only one management server can communicate with the BladeCenter management module at any one time.

Database management

IBM Director supports the following database applications:

- Microsoft Jet 4.0 database engine, Service Pack 6, and Microsoft Data Access Control (MDAC) 2.7 (Windows only)
- Microsoft Data Engine (MSDE) 1.0, Service Pack 3, and MDAC 2.7 (Windows only)
- Microsoft SQL Server 2000 Desktop Engine, Service Pack 3, and MDAC 2.7 (Windows only)
- Microsoft SQL Server 7.00, Service Pack 3, and MDAC 2.7 (Windows only)
- Microsoft SQL Server 2000, Service Pack 3, and MDAC 2.7 (Windows only)
- IBM DB2 Universal Database 6.1, Fix Pack 11 (Windows only)
- IBM DB2 Universal Database 7.2, Fix Pack 9
- IBM DB2 Universal Database 8.1, Fix Pack 2
- Oracle Server, versions 8.1.7 and 9.0.x
- PostgreSQL, versions 7.2 and 7.3 (Linux only)

If you plan to use a database application other than Microsoft Jet, your database administrator must prepare the database application before you install IBM Director Server.

Determine an appropriate size for the database file. If you intend to manage 300 to 500 systems, an initial size of 100 MB is sufficient. You might need a larger database if you manage additional systems or have extensive inventory data.

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

Microsoft Jet 4.0

If the management server is running Windows 2000 or Windows 2003, you can use Microsoft Jet 4.0 as the IBM Director database. The Microsoft Jet 4.0 database engine is built into Windows 2000 and will create a single database file that is installed on the management server. The database has a maximum size of 2.14 GB. If you plan to manage more than 300 to 500 systems, use another database application.

Microsoft Data Engine 1.0 or SQL Server 2000 Desktop Engine

If you plan to use Microsoft Data Engine 1.0 or SQL Server 2000 Desktop Engine, install the database application before installing IBM Director.

Microsoft SQL Server

Note: If the management server and the database server are located in different domains, the following conditions apply:

- The IBM Director service account must be a domain account.
- There must be a trust relationship between the domains.

Complete the following tasks before installing IBM Director Server:

1. Install SQL Server on the database server, if you have not already done so.
2. Set the security levels for the database server. If you use trusted connections, set the database server security to support trusted connections. (If you configure the database server for mixed security, you also must authorize the IBM Director service account to access SQL Server.)
3. Authorize the IBM Director service account to log on to SQL Server.
4. Complete one of the following tasks:
 - Assign the IBM Director service account Create Database permission in the master database. This allows the SQL Server database to be created *during* the installation of IBM Director. When the database is created during the IBM Director installation, the size of the database defaults to the larger of the following sizes:
 - The size of the model database
 - The default database size specified in the SQL Server configuration options
 - Create the SQL Server database. Either transfer ownership of the database to the IBM Director service account or give the IBM Director service account user-level access to the database and Create Table permission. Provide the host name of the database server and the name of the database to the system administrator who will install IBM Director Server.

IBM DB2 Universal Database

You can use IBM DB2 Universal Database with management servers running either Windows or Linux.

Configuring a management server running Windows to use DB2

Notes:

1. If you have a remote connection to DB2, you must have a node entry for the database server.
2. If the management server and the database server are located in different domains, the following conditions apply:
 - The IBM Director service account must be a domain account.
 - There must be a trust relationship between the domains.

Complete the following tasks before installing IBM Director Server:

1. Install DB2 Universal Database on the database server, if you have not done so already.
2. Install the DB2 Administration Client on the management server. Be sure to install the following components.

Version 6.1	Version 7.2
<ul style="list-style-type: none"> • Communications protocols • ODBC support • Java enablement • System bind files • Fix Pack 11 	<ul style="list-style-type: none"> • Communications protocols • Applications development interface • Base DB2 client support • System bind files • Fix Pack 9

3. Copy the db2schem.bnd file to the management server. This file is located in the SQLLIB\bnd\ directory on the DB2 server. Be sure to duplicate that directory structure on the management server.
4. Verify that the CLASSPATH statement points to the db2java.zip directory that contains the DB2 Java Database Connectivity (JDBC) driver.
5. Configure DB2 to use the JDBC 2.0 driver. For more information about the JDBC 2.0 driver, see the release notes for DB2, version 7.2. You can download these release notes from the IBM Web site at <http://www.ibm.com>. In the **Search** field, type JDBC 2.0 driver and press Enter.
6. From a command prompt, type the following command and press Enter:


```
cd sqllib\java12
```

where *sqllib* is the directory where DB2 is installed.
7. Ensure that the DB2 JDBC Applet Server and the DB2 JDBC Applet Server-Control Center services are stopped.
8. From the command prompt, type the following command and press Enter:


```
usejdbc2
```

This command creates a sqllib\java11 directory, backs up the JDBC 1.22 driver files into the sqllib\java11 directory, and makes the JDBC 2.0 driver the default.
9. Verify that all of the files are copied to the sqllib\java and sqllib\bin directories. If Access is denied. The process cannot access the file because it is being used by another process. is displayed, one or more services might be running. Complete the following steps:
 - a. From the "Windows Services" window, stop all DB2 services.
 - b. From a command prompt, type the following command and press Enter:


```
usejdbc2
```
 - c. If errors continue, issue the db2stop force command and issue the usejdbc2 command again.
10. If you use trusted connections, set the database server security to support trusted connections. See the *DB2 Administration Guide* for information about trusted DB2 client scenarios.
11. Authorize the IBM Director service account to log on to DB2. See the *DB2 Administration Guide* for additional information about DB2 security.

12. Complete one of the following tasks:
 - Assign the IBM Director service account Create Database permission. This allows the DB2 database to be created *during* the installation of IBM Director Server.
 - Create the DB2 database. Either transfer ownership of the database to the IBM Director service account or give the IBM Director service account user-level access to the database, as well as Create Table permission. Provide the host name of the database server and the name of the database to the system administrator who will install IBM Director Server.

Configuring a management server running Linux to use DB2

Notes:

1. Verify that you have installed the correct level of the Fix Pack 8. See “Database management” on page 29 for more information.
2. If you have a remote connection to DB2, you must have a node entry for the database server.

Complete the following steps before you install IBM Director Server:

1. Install DB2 Universal Database, if you have not done so already.
2. Verify that the DB2 Administration Client is installed on the management server.
3. Give root the appropriate DB2 authority.

Oracle Server

Note: IBM Director is certified to run with the Oracle *9i* JDBC driver, version 9.0.1 for use with Java Development Kit (JDK) 1.2 and 1.3 *only*.

Complete the following tasks before installing IBM Director Server:

1. Install Oracle Server, if you have not done so already.
2. Verify that the JDBC Thin Driver version 9.0.1 is installed. You can download it from <http://www.otn.oracle.com/software/content.html>.
3. (Windows only) Verify that the CLASSPATH statement points to the fully qualified name of the file that contains the Oracle JDBC driver, for example *d:\oracle\lib\classes12.zip*, where *d* is the drive letter of the hard disk drive where Oracle Server is installed.
4. Create the Oracle Server database.
5. Configure and start the Oracle TCP/IP listener.

Note: The Oracle JDBC driver does not require Oracle client software to be installed. However, it does require that the Oracle Server be configured with a TCP/IP listener.

6. Provide the following information to the system administrator who will install IBM Director Server:
 - Oracle TCP/IP listener port
 - TCP/IP host name of the Oracle Server
 - Oracle system identifier
 - Oracle administrator account ID and password

The Oracle administrator account ID and password are used to create tablespaces and a role (TWG_ROLE) and to assign a user ID and password. IBM Director *does not* save the Oracle administrator account ID and password.

PostgreSQL

Complete the following tasks before installing IBM Director Server:

1. Install PostgreSQL, if you have not done so already. The IBM Redbooks publication *Implementing Systems Management Solutions Using IBM Director* (SG24-6188-01) contains tips and additional information that might be helpful. See “IBM Director publications” on page xiv for more information.
2. Verify that the JDBC driver for PostgreSQL, version 7.2 is installed. You can download it from <http://www.jdbc.postgresql.org/>.
3. Verify that the PostgreSQL postmaster is running with the `-i` flag.

IBM Director security

IBM Director offers several security features, including user-administration options that enable system administrators to specify user privileges, support for secure socket layers (SSL), and optional encryption of interprocess communication.

IBM Director service account (Windows only)

Before installing IBM Director Server, create an operating-system user account with local administrator privileges on the management server. This account is the *IBM Director service account*. Use this account to install IBM Director Server. The IBM Director Server service runs as this account, so consider selecting **Password never expires** when you create the account.

Note: It is a best practice to use the IBM Director service account *only* for IBM Director system administration.

IBM Director user accounts

IBM Director user accounts are based upon the underlying operating-system accounts. When IBM Director Server is installed, two groups of IBM Director users are automatically created: DirAdmin and DirSuper. Members of the DirAdmin group have general access to IBM Director, whereas members of the DirSuper group have the additional ability to create and edit user profiles.

On Windows, the IBM Director service account is automatically assigned to the DirSuper group and all accounts with administrator privileges are automatically assigned to the DirAdmin group. You can manually add users to either the DirAdmin or DirSuper group, but you cannot remove users with administrator privileges on the underlying operating system from the DirAdmin group.

On Linux, the groups are not automatically populated. A user with root privileges must assign users to the appropriate groups.

IBM Director Console – IBM Director Server security

You can use SSL to protect data flowing between IBM Director Server and IBM Director Console.

IBM Director supports the following cipher suites:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SH
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_WITH_NULL_MD5
- SSL_RSA_WITH_NULL_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

Encryption

IBM Director contains a new security feature that encrypts all data in interprocess communications, except for the transport-layer datagrams used during discovery. This encryption feature provides automatic key management and enables the user to select an encryption algorithm from the provided libraries: IBM Java Cryptography Extensions (JCE) and OpenSSL. JCE provides ciphers for all Java-based platforms, including Linux and Open UNIX; OpenSSL provides ciphers for Windows.

Encryption is disabled by default. To encrypt data transmitted between IBM Director Agent and IBM Director Server, you must enable encryption on both IBM Director Server and IBM Director Agent.

When installing IBM Director Server, you can select one of the following encryption algorithms: data encryption standard (DES) and triple DES. IBM Director Server automatically generates a key, based on the encryption algorithm selected. IBM Director Server stores the key in memory and presents it to IBM Director Agent each time IBM Director Agent is started, using the Diffie-Hellman key exchange. This makes it unnecessary for a key to be stored on each managed system.

The following table outlines how data is transmitted between IBM Director Server and IBM Director Agent.

	IBM Director Agent (encryption enabled)	IBM Director Agent (encryption disabled)
IBM Director Server (encryption enabled)	Encrypted	Unencrypted
IBM Director Server (encryption disabled)	No data transmission possible	Unencrypted

An exception to the matrix described in the table is the following scenario: There are two management servers. Encryption is disabled on one (server A) and enabled on the other (server B). Server A is authorized to manage server B, *and* server B is authorized to manage server B. Unencrypted transmissions sent by server A to server B are not rejected, despite the fact that server B had elected to encrypt all data transmissions. This occurs because server B, in its role as management server, is already communicating with server A (in its role as managed system) in plain text.

Notes:

1. Encryption is not supported on managed systems running NetWare or using SNA as a network protocol.
2. Neither out-of-band communications nor communication used by Internet tools, such as Telnet or File Transfer Protocol (FTP), are encrypted.
3. Enabling encryption imposes a performance penalty. Encrypting data packets and exchanging encryption keys has an effect on the speed with which IBM Director completes management operations. When either the management server or the managed systems are restarted, keys are regenerated and exchanged. Consequently, an unsecured managed system might appear to be unmanageable for a period of time.

Web-based Access security

To use Web-based Access, a user must log in to an operating-system account on the local system. When the user is logged in, user privileges are based on operating-system privileges. Users with Administrator authority can use Web-based Access to modify system settings, but users with User authority can view system settings only.

Part 2. Installing IBM Director

Chapter 4. Installing IBM Director Server

This chapter contains instructions for installing IBM Director Server. If you are upgrading from IBM Director 3.x or later, go to Chapter 10, “Upgrading IBM Director Server”, on page 135.

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

- Microsoft Windows 2000 Server and Advanced Server (Service Pack 3 required)
- Windows Server 2003 (Standard, Enterprise, and Web Editions)
- Red Hat Linux, version 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- SuSE Linux, version 8.0
- SuSE Linux Enterprise Server, version 8.0

Before you install IBM Director Server, verify that you have performed any necessary preinstallation steps. See “Database management” on page 29 for more information.

Installing IBM Director Server on Windows

This section provides instructions for installing IBM Director Server. When you install IBM Director Server, the InstallShield wizard also automatically installs IBM Director Console and IBM Director Agent. During the installation process, you can install the Server Plus Pack extensions and several IBM Director Agent features.

Note: Earlier versions of Active PCI Manager are not compatible with IBM Director. Before you install IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.

Complete the following steps to install IBM Director Server:

1. Log on to the operating system with the IBM Director service account. For more information, see “IBM Director service account (Windows only)” on page 33.
2. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
3. If the installation program starts automatically and the InstallShield wizard starts, go to step 5. Otherwise, click **Start** → **Run**.
4. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

5. Click **Install IBM Director**. The “IBM Director Installation” window opens.
6. Click **IBM Director Server installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
7. Click **Next**. The “License Agreement” window opens.
8. Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.

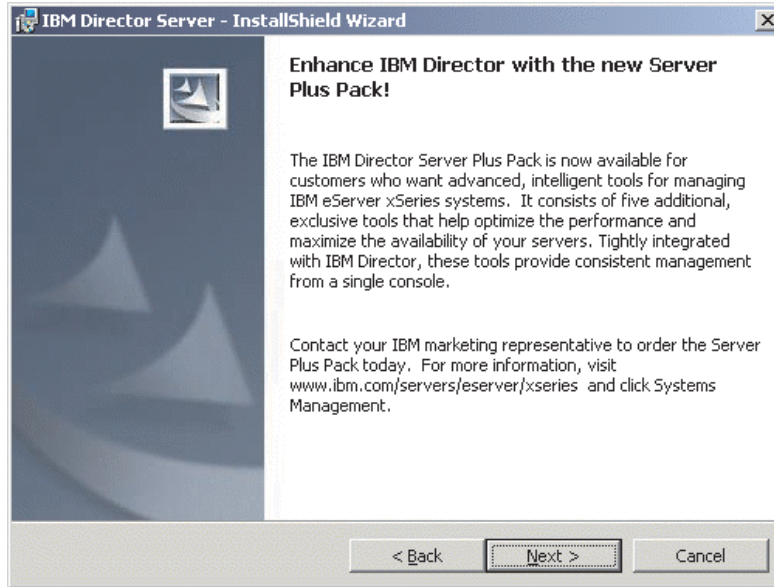


Figure 4. Installing IBM Director Server on Windows: “Server Plus Pack” window

9. Click **Next**. The “Feature and installation directory selection” window opens.

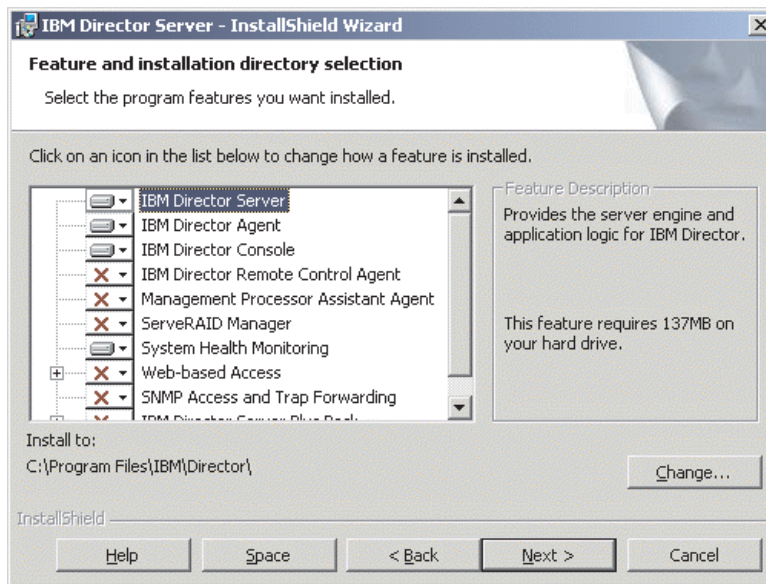




Figure 5. Installing IBM Director Server on Windows: “Feature and installation directory selection” window

IBM Director Server, IBM Director Agent, and IBM Director Console are selected automatically for installation; a hard disk drive icon  is displayed to the left of each component.  is displayed to the left of the optional features not selected by default.

You can install the following optional features:

IBM Director Remote Control Agent

Enables a system administrator to perform remote desktop functions on a managed system.

Management Processor Assistant Agent

Enables communication with service processors in IBM xSeries and Netfinity servers.

ServeRAID Manager

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities.

System Health Monitoring


Monitors the status of hardware components, produces and relays hardware alerts, and facilitates upward integration.

Web-based Access

Enables a system administrator to access the managed-system data through a Web browser or the Microsoft Management Console (MMC).

SNMP Access and Trap Forwarding

Enables access to managed-system data and alerts through SNMP.

10. To select a feature, click  to the left of the feature name. A menu opens.

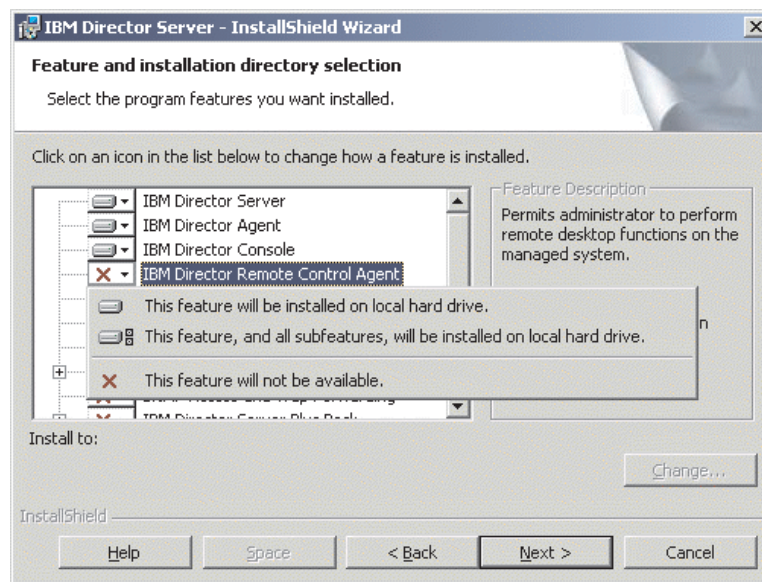


Figure 6. Installing IBM Director Server on Windows: “Features and installation directory selection” window

To select the feature, click **This feature will be installed on local hard drive** or **This feature, and all its subfeatures, will be installed on local hard drive**.

11. Select the Server Plus Pack extensions that you want to install:

Capacity Manager

Tracks system resource utilization, identifies bottlenecks, and provides performance information.

Rack Manager

Manages IBM servers, storage devices, and other components located in an IBM enclosure.

Active PCI Manager

Manages PCI and PCI-X adapters in managed systems.

Software Rejuvenation

Schedules restarts of managed systems.

System Availability

Determines availability of managed systems and provides statistical data.

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all its subfeatures, will be installed on local hard drive**. Otherwise, select the Server Plus Pack extensions individually.

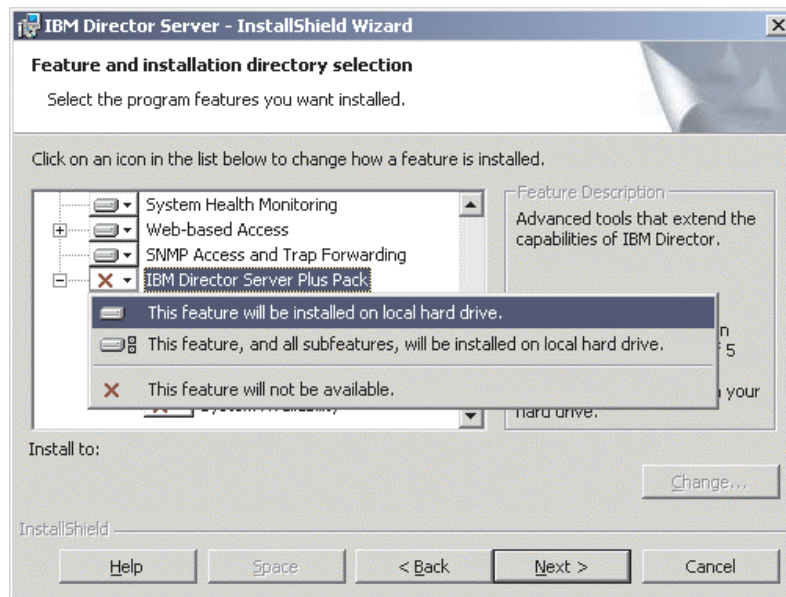


Figure 7. Installing IBM Director Server on Windows: Installing the Server Plus Pack

Notes:

- a. Rack Manager will not function until the Rack Manager component, located on the *IBM Director Server Plus Pack* CD, is installed on the management server.
 - b. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.
12. Click **Next**. The “IBM Director service account information” window opens. (For more information about the IBM Director service account, see “IBM Director security” on page 33.)

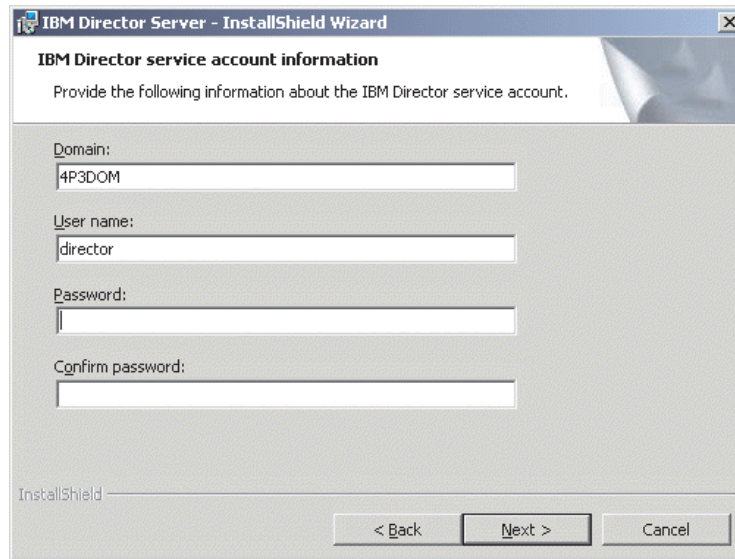


Figure 8. Installing IBM Director Server on Windows: “IBM Director service account information” window

13. Type information about the IBM Director service account:
 - a. In the **User Name** field, type the user ID for the IBM Director service account.
 - b. In the **Domain** field, type the domain of the IBM Director service account.
 - c. In the **Password** and **Confirm Password** fields, type the password for the IBM Director service account.

Note: The domain, user name, and password information must correspond to a Windows account with administrator privileges on the management server. Otherwise, the installation will fail.

14. Click **Next**. The “Encryption settings” window opens.

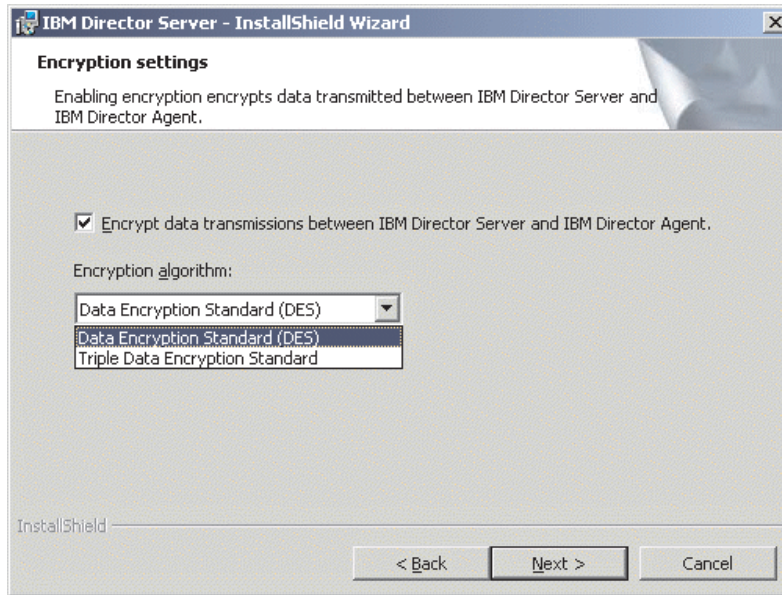


Figure 9. Installing IBM Director Server on Windows: “Encryption settings” window

15. To encrypt data transmitted between IBM Director Server and IBM Director Agent, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box; then, select the encryption algorithm.
16. Click **Next**. The “Software-distribution settings” window opens.

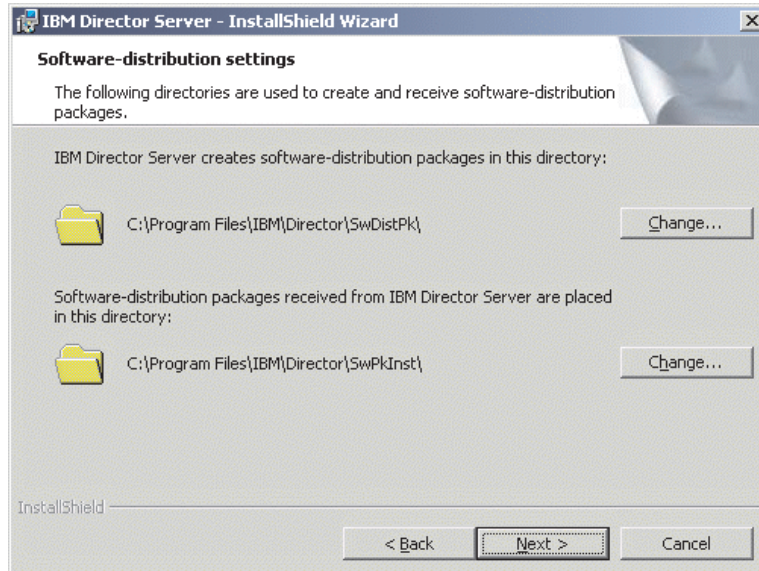


Figure 10. Installing IBM Director Server on Windows: “Software-distribution settings” window

17. To select an alternative location for where IBM Director Server creates software-distribution packages, click **Change** and select another directory. To select an alternative location for where software-distribution packages received from IBM Director Server are placed, click **Change** and select another directory.

18. Click **Next**. If you did not select to install the Web-based Access feature, the “Ready to Install the Program” window opens; go to step 20. Otherwise, the “Web-based Access information” window opens.

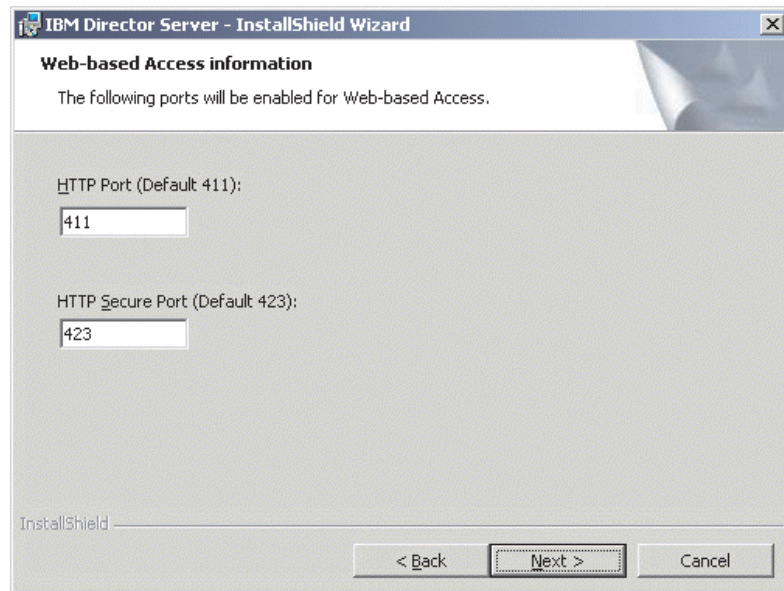


Figure 11. Installing IBM Director Server on Windows: “Web-based Access information” window

19. Change the default HTTP ports (if necessary); then, click **Next**. The “Ready to Install the Program” window opens.
20. Click **Install**. The “Installing IBM Director Server” window opens. The progress of the installation is displayed in the **Status** field. When the installation is completed, the “Network driver configuration” window opens.

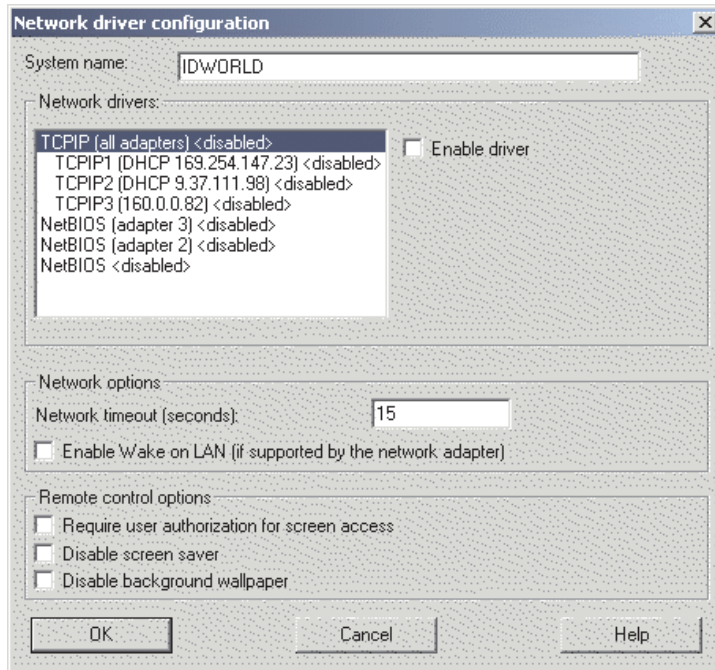


Figure 12. Installing IBM Director Server on Windows: “Network driver configuration” window

21. In the **System name** field, type the name that you want displayed in IBM Director Console. By default, this is the NetBIOS name of the management server.
22. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
 - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

Note: If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Server will receive data packets addressed to the individual adapter *only*.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
 - c. Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN[®] feature.

Note: To determine whether your server supports the Wake on LAN feature, see your server documentation.

23. If you selected to install the IBM Director Remote Control Agent, the following options are available:

Require user authorization for system access

Select this check box to request authorization from the local user before controlling a managed system remotely.

Disable screen saver

Select this check box to disable the screen saver on the managed system being controlled remotely.

Disable background wallpaper

Select this check box to disable desktop wallpaper on the managed system being controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

24. Click **OK**. The “IBM Director database configuration” window opens.

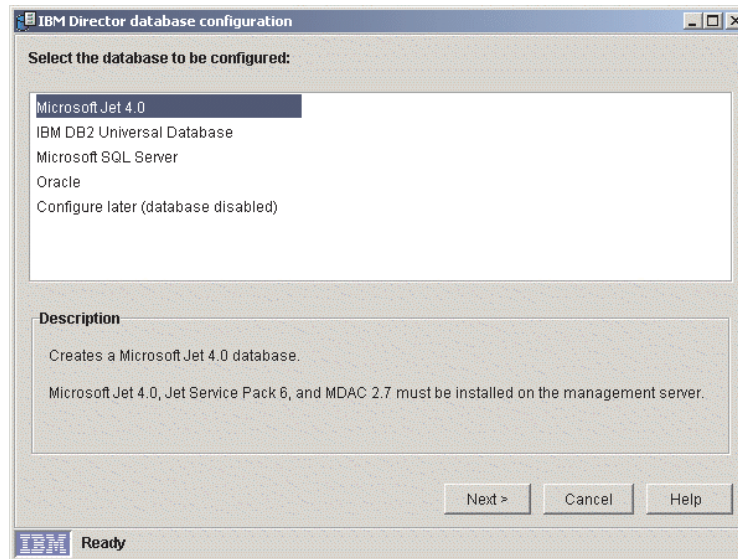


Figure 13. Installing IBM Director Server: “IBM Director database configuration” window

25. Click the database application you want to use with IBM Director. You have the following options:

Microsoft Jet 4.0

Creates a Microsoft Jet 4.0 database. Microsoft Jet 4.0, Jet Service Pack 6, and MDAC 2.7 must be installed on the management server.

IBM DB2 Universal Database

Creates a DB2 database. Either DB2 Administration Client or IBM DB2 Universal Database must be installed and configured on the management server.

Microsoft SQL Server

Creates a Microsoft SQL Server database. Microsoft SQL Server must be installed and configured on a system in your network.

Oracle

Configures an Oracle database. Oracle must be installed and configured on a system in your network.

Configure later (database disabled)

IBM Director will be installed without a database. Tasks requiring a database will be absent or not functional.

26. Click **Next** and begin configuring the IBM Director database.

If you selected	Go to
Microsoft Jet 4.0	Step 32 on page 51
IBM DB2 Universal Database	Step 27
Microsoft SQL Server	Step 29
Oracle	Step 30 on page 49
Configure later (database disabled)	Step 32 on page 51

27. The “IBM Director DB2 Universal Database configuration” window opens.

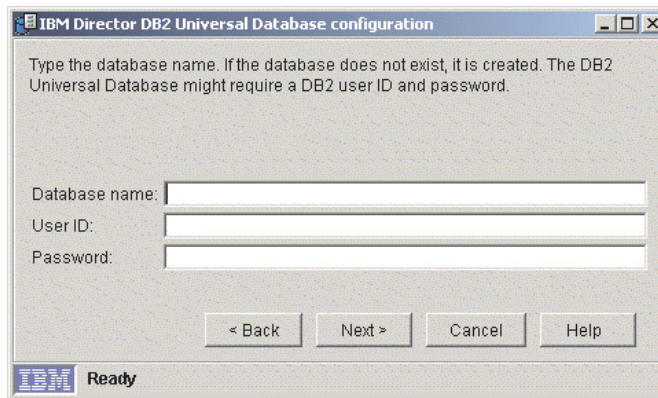


Figure 14. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window

Type information in the following entry fields:

- In the **Database name** field, type the name of the database. If it does not exist, it will be created.
- In the **User ID** field, type a valid DB2 user ID.
- In the **Password** field, type the password for the DB2 user ID.

28. Click **Next**. The second “IBM Director DB2 Universal Database configuration” window opens.



Figure 15. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window

In the **DB2 node name** field, select the location of the DB2 database. Then click **OK** and go to step 32 on page 51.

29. The “IBM Director Microsoft SQL Server database configuration” window opens.

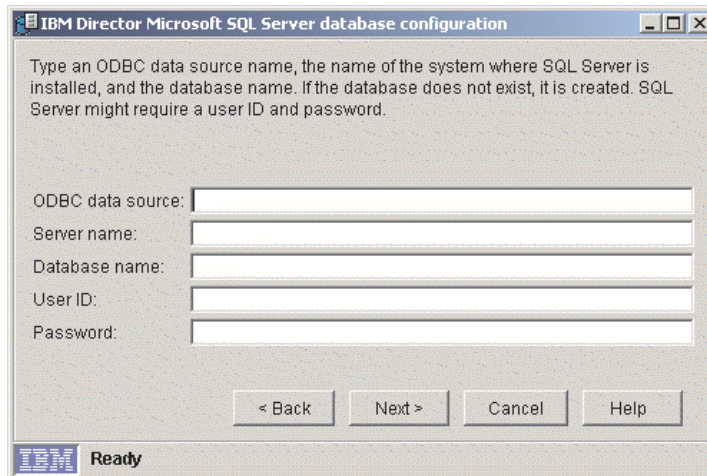


Figure 16. Installing IBM Director Server: “IBM Director Microsoft SQL Server database configuration” window

Type information in the following entry fields:

- a. In the **ODBC data source** field, type the ODBC data source name. If it does not exist, it will be created.
- b. In the **Server name** field, type the name of the server where SQL Server is installed.
- c. In the **Database name** field, type name of the database. If it does not exist, it will be created.
- d. In the **User ID** field, type a valid SQL Server user ID.
- e. In the **Password** field, type the password for the SQL Server user ID (if required).

Click **Next**. Go to step 32 on page 51.

30. The “IBM Director Oracle database configuration” window opens.

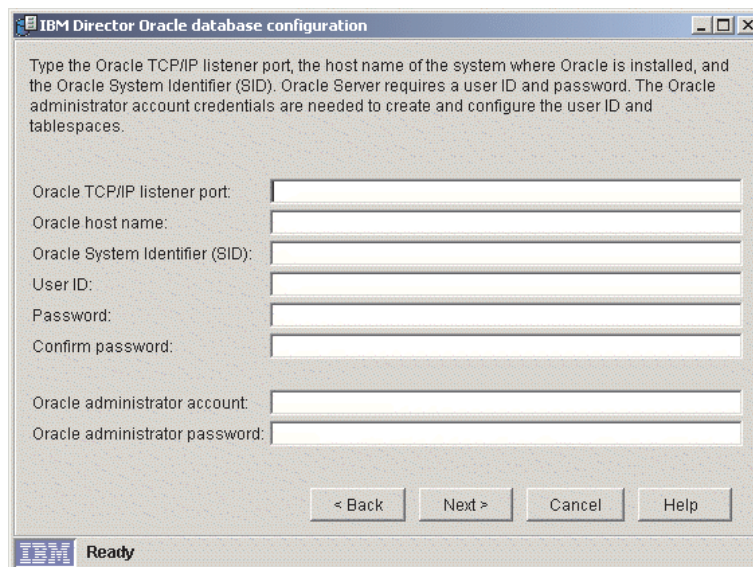


Figure 17. Installing IBM Director Server: “IBM Director Oracle database configuration” window

Type information in the following entry fields:

- a. In the **Oracle TCP/IP listener port** field, type the number of the port used by the Oracle TCP/IP listener.
 - b. In the **Oracle host name** field, type the TCP/IP host name of the Oracle Server.
 - c. In the **Oracle System Identifier (SID)** field, type the Oracle system identifier (SID).
 - d. In the **User ID** field, type a valid Oracle user ID. If it does not exist, it is created. By default, this user ID is assigned to the IBM Director tablespace.
 - e. In the **Password** and **Confirm password** fields, type the password associated with the user ID you typed in step 30d.
 - f. In the **Oracle administrator account** field, type a valid Oracle administrator account user ID.
 - g. In the **Oracle administrator password** field, type the password associated with the user ID you typed in step 30f.
31. Click **Next**. The second “IBM Director Oracle database configuration” window opens.

Tablespace information

Type the tablespace name, data-file location, and data-file size. You can use the default information provided.

If you do not specify a directory path, the tablespace data files will be created in the Oracle default directory. If you specify a directory path and it cannot be found, the Oracle configuration will fail.

Default tablespace name:

Default tablespace data file:

Default tablespace size (MB):

Temporary tablespace information

Type the temporary tablespace name, data-file location, and data file. You can use the default information provided.

If you do not specify a directory path, the temporary tablespace data files will be created in the Oracle default directory. If you specify a directory path and it cannot be found, the Oracle configuration will fail.

Temporary tablespace name:

Temporary tablespace data file:

Temporary tablespace size (MB):

OK Cancel Help

Figure 18. Installing IBM Director Server: “IBM Director Oracle database configuration” window

Type information in the following entry fields:

- a. In the **Default tablespace name** field, type a tablespace name.
- b. In the **Default tablespace data file** field, type the name of the tablespace data file. If you do not specify the directory path, the tablespace data file will be created in the Oracle Server default directory. If you specify an invalid directory path, the database configuration will fail.
- c. In the **Default tablespace size (MB)** field, type the size of the tablespace in MB.

- d. In the **Temporary tablespace name** field, type a name for the temporary tablespace.
 - e. In the **Temporary tablespace data file** field, type the name of the temporary tablespace data file. If you do not specify the directory path, the tablespace data file will be created in the Oracle Server default directory. If you specify an invalid directory path, the database configuration will fail.
 - f. In the **Temporary tablespace size (MB)** field, type the size of the temporary tablespace in MB.
32. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
 33. Click **Finish**. A window opens, asking you if you want to restart the server.
 34. Remove the *IBM Director 4.11* CD from the CD-ROM drive.
 35. Click **Yes** to restart the server.

For instructions on how to install IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 121 and “Installing Software Distribution (Premium Edition)” on page 122.

Installing IBM Director Server on Linux

Complete the following steps to install IBM Director Server on Linux:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. If you want to customize the installation, go to step 6. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 18 on page 53.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the `dirinstall` script. This file is fully commented.

You can specify the location of the Red Hat Package Manager (RPM) files, select the IBM Director extensions and features that you want to install, and select log file options.

8. Save the modified installation script.
9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. Prepare to configure your database application for use with IBM Director.

If the database application is	Go to
IBM DB2 Universal Database	Step 11
Oracle Server	Step 13
PostgreSQL	Step 15
Configure later (database disabled)	Step 18 on page 53

11. (DB2 only) Create a `/etc/TWGserver/setup_env` file. Add the following statements to the file:

```
. /home/db2inst1/sql1lib/db2profile
. /home/db2inst1/sql1lib/java12/usejdbc2
```

where *home/db2inst1* is the directory where DB2 is installed. These statements set up the DB2 environment and configure DB2 to use the JDBC 2.0 driver.

12. Set the `setup_env` file attributes to read-execute. Go to step 18 on page 53.
13. (Oracle only) Create a `/etc/TWGserver/setup_env` file. Add the following statements to the file:

```
CLASSPATH=filename
export CLASSPATH
```

where *filename* is the fully qualified name of the Oracle JDBC driver, for example, `/opt/oracle/lib/classes12.zip`.

14. Set the `setup_env` file attributes to read-execute. Go to step 18 on page 53.
15. (PostgreSQL only) If the PostgreSQL JDBC driver is named `postgresql.jar`, go to step 16. Otherwise, you must create a symbolic link. From a command prompt, type the following command and press Enter:

```
ln -s realname path/postgresql.jar
```

where *realname* is the fully qualified name of the PostgreSQL JDBC driver, for example, `/opt/postgres/lib/jdbc7.1-2.jar`, and *path* is the path of the symbolic link, for example, `/opt/postgres/lib/`.

16. Create a `/etc/TWGserver/setup_env` file. Add the following statement to the file:

```
export CLASSPATH=path/postgresql.jar
```

where *path* is the path of the PostgreSQL JDBC driver, for example, `/opt/postgres/lib`.

Note: If you created a symbolic link in step 15, *path* is the path of the symbolic link.

17. Set the `setup_env` file attributes to read-execute.

18. To configure the database for use with IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgdb
```

Follow the instructions on the screen.

19. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```

20. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

21. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.

- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

22. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

For instructions on how to install IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 121 and “Installing Software Distribution (Premium Edition)” on page 122.

Chapter 5. Installing IBM Director Console

This chapter contains instructions for installing IBM Director Console. If you are upgrading from IBM Director 3.x or later, go to Chapter 11, “Upgrading IBM Director Console”, on page 145.

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

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)
- Windows Server 2003 (Standard, Enterprise, and Web Editions)
- Red Hat Linux, version 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- SuSE Linux, version 8.0
- SuSE Linux Enterprise Server, version 8.0

Installing IBM Director Console on Windows

This section describes how to install IBM Director Console. You can install IBM Director Console on any system from which you want to remotely access IBM Director Server.

This section provides instructions for installing IBM Director Console using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

Note: Earlier versions of Active PCI Manager are not compatible with IBM Director. Before you install IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.

Installing IBM Director Console using the InstallShield wizard

Complete the following steps to install IBM Director Console on Windows:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. If the installation program starts automatically and the InstallShield wizard starts, go to step 4. Otherwise, click **Start** → **Run**.
3. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

4. Click **Install IBM Director**. The “IBM Director Installation” window opens.
5. Click **IBM Director Console installation**. The “Welcome to the InstallShield Wizard” window opens.
6. Click **Next**. The “License Agreement” window opens.
7. Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.

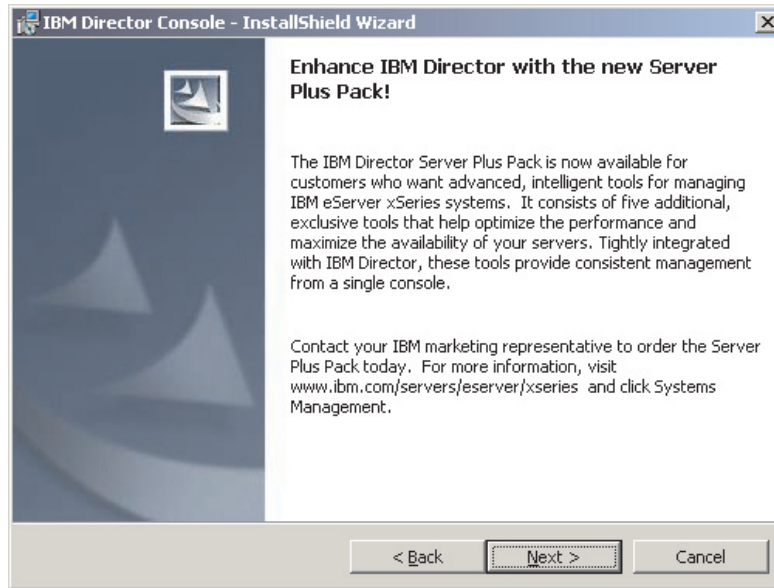


Figure 19. Installing IBM Director Console: “Server Plus Pack” window

8. Click **Next**. The “Feature and installation directory selection” window opens.

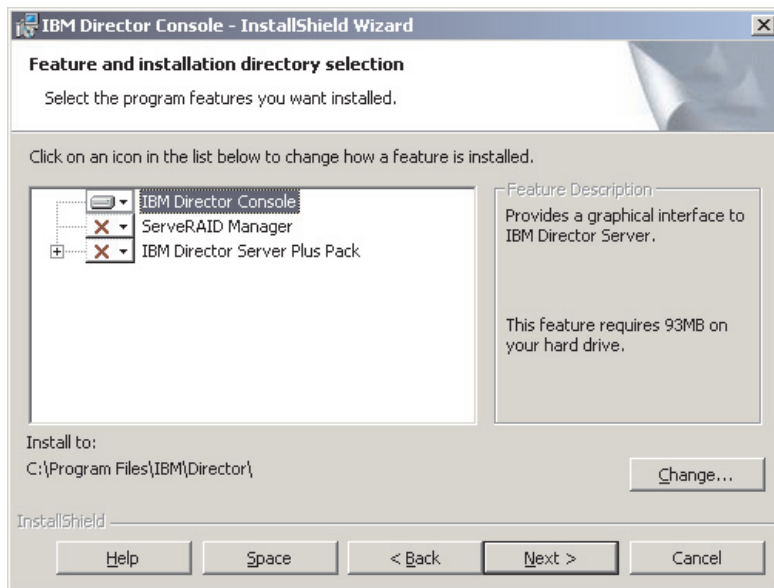





Figure 20. Installing IBM Director Console: “Feature and destination directory selection” window

IBM Director Console is selected automatically for installation; a hard disk drive icon  is displayed to its left.  is displayed to the left of the optional feature: ServeRAID Manager.

9. To select ServeRAID Manager, a feature that manages and monitors IBM ServeRAID adapters, click  to the left of the feature name. A menu opens.

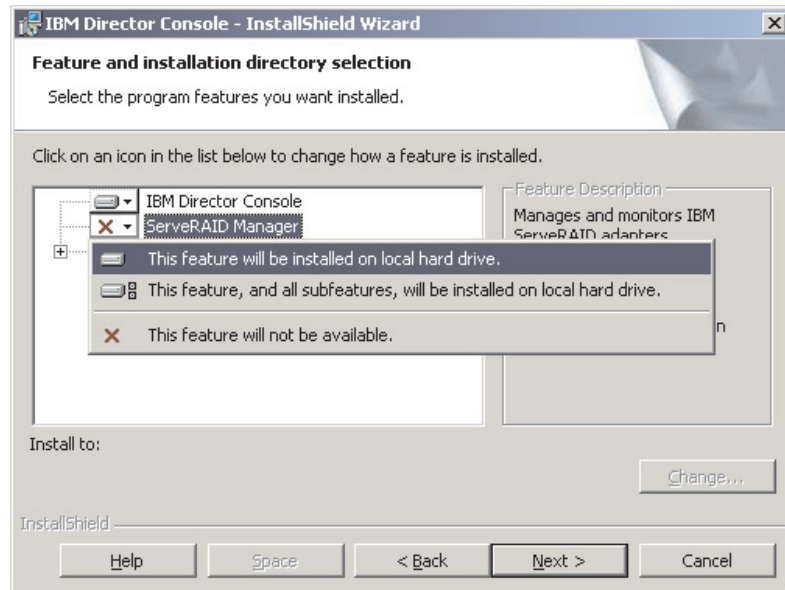


Figure 21. Installing IBM Director Console: Installing ServeRAID Manager

Click **This feature will be installed on local hard drive.**

10. Select the Server Plus Pack extensions that you want to install:

Capacity Manager

Tracks system resource utilization, identifies bottlenecks, and provides performance information.

Rack Manager

Manages IBM servers, storage devices, and other components located in an IBM enclosure.

Active PCI Manager

Manages PCI and PCI-X adapters in managed systems.

Software Rejuvenation

Schedules restarts of managed systems.

System Availability

Determines availability of managed systems and provides statistical data.

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all its subfeatures, will be installed on local hard drive.** Otherwise, select the Server Plus Pack extensions individually.

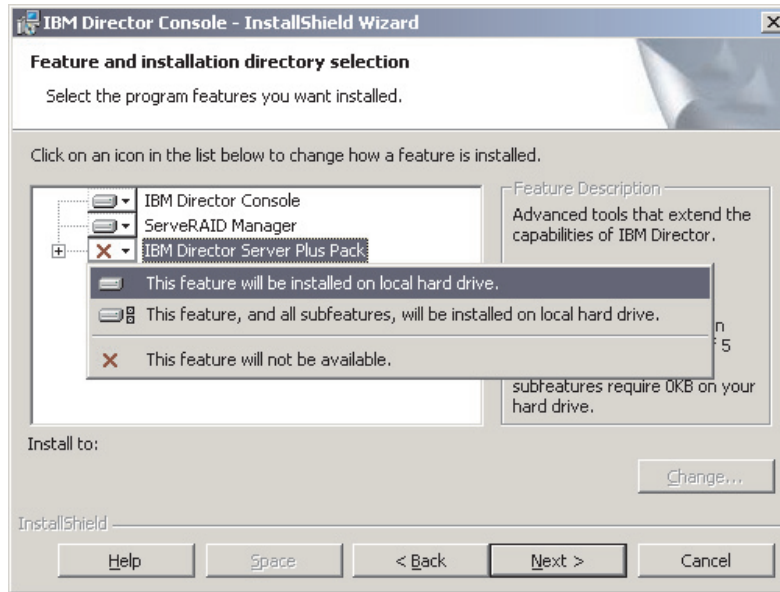


Figure 22. Installing IBM Director Console: Installing the Server Plus Pack

Notes:

- a. Rack Manager will not function until the Rack Manager component, located on the *IBM Director Server Plus Pack* CD, is installed on the management server.
 - b. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.
11. Click **Next**. The “Ready to Install the Program” window opens.
 12. Click **Install**. The “Installing IBM Director Management Console” window opens. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
 13. Click **Finish**.
 14. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

Performing an unattended installation of IBM Director Console

You can perform an unattended installation of IBM Director Console using a response file, which provides answers to the questions posed by the InstallShield wizard. You can use this method to create a standard installation file that can be used on many systems.

Complete the following steps to install IBM Director Console:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. Copy the `dircon.rsp` file to a local directory. This file is located in the `director\console\windows\i386` directory on the *IBM Director 4.11* CD.
3. From Windows Explorer, right-click the copy of the `dircon.rsp` file and then click **Properties**. The “`dircon.rsp` Properties” window opens. Clear the **Read-Only** check box and click **OK**.
4. Open the copy of the `dircon.rsp` file in an ASCII text editor.
5. Modify and save the `dircon.rsp` file. This file follows the Windows INI file format and is fully commented.

6. Change to the directory that contains the IBM Director Console installation file (`ibmsetup.exe`). This file is located in the `director\console\windows\i386` directory on the *IBM Director 4.11* CD.
7. From the command prompt, type the following command and press Enter:


```
ibmsetup.exe installationtype rsp="responsefile.rsp"
```

where:

 - *installationtype* is one of the following commands:
 - UNATTENDED shows the progress of the installation but does not require any user input.
 - SILENT suppresses all output to the screen during installation.
 - *responsefile.rsp* is the path and name of the response file that you created in step 5 on page 58.
8. When the installation is completed, remove the *IBM Director 4.11* CD from the CD-ROM drive.

Installing IBM Director Console on Linux

Complete the following steps to install IBM Director Console on Linux:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/console/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. If you want to customize the installation, go to step 6. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 10 on page 60.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the `dirinstall` script. This file is fully commented.

You can specify the location of the RPM files, select the IBM Director extensions and features that you want to install, and select log file options.

8. Save the modified installation script.

9. To install IBM Director, type the following command and press Enter:
`/directory/dirinstall`

where *directory* is the local directory to which you copied the installation script.

10. To unmount the CD-ROM drive, complete the following steps:
 - a. Type `cd /` and press Enter.
 - b. Type the following command and press Enter:
`umount /mnt/cdrom`

where *mnt/cdrom* is the mount point of the CD-ROM drive.

11. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

Chapter 6. Installing IBM Director Agent

This chapter contains instructions for installing IBM Director Agent. If you are upgrading from IBM Director 3.x or later, go to Chapter 12, “Upgrading IBM Director Agent”, on page 151.

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

- 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 Professional, Server, Advanced Server, and Datacenter Server (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)
- Windows Server 2003 (Standard, Enterprise, Datacenter, and Web Editions)
- Red Hat Linux, versions 7.1, 7.2, and 7.3
- Red Hat Enterprise Linux AS, version 2.1 (formerly Red Hat Linux Advanced Server, version 2.1)
- Red Hat Enterprise Linux ES and WS, version 2.1
- SuSE Linux, versions 7.2, 7.3, and 8.0
- SuSE Linux Enterprise Server, version 8.0
- Novell NetWare, version 6.0
- Caldera Open UNIX, version 8.0
- SCO UnixWare, version 7.1.3
- VMware ESX Server, versions 1.5.2 and 2.0

Installing IBM Director Agent on Windows

This section provides information about installation prerequisites and instructions for installing IBM Director Agent using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

Preparing to install IBM Director Agent

Before you install IBM Director Agent, make sure that you have uninstalled any incompatible files and installed any necessary prerequisites and device drivers. Consider the following information:

1. Earlier versions of Active PCI Manager are not compatible with IBM Director. Make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
2. (Windows NT 4.0 only) Make sure that you have installed the following prerequisites:
 - Microsoft Run-Time Components for Visual C++ Applications: You can download `vcredist.exe`, a self-extracting, executable file from <http://www.microsoft.com>. For more information, see Microsoft Knowledge Base Article 259403.
 - Windows Management Instrumentation (WMI) CORE 1.5: You can download `wmint4.exe`, a self-extracting, executable file from <http://www.microsoft.com>.

3. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

Installing IBM Director Agent using the InstallShield wizard

Note: (Windows XP only) During the installation, message windows might open behind the installation window. These message windows stop the installation process. To check for hidden message windows, press Alt+Tab to cycle through the active windows.

Complete the following steps to install IBM Director Agent on Windows:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. If the installation program starts automatically and the InstallShield wizard starts, go to step 4. Otherwise, click **Start** → **Run**.
3. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

4. Click **Install IBM Director**. The “IBM Director Installation” window opens.
5. Click **IBM Director Agent installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
6. Click **Next**. The “License Agreement” window opens.
7. Click **I accept the terms in the license agreement** and click **Next**. The “Feature and installation directory selection” window opens.

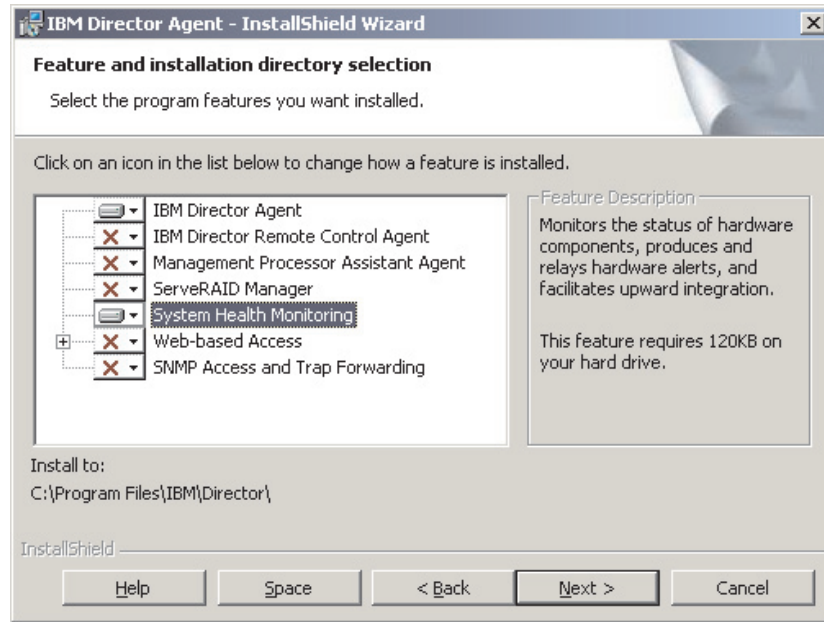




Figure 23. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

8. Select the optional features that you want to install. IBM Director Agent is selected automatically for installation; a hard disk drive icon  is displayed to the left of the component.  is displayed to the left of the optional features not selected by default.

You can install the following optional features:

IBM Director Remote Control Agent

Enables a system administrator to perform remote desktop functions on a managed system.

Management Processor Assistant Agent

Enables communication with service processors in IBM xSeries and Netfinity servers.

ServeRAID Manager

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities.

System Health Monitoring


Monitors the status of hardware components, produces and relays hardware alerts, and facilitates upward integration.

Web-based Access

Enables system administrator to access managed-system data through a Web browser or the Microsoft Management Console (MMC).

SNMP Access and Trap Forwarding

Enables access to managed-system data and alerts through SNMP.

To select a feature, click  to the left of the feature name. A menu opens.

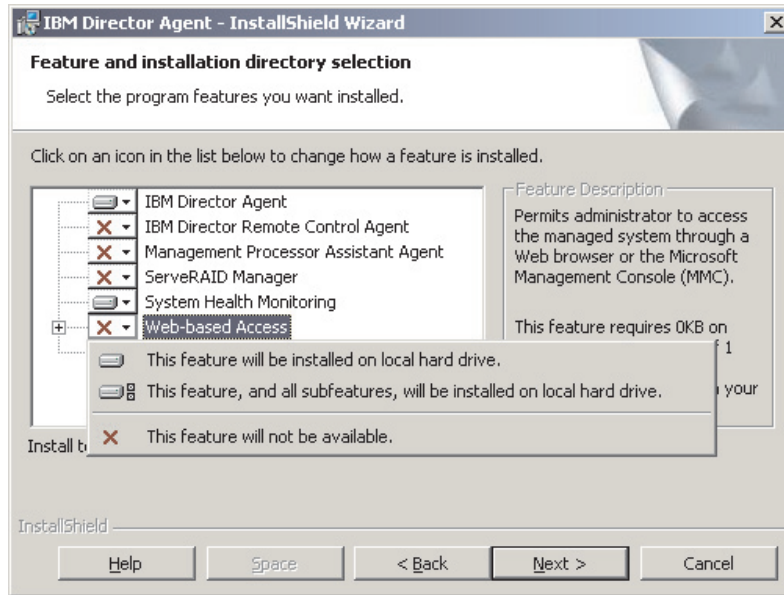


Figure 24. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

To install the feature, click **This feature will be installed on local hard drive** or **This feature, and all its subfeatures, will be installed on local hard drive**.

9. Click **Next**. The “Security settings” window opens.

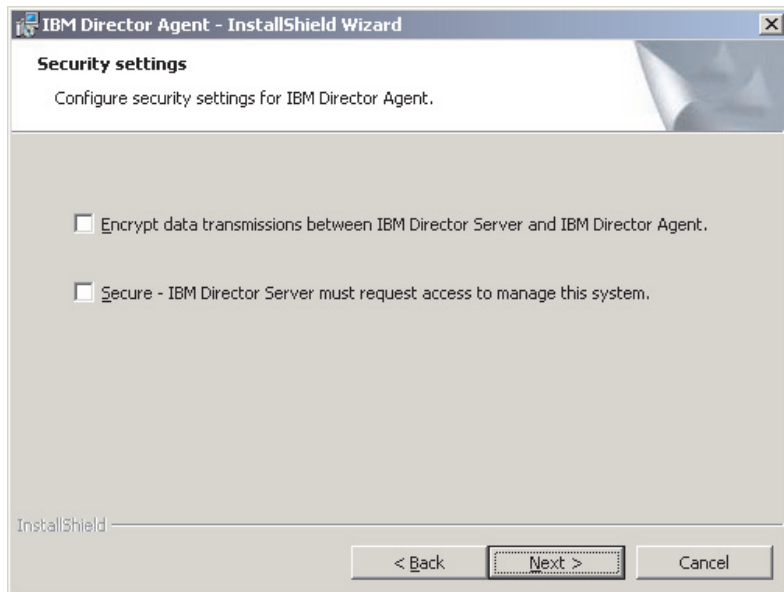


Figure 25. Installing IBM Director Agent on Windows: “Security settings” window

10. If you do not want to encrypt transmissions between IBM Director Server and IBM Director Agent, go to step 11. Otherwise, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box.

Note: If encryption is enabled, the following conditions apply:

- The managed system is automatically secured, and the **Secure – IBM Director Server must request access to manage this system** check box is unavailable.
 - Only management servers with encryption enabled are able to communicate with the managed system.
11. To set IBM Director Agent to the secured state, select the **Secure – IBM Director Server must request access to manage this system** check box. This ensures that IBM Director Server cannot manage this system until it is granted access.
 12. Click **Next**. The “Software Distribution settings” window opens.

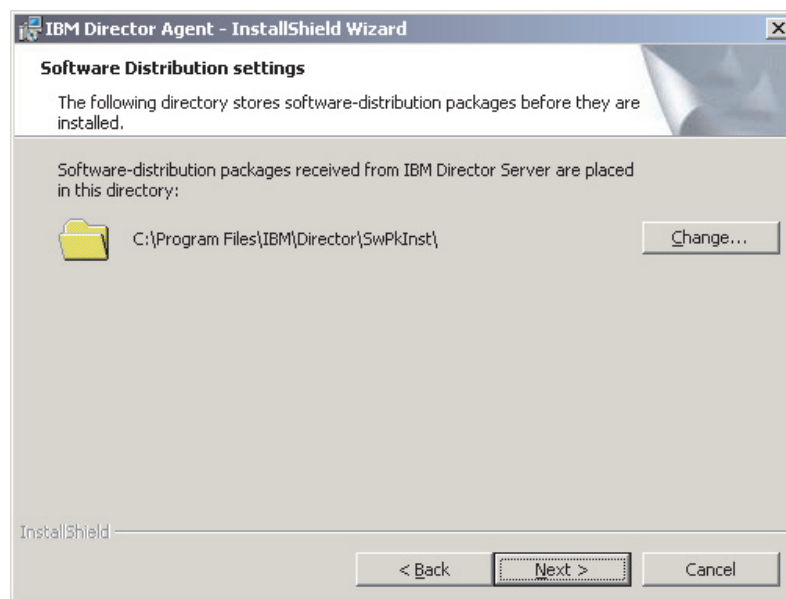


Figure 26. Installing IBM Director Agent on Windows: “Software Distribution settings” window

To select an alternative location for where software-distribution packages are stored before being applied to IBM Director Agent, click **Change** and select another directory.

13. Click **Next**. If you did not select to install the Web-based Access feature, go to step 15 on page 66. Otherwise, the “Web-based Access information” window opens.

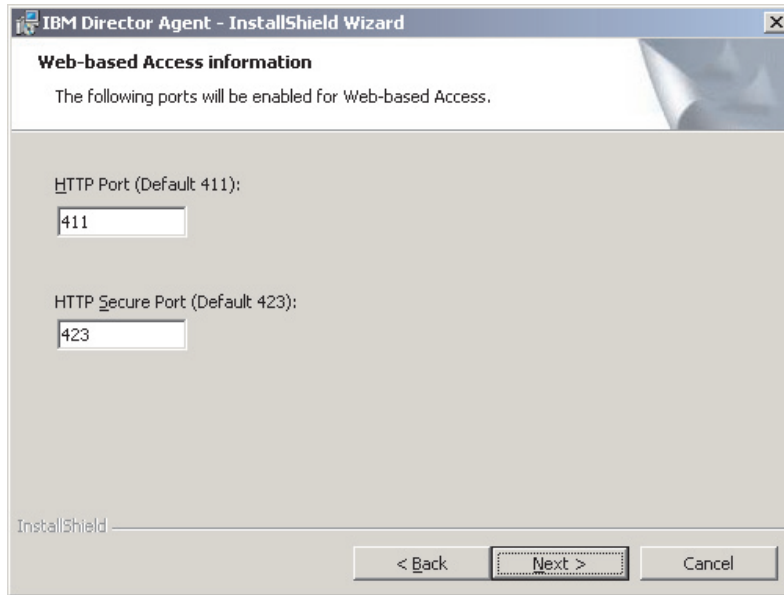


Figure 27. Installing IBM Director Agent on Windows: “Web-based Access information” window

14. Change the default HTTP port numbers (if necessary), and click **Next**. The “Ready to Install the Program” window opens.
15. Click **Install**. The “Installing IBM Director Agent” window opens. The status bar indicates the progress of the installation. When the installation is completed, the “Network driver configuration” window opens.

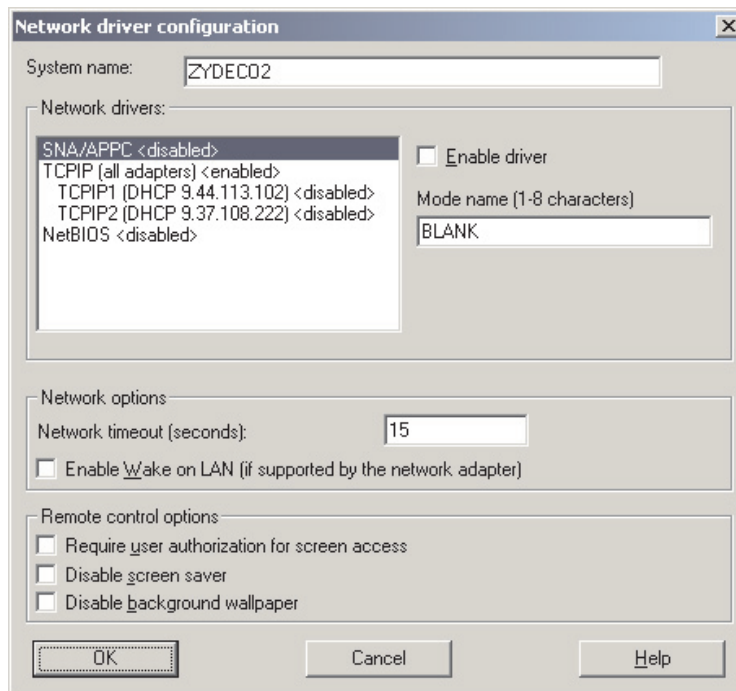


Figure 28. Installing IBM Director Agent on Windows: “Network driver configuration” window

16. In the **System Name** field, type the name that you want displayed in IBM Director Console. By default, this is the NetBIOS name of the managed system.
17. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
 - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

Note: If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive data packets addressed to the individual adapter *only*.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
- c. Click **Enable Wake on LAN** if the network adapter supports the Wake on LAN feature.

Note: To determine whether your server supports the Wake on LAN feature, see your server documentation.

18. If you selected to install the IBM Director Remote Control Agent, the following options are available:

Require User Authorization for System Access

Select this check box to request authorization from the local user before accessing a managed system remotely.

Disable Screen Saver

Select this check box to disable the screen saver on the managed system being controlled remotely.

Disable Background Wallpaper

Select this check box to disable desktop wallpaper on the managed system being controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

19. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the "InstallShield Wizard Completed" window opens.
20. Click **Finish**. The "IBM Director Agent Installer Information" window opens.
21. Remove the *IBM Director 4.11* CD from the CD-ROM drive.
22. Click **Yes** to restart your system.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, "Installing IBM Director extensions", on page 121.

Performing an unattended installation of IBM Director Agent

Note: You cannot perform an unattended installation of IBM Director Agent on Windows XP.

You can perform an unattended installation of IBM Director Agent using a response file, which provides answers to the questions posed by the InstallShield wizard. You can use this method to create a standard installation file that can be used on many systems.

Complete the following steps to install IBM Director Agent on Windows:

1. If you are installing IBM Director Agent on an IBM server that contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

2. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
3. Copy the `diragent.rsp` file to a local directory. This file is located in the `director\agent\windows\i386` directory on the *IBM Director 4.11* CD.
4. From Windows Explorer, right-click the copy of the `diragent.rsp` file and then click **Properties**. The “`diragent.rsp` Properties” window opens. Clear the **Read-Only** check box and click **OK**.
5. Open the copy of the `diragent.rsp` file in an ASCII text editor.
6. Modify and save the `diragent.rsp` file. This file follows the Windows INI file format and is fully commented.
7. Change to the directory that contains the IBM Director Agent installation file (`ibmsetup.exe`). This file is located in the `director\agent\windows\i386` directory on the *IBM Director 4.11* CD.
8. From the command prompt, type the following command and press Enter:
`ibmsetup.exe installationtype rsp="responsefile.rsp" waitforme`

where:

- `installationtype` is one of the following commands:
 - `UNATTENDED` shows the progress of the installation but does not require any user input.
 - `SILENT` suppresses all output to the screen during installation.
 - `responsefile.rsp` is the path and name of the response file that you created in step 6.
 - `waitforme` is an optional parameter that ensures that `ibmsetup.exe` process will not end until the installation of IBM Director Agent is completed.
9. If you issued the `UNATTENDED` command in step 8, restart the operating system when prompted to do so.
 10. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions”, on page 121.

Installing IBM Director Agent on Red Hat Linux, SuSE Linux, or VMware ESX

This section provides information about installation prerequisites and instructions for installing IBM Director Agent.

Preparing to install IBM Director Agent

Before you install IBM Director Agent, make sure you have installed any necessary prerequisites and device drivers. Consider the following information:

1. (IBM servers only) Determine the type of service processor installed in the server. If the server does not contain a Remote Supervisor Adapter or a Remote Supervisor Adapter II, you must install the IBM SMBus device driver for Linux before you install IBM Director Agent. The IBM SMBus device driver ensures that the Asset ID™ and Management Processor Assistant tasks function properly. See “Downloading, building, and installing the IBM SMBus device driver” for more information.
2. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

3. Verify that the operating-system password-encryption method is set to message digest 5 (MD5) or DES.
4. (SuSE Linux 7.x only) Verify that the following libraries and packages are upgraded to level 2.2.4-64 or later:
 - glibc libraries
 - glibc-devel package (if installed)
 - glibc-profile package (if installed)
5. If you want to use the Remote Session task on the managed system, verify that the package containing telnetd is installed and configured. This is usually in the `telnet_server_version.i386.RPM` package, where *version* is the code level of your Linux distribution.

Downloading, building, and installing the IBM SMBus device driver

You must download the IBM SMBus device driver source files:

- `ibmsmb-src-redhat-4.10-1.i386.rpm`
- `ibmsmb-src-suse-4.10-1.i386.rpm`

You can download the files from the IBM Systems Management Software:

Download/Electronic Support page at

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

Before installing the IBM SMBus driver, you must install the source RPM file, which builds the binary RPM file. You must build the binary RPM file on a system with the same kernel version and hardware configuration as the target system. Be sure that hardware configuration is similar in regard to the number of processors.

Complete the following steps to build and install the IBM SMBus device driver:

1. Configure a system with the appropriate operating system and hardware configuration. Verify that the Linux kernel source is installed and properly configured.
2. To install the source RPM file, from a command prompt, type one of the following commands and press Enter:

Red Hat Linux and VMware ESX Server	<code>rpm -ivh ibmsmb-src-redhat-4.10-1.i386.rpm</code>
SuSE Linux	<code>rpm -ivh ibmsmb-src-suse-4.10-1.i386.rpm</code>

This creates a binary RPM file in the `/usr/local/ibmsmb` directory.

3. Change to the `/usr/local/ibmsmb` directory.
4. To install the IBM SMBus device driver, type the following command and press Enter:

```
rpm -ivh ibmsmb-4.10-1.i386.rpm
```

Issuing this command accomplishes the following tasks:

- Uncompresses and untars the archive into the `/usr/local/ibmsmb` directory
- Copies the device driver, shared library, and all configuration files to their appropriate locations
- Loads the device driver

Installing IBM Director Agent

Complete the following steps to install IBM Director Agent on Linux:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where `mnt/cdrom` is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where `dev/cdrom` is the specific device file for the CD-ROM block device and `mnt/cdrom` is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/agent/linux/i386/
```

where `mnt/cdrom` is the mount point of the CD-ROM drive.

5. If you want to customize the installation, go to step 6 on page 71. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 10 on page 71.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the *dirinstall* script. This file is fully commented.

You can specify the location of the RPM files, select the IBM Director Agent features you want to install, and select log file options.

8. Save the modified installation script.
9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```

11. To start IBM Director Agent, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

12. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.
- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

13. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable the Wake on LAN feature. See “Enabling Wake on LAN” on page 178.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions”, on page 121.

Installing IBM Director Agent on NetWare

Notes:

1. If both the following conditions are true, do not install the MPA Agent:
 - The managed system is one of the following servers: xSeries 232, 235, 255, 335, 342, or 345.
 - You have not installed an optional Remote Supervisor Adapter.

The MPA Agent will not work with servers managed by an integrated system management processor and running NetWare or Caldera Open UNIX.

2. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

3. To install IBM Director Agent, you must log on to the NetWare server from a Windows workstation running the NetWare Client for Windows. The SYS volume must be mapped as a drive to the system running Windows. Also, you must have administrator or supervisor access on the NetWare server.

Complete the following steps to install IBM Director Agent on NetWare:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive of the system running Windows. If the autorun window opens, close it.
2. Start Windows Explorer and open the `\director\agent\netware` directory.
3. Double-click **setup.exe**. The InstallShield wizard starts.
4. Click **Next**. The “Installing IBM Director Agent” window opens.
5. Click **Next** to accept the license agreement. The “Choose destination location” window opens.

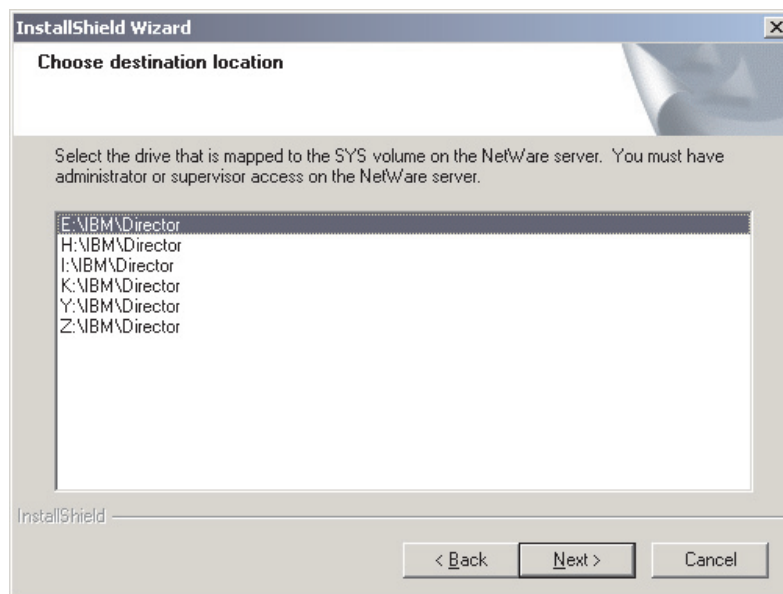


Figure 29. Installing IBM Director Agent on NetWare: “Choose destination location” window

6. Click the drive that is mapped to the SYS volume on the server running NetWare; then, click **Next**. The “Select Components” window opens.

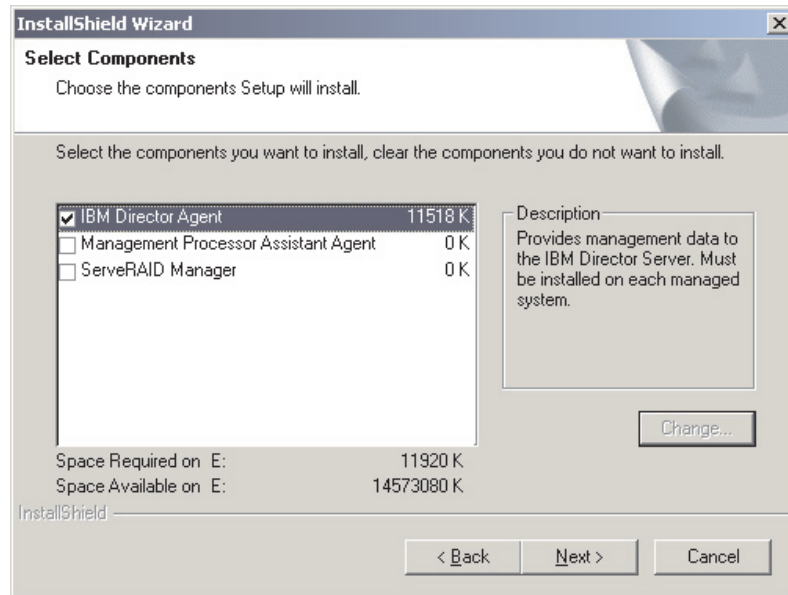


Figure 30. Installing IBM Director Agent on NetWare: “Select Components” window

7. Select the check boxes for the components you want to install; then, click **Next**. The “Setup Status window” opens, and IBM Director Agent installation begins. When the installation is completed, the “InstallShield Wizard complete” window opens.

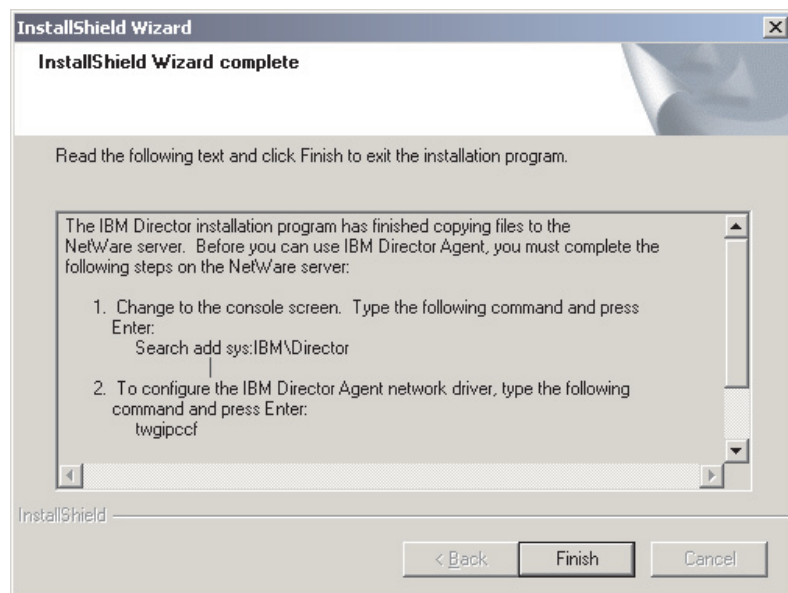


Figure 31. Installing IBM Director Agent on NetWare: “InstallShield Wizard complete” window

8. Click **Finish**.
9. Remove the *IBM Director 4.11* CD from the CD-ROM drive.
10. On the server running NetWare, change to the console screen.
11. From the console, type the following command and press Enter:
Search add sys:IBM\Director

12. To define the protocols to use for communication between IBM Director Server and IBM Director Agent, type the following command and press Enter:

```
twgipccf
```

Note: If you enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive data packets addressed to the individual adapter *only*.

13. To start IBM Director Agent, type the following command and press Enter:

```
load twgipc
```

IBM Director Agent will start automatically whenever the server running NetWare starts.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, "Installing IBM Director extensions", on page 121.

Installing IBM Director Agent on Caldera Open UNIX

Notes:

1. (IBM servers only) If both the following conditions are true, do not install the MPA Agent:
 - The managed system is one of the following servers: xSeries 232, 235, 255, 335, 342, or 345.
 - You have not installed an optional Remote Supervisor Adapter.

The MPA Agent will not work with servers managed by an integrated system management processor and running NetWare or Caldera Open UNIX.

2. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

3. Before installing IBM Director Agent, verify that the operating-system password encryption method is set to MD5 or DES.

Complete the following steps to install IBM Director Agent on Caldera Open UNIX:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. To mount the CD-ROM drive, type the following command and press Enter:

```
mount -F cdfs -o ro,nmconv=c,fperm=+x /dev/cdromdevicefile /mountpoint
```

where *cdromdevicefile* is the specific device file for the CD-ROM block device and *mountpoint* is the mount point of the CD-ROM drive.

3. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mountpoint/director/agent/openunix/i386
```

where *mountpoint* is the mount point of CD-ROM drive.

4. Copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /destinationdirectory/dirinstall
```

where *destinationdirectory* is the local directory.

5. Open an ASCII text editor and modify the “User configuration” section of the installation script. This file is fully commented. You can specify the location of the PKG files, select the IBM Director Agent features you want to install, and select log file options.

6. Save the modified installation script.

7. To install IBM Director Agent, type the following command and press Enter:

```
/destinationdirectory/dirinstall
```

where *destinationdirectory* is the local directory to which you copied the installation script.

8. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```

9. To start IBM Director Agent, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

10. To unmount the CD-ROM drive, type the following command and press Enter:

```
umount /mountpoint
```

where *mountpoint* is the mount point of the CD-ROM drive.

11. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable the Wake on LAN feature. See “Enabling Wake on LAN” on page 178.

Part 3. Configuring IBM Director

Chapter 7. Configuring an IBM BladeCenter chassis

This chapter contains information about discovering and configuring an IBM BladeCenter chassis. It also includes information about creating a chassis detect-and-deploy profile.

You must use the BladeCenter Deployment wizard to configure the BladeCenter chassis. If you have Remote Deployment Manager (RDM) installed on your management server, you also can use the wizard to install the operating systems on the blade servers.

Attention: After configuring the BladeCenter chassis, avoid changing the database application used with IBM Director Server. Doing so will cause inventory errors.

Starting IBM Director Console

After installing IBM Director Server, complete the following steps to start IBM Director Console:

1. If you are starting IBM Director Console from the management server, verify that the IBM Director Server is running.

For Windows	Make sure that the task bar in the lower-right corner of the screen contains a bright green circle.
--------------------	---

For Linux	From a command prompt, type the following command and press Enter:
------------------	--

```
/opt/IBM/director/bin/twgstat -r
```

The current status of IBM Director Server is displayed.

2. Start IBM Director Console.

For Windows	Click Start → Programs → IBM Director Console .
--------------------	--

For Linux	From a command prompt, type the following command and press Enter:
------------------	--

```
twgcon
```

The “IBM Director Login” window opens.



Figure 32. "IBM Director Login" window

3. In the **IBM Director Server** field, type the name of the management server.
4. In the **User ID** field, type *DirectorUserID* where *DirectorUserID* is a valid IBM Director user ID.
5. In the **Password** field, type the password that corresponds to the user ID.
6. Click **OK**. IBM Director Console starts.

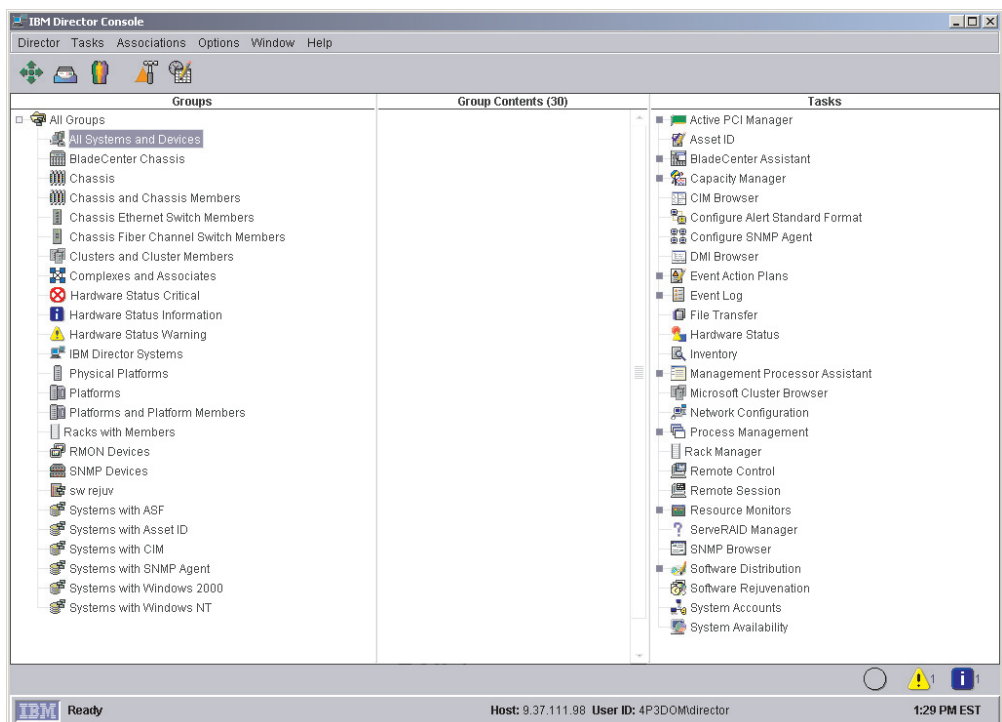


Figure 33. IBM Director Console

Discovering a BladeCenter chassis

Before you can run the BladeCenter Deployment wizard and configure the BladeCenter chassis, IBM Director must discover the BladeCenter chassis and create a BladeCenter chassis managed object.

IBM Director discovers the BladeCenter chassis through the external Ethernet port on the BladeCenter management module. When the BladeCenter management module is first started, the management module attempts to acquire an IP address for the external management port using DHCP. If this attempt fails, the BladeCenter management module assigns a nonroutable IP address (192.168.70.125) to the external management port.

If the management server and the BladeCenter chassis are on the same subnet, IBM Director can discover the BladeCenter chassis automatically. You must either use a DHCP server to assign a temporary IP address to the BladeCenter chassis or manually assign the management module a static IP address on the same subnet as the management server. Go to “Automatically discovering the BladeCenter chassis”.

If the management server and the BladeCenter chassis are not on the same subnet, you must create the BladeCenter chassis managed object manually. Go to “Manually creating a BladeCenter chassis managed object” on page 82.

Note: If you do not use a DHCP server to assign a temporary IP address to the BladeCenter chassis, introduce only *one* BladeCenter chassis onto the network at a time. IBM Director must discover and configure the chassis before another chassis is added to the LAN. Otherwise, an IP address conflict will occur.

Automatically discovering the BladeCenter chassis

IBM Director uses the Service Location Protocol (SLP) to discover the BladeCenter management module and create a BladeCenter chassis managed object.

The management server and the BladeCenter chassis must be connected to the network and on the same subnet. You must assign a valid IP address to the external port of the BladeCenter management module. One of the following conditions must be true:

- The network contains a DHCP server which has assigned a temporary IP address to the management module.
- You have manually changed the default, nonroutable IP address of the management module to a valid IP address.

Complete the following steps to discover the BladeCenter management module and create a BladeCenter chassis managed object:

1. Start IBM Director Console.
2. Click **Tasks** → **Discover Systems** → **BladeCenter Chassis**. The BladeCenter chassis managed object is displayed in the Group Contents pane.

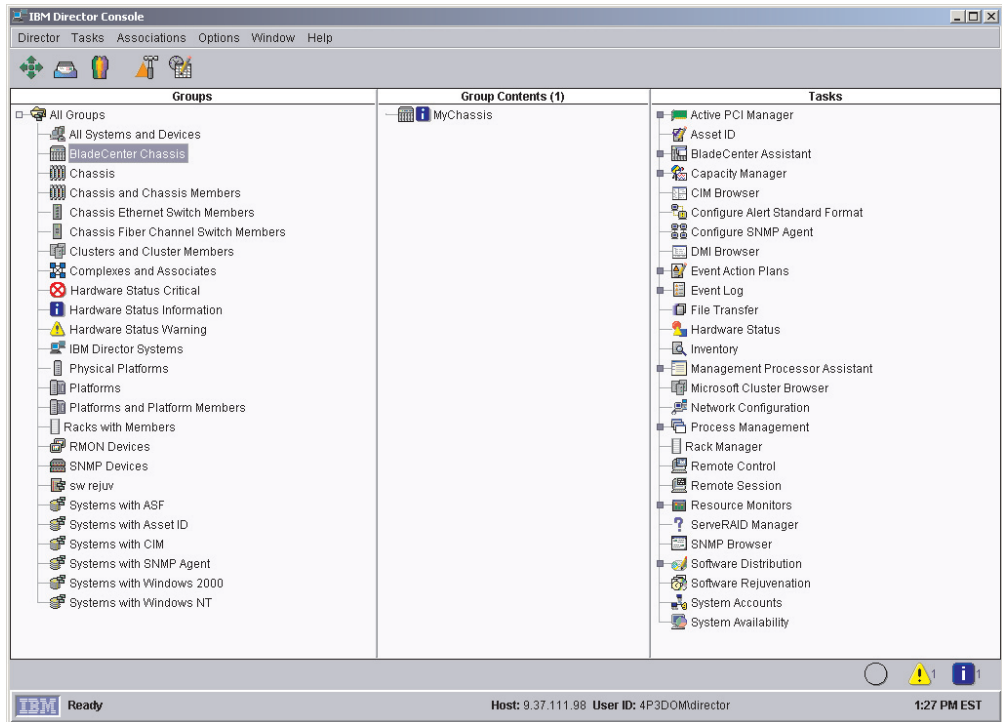


Figure 34. IBM Director Console: Group Contents pane

Manually creating a BladeCenter chassis managed object

If the BladeCenter chassis is on a remote network, IBM Director cannot discover the BladeCenter chassis automatically. Before you can run the BladeCenter Deployment wizard, you must create the BladeCenter chassis managed object manually.

Complete the following steps to create a BladeCenter chassis managed object manually:

1. Manually change the IP address of the management module, if it is set to the default nonroutable IP address. For instructions, see “Manually changing the IP address of the BladeCenter chassis” on page 83.
2. From IBM Director Console, right-click in the Group Contents pane; then click **New → BladeCenter Chassis**. The “Add BladeCenter Chassis” window opens.

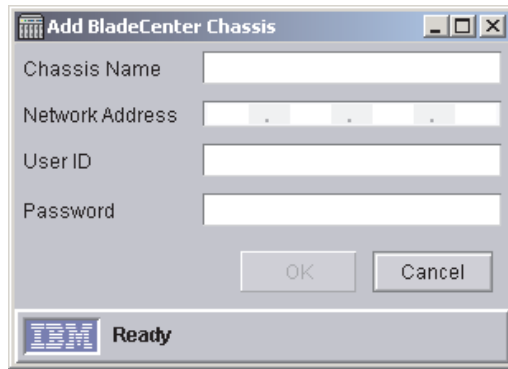


Figure 35. “Add BladeCenter Chassis” window

3. In the **Chassis Name** field, type a name to identify the chassis. This name is displayed in the Groups pane of IBM Director Console.
4. In the **Network Address** field, type the IP address of the external port of the BladeCenter management module.
5. In the **User ID** field, type a valid user ID for the management module.
6. In the **Password** field, type the password that corresponds to the user ID you typed in step 5.
7. Click **OK**. The BladeCenter chassis managed object is created. It is displayed in the Groups pane of IBM Director Console.

Manually changing the IP address of the BladeCenter chassis

Complete the following steps to change the IP address of the BladeCenter chassis manually:

1. Cable a system to the external port of the management module.
2. Change the IP address of the non-chassis system to an address on the 192.168.70.0 subnet.
3. Using the non-chassis system, open a Web browser.
4. In the **Address** or **Location** field, type the following address and press Enter:
http://192.168.70.125

A password window opens.

5. In the applicable fields, type the default user name (USERID) and password (PASSWORD) for the BladeCenter management module. (Use uppercase letters and a zero, not the letter O.)
6. Click **OK**. The “BladeCenter Management Module” window opens.
7. Click **Continue**. The “System Status Summary” window opens.
8. In the left pane, click **Network Interfaces**. The “Management Module Network Interfaces” window opens.

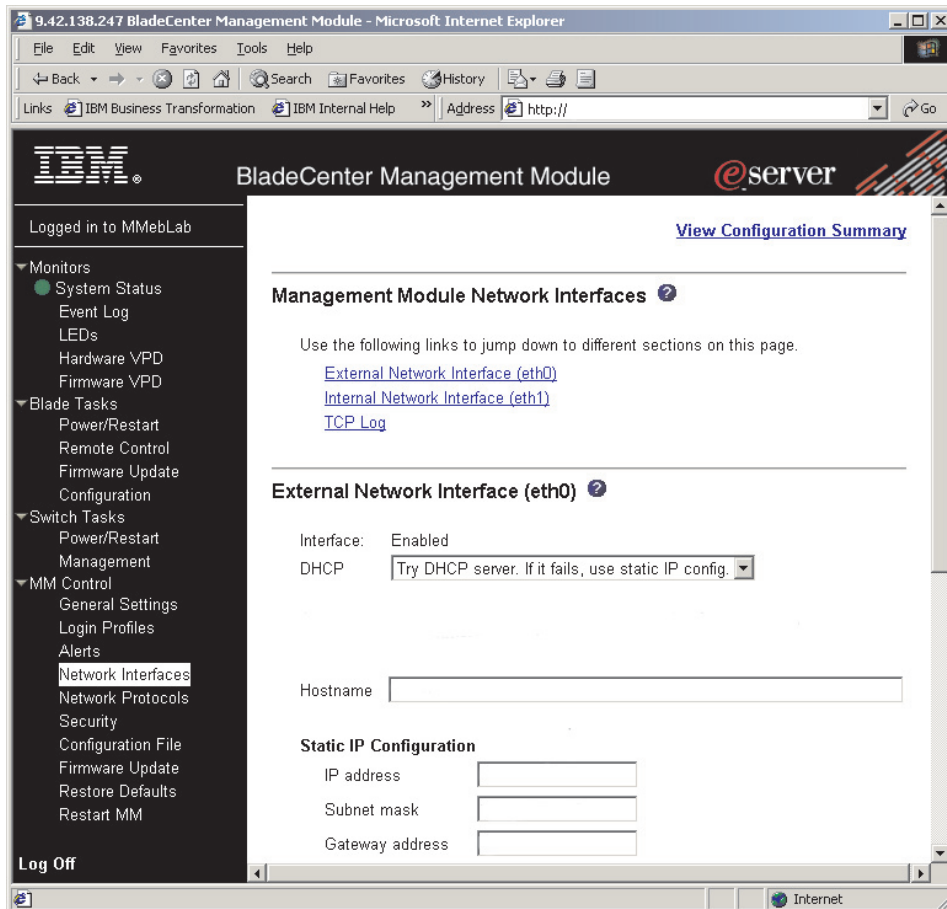


Figure 36. “Management Module Network Interfaces” window

9. In the **DHCP** field, click **Disabled—Use static IP configuration**.
10. In the **IP address** field, type a valid IP address on the same subnet as the management server.
11. In the **Subnet mask** and **Gateway address** fields, type IP addresses for the subnet mask and network gateway.
12. Click **Save**.
13. In the left pane, click **Restart MM**.

Using the BladeCenter Deployment wizard

You can use the BladeCenter Deployment wizard to complete the following tasks:

- Configure a BladeCenter chassis, including setting up security profiles (user name and password), enabling network protocols, and assigning IP addresses for both the BladeCenter management modules and switch modules
- Create reusable profiles that can be used to configure BladeCenter chassis
- Enable a chassis detect-and-deploy profile that automatically configures new BladeCenter chassis when they are added to the IBM Director environment

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 contains the following items:

- IP addresses for the management module and switch modules
- User ID and password for the management module
- Optional prefix used to generate the management module name
- Network protocol configuration information

The profile can include deployment policies, if you have RDM 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 located in the bays that are assigned deployment policies. The blade servers must be powered 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 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 in the following situation:

- The blade server used in conjunction 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.

You can designate one profile as the *chassis detect-and-deploy profile*. IBM Director automatically applies the chassis detect-and-policy when it discovers a new BladeCenter chassis or if you create a new BladeCenter chassis managed object.

Attention: Be careful when deleting and manually recreating chassis managed objects for BladeCenter chassis that are already configured. If you delete and manually recreate a BladeCenter chassis managed object, IBM Director automatically applies the chassis detect-and-deploy profile to that chassis.

Configuring the BladeCenter chassis

Notes:

1. To use the BladeCenter Deployment wizard, IBM Director must have created a managed object for the BladeCenter chassis.
2. 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 configure a BladeCenter chassis:

1. In the IBM Director Console Tasks pane, expand the **BladeCenter Assistant** task.
2. Drag the **Deployment Wizard** task onto the BladeCenter chassis that you want to configure. The BladeCenter Deployment wizard starts and the “Welcome to the BladeCenter Deployment wizard” window opens.

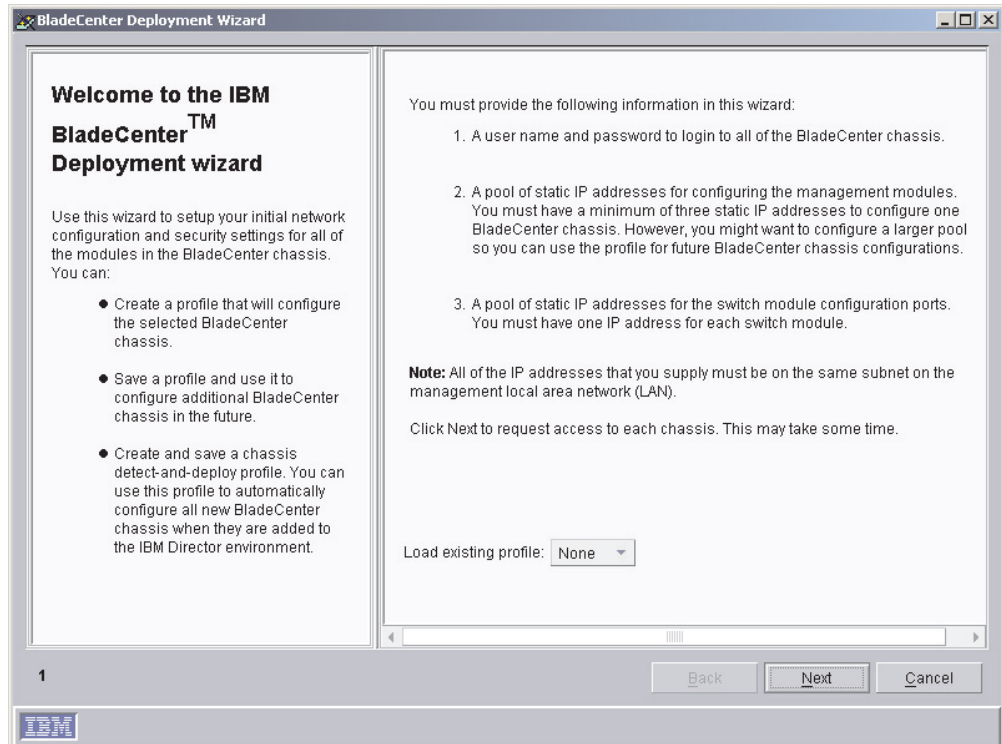


Figure 37. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window

3. Click **Next**. If you are already logged in to the management module, the “Change the user name and password for the management module” window opens. Go to step 5 on page 88. Otherwise, the “Login to the BladeCenter management module” window opens.

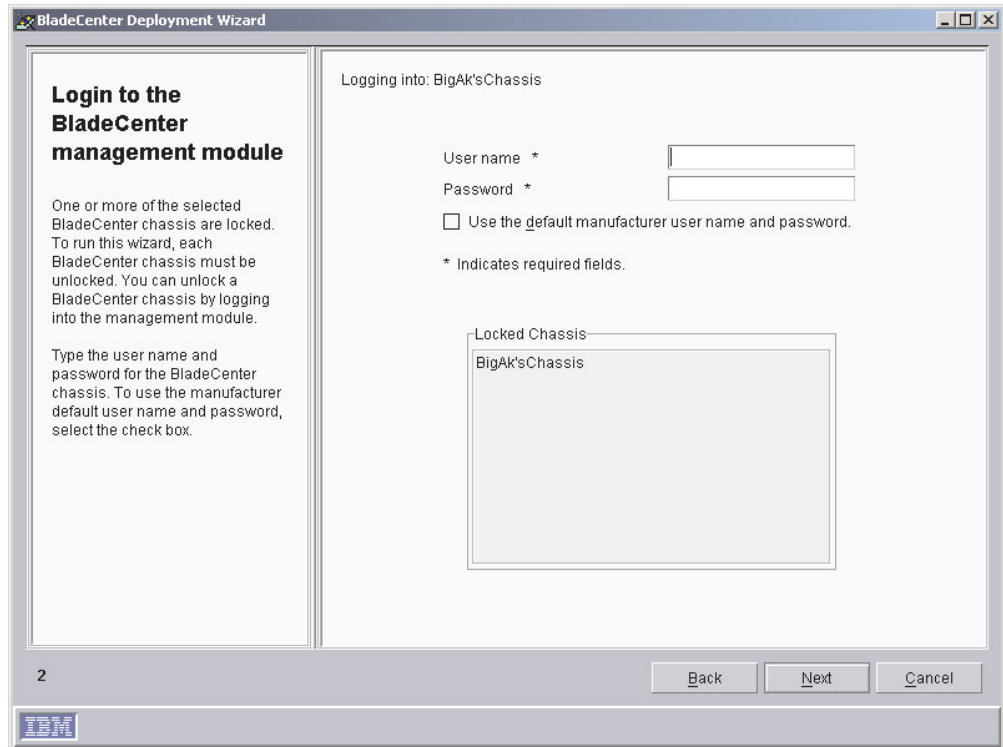


Figure 38. BladeCenter Deployment wizard: "Login to the BladeCenter management module" window

4. In the applicable fields, type the current user name and password; then, click **Next**. The "Change the user name and password for the management module" window opens.

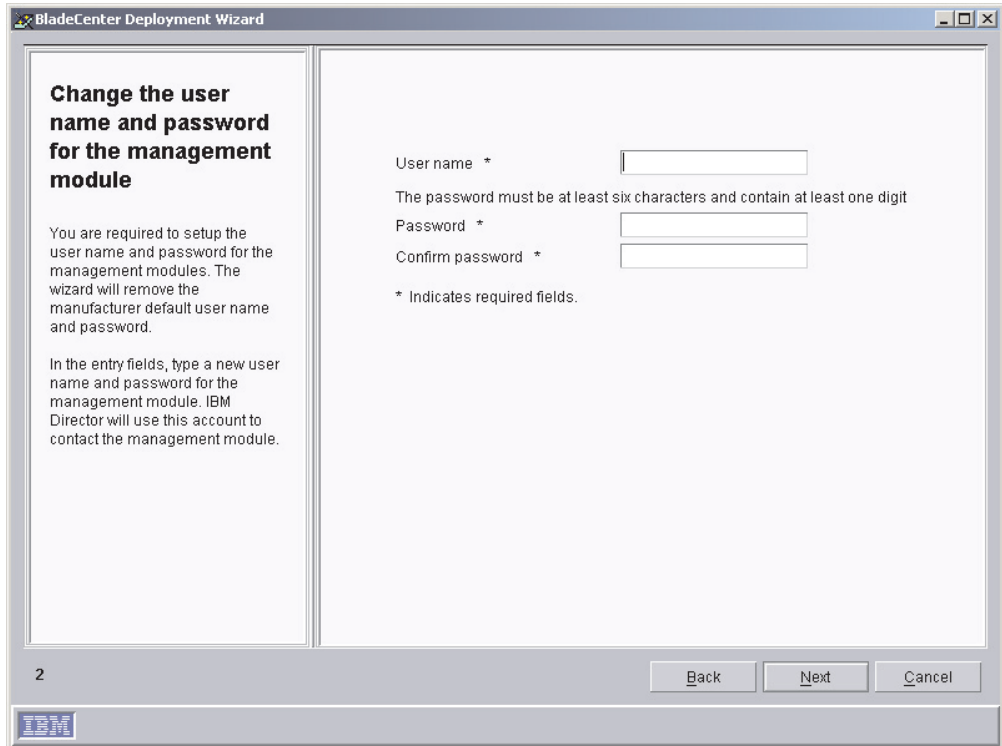


Figure 39. BladeCenter Deployment wizard: “Change the user name and password for the management module” window

5. If you logged in to the management module using the factory-default user name and password, change them now.
 - a. In the **User name** field, type a new user name.
 - b. In the **Password** and **Confirm password** fields, type a new password. It must be at least six characters and contain at least one digit. This user name and password will be used for all BladeCenter chassis selected.

If you logged in to the management module using an existing management module account, type that user name and password in the entry fields.

Note: If you modify an existing user name or password, the wizard saves the changes.

6. Click **Next**. The “Configure the management module properties” window opens.

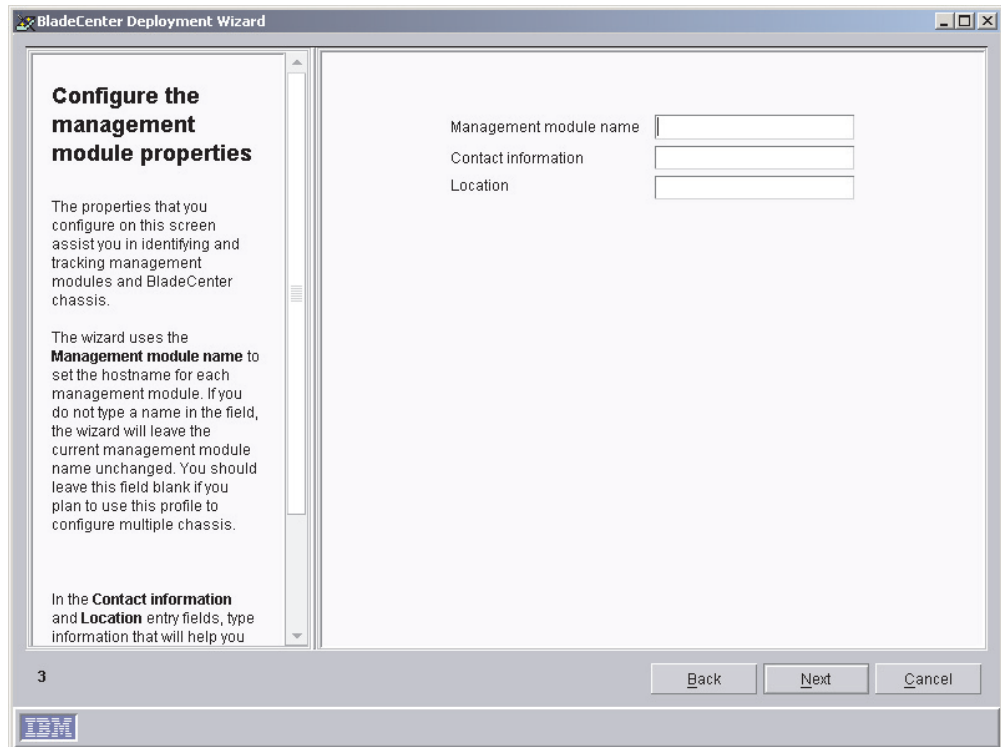


Figure 40. BladeCenter Deployment wizard: “Configure the management module properties” window

7. Configure the management module properties:

- a. In the **Management module name** field, type a name for the BladeCenter management module. If you run the BladeCenter Deployment wizard against multiple BladeCenter chassis, the wizard adds a unique number to this string.

If you leave this entry field blank, the default management module name is MMxxxxxxxxxxx, where xxxxxxxxxxxx is the burned-in media access control (MAC) address of the management module.

- 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.

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

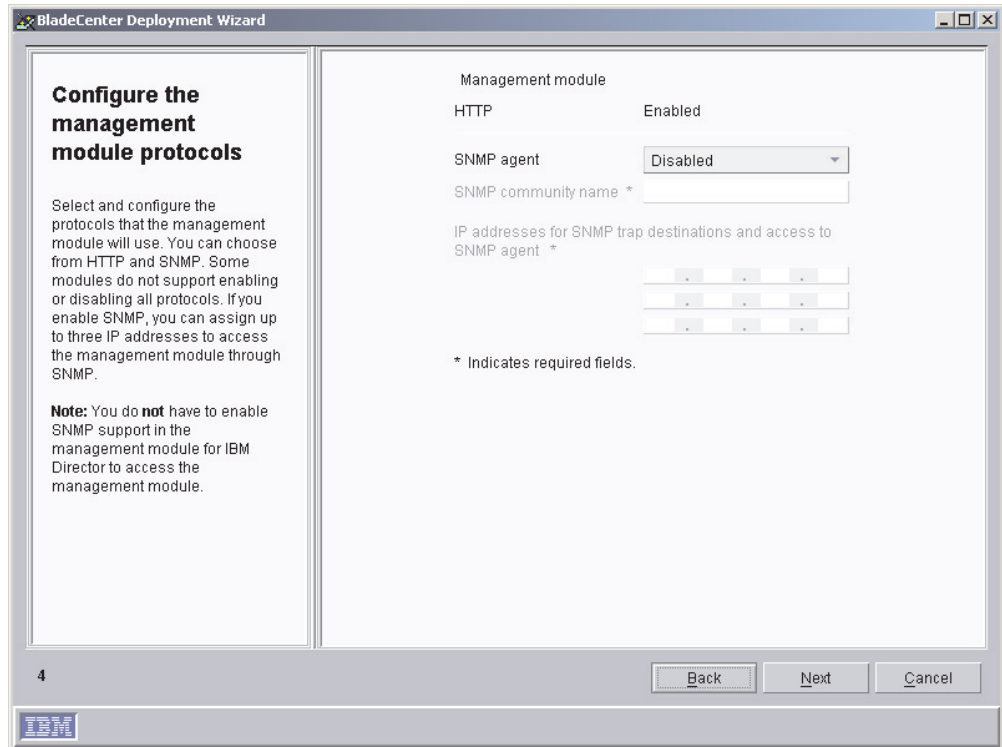


Figure 41. BladeCenter Deployment wizard: “Configure the management module protocols” window

9. Enable the network protocols for the BladeCenter management module.
If you enable SNMP, you must provide an SNMP community name and at least one IP address. You can assign up to three IP addresses to access the management module through SNMP.

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.

10. Click **Next**. The “Configure the IP settings” window opens.

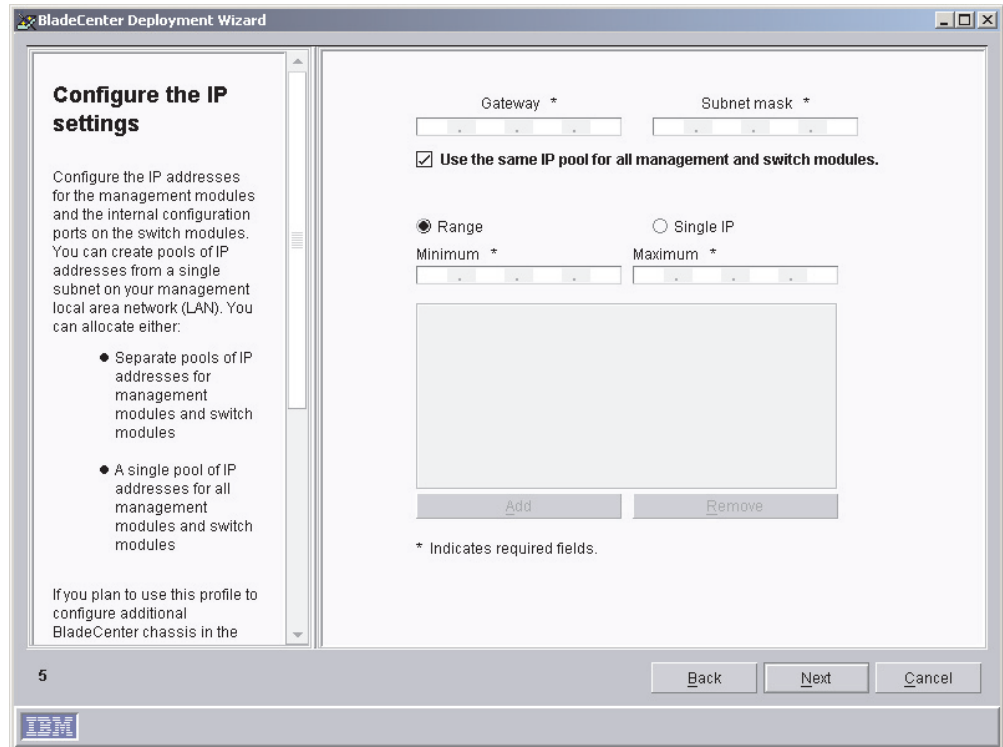


Figure 42. BladeCenter Deployment wizard: “Configure the IP settings” window

11. In the **Gateway** field, type the IP address for the network gateway. In the **Subnet mask** field, type the IP address for the subnet mask.
12. To configure separate pools of IP addresses for the management modules and switch modules, go to step 15. Otherwise, select the **Use the same IP pool for all management and switch modules** check box.
13. Create a pool of IP addresses. You can add IP addresses to the pool individually or by specifying a range.
 - a. To add a single IP address to the pool, click **Single IP**. In the **IP address** field, type the IP address; then, click **Add**.
 - b. 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**.
14. When you have finished creating the pool of IP addresses for the management modules and switch modules, go to step 16.
15. Clear the **Use the same IP pool for all management and switch modules** check box; the **Management Module** and **Network Switch Module** tabs are displayed.
 - a. To create the pool of IP addresses for the management modules, click **Management Module** and follow the instructions outlined in step 13.
 - b. To create the pool of IP addresses for the switch modules, click **Network Switch Module** and follow the instructions outlined in step 13.
16. Click **Next**. The “Change the user name and password for switch modules” window opens.

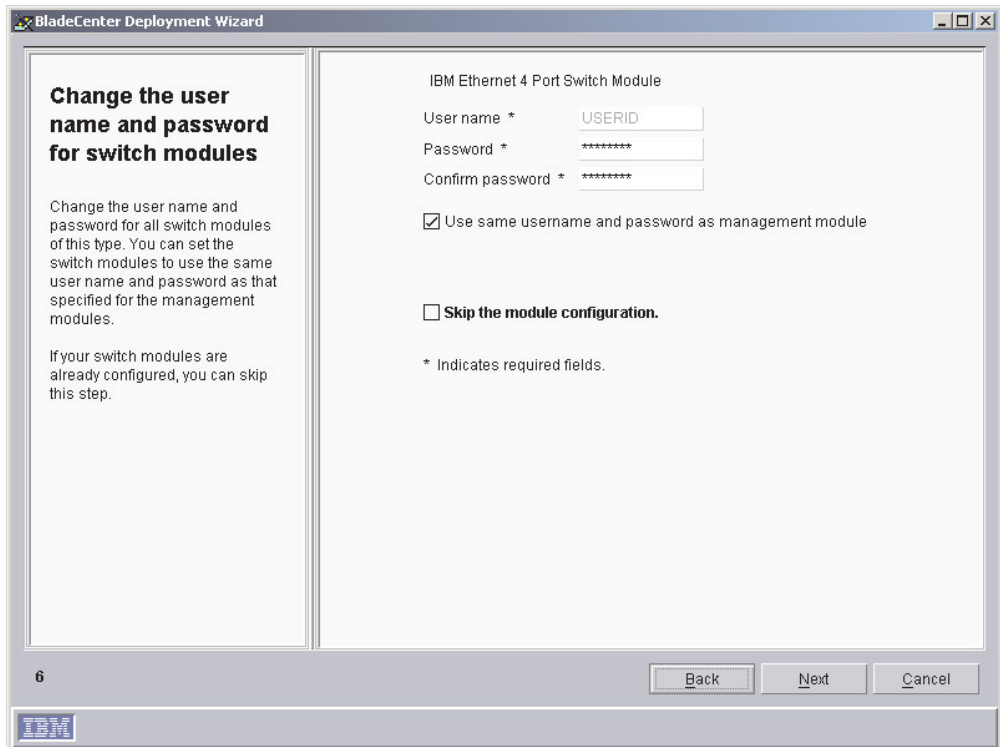


Figure 43. BladeCenter Deployment wizard: “Change the user name and password for switch modules” window

17. If you want to use the same user name and password for both the BladeCenter management modules and switch modules, select the **Use the same username and password as management module** check box. Go to step 18.
If the switch modules are configured already, select the **Skip the module configuration** check box. Go to step 22 on page 93.
If you want to change the user name and password for all BladeCenter switch modules of this specific type, complete the following steps:
 - a. In the **User name** field, type the new user name.
 - b. In the **Password** and **Confirm password** fields, type the new password.
18. Click **Next**. The “Configure the switch module” window opens.

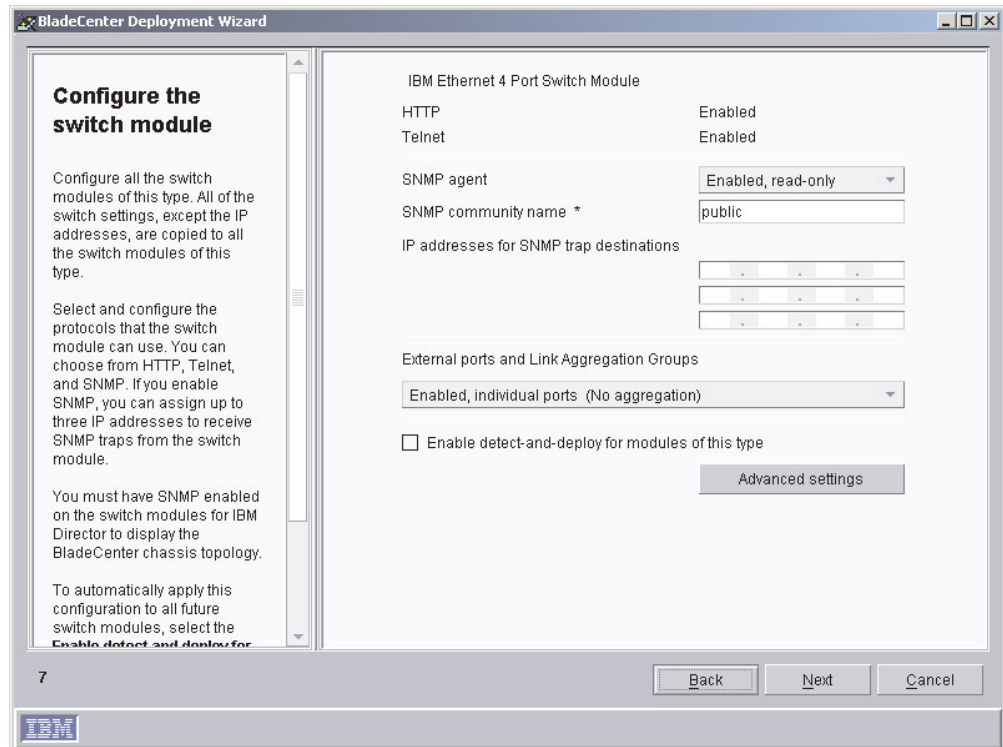


Figure 44. BladeCenter Deployment wizard: “Configure the switch module” window

19. Enable network protocols for all BladeCenter switch modules of this type. If you enable SNMP, you must provide an SNMP community name and at least one IP address. You can assign up to three IP addresses. If you want to use the same pool of IP addresses as that used for the management module, select the **Use the same IP access list as the management module** check box.

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.
20. In the **External ports and link aggregation** list, click the option that indicates how you want to configure the external ports. They can be aggregated into either one-link or two-link aggregation groups (trunks), enabled without aggregation, or disabled.

Note: Before you configure the external ports as link aggregation groups, verify that the LAN switch has a compatible multiport trunk configuration.
21. 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. Click **Advanced settings** to edit additional switch settings.
22. Click **Next**. The “Deploy the operating systems on the blade servers” window opens.

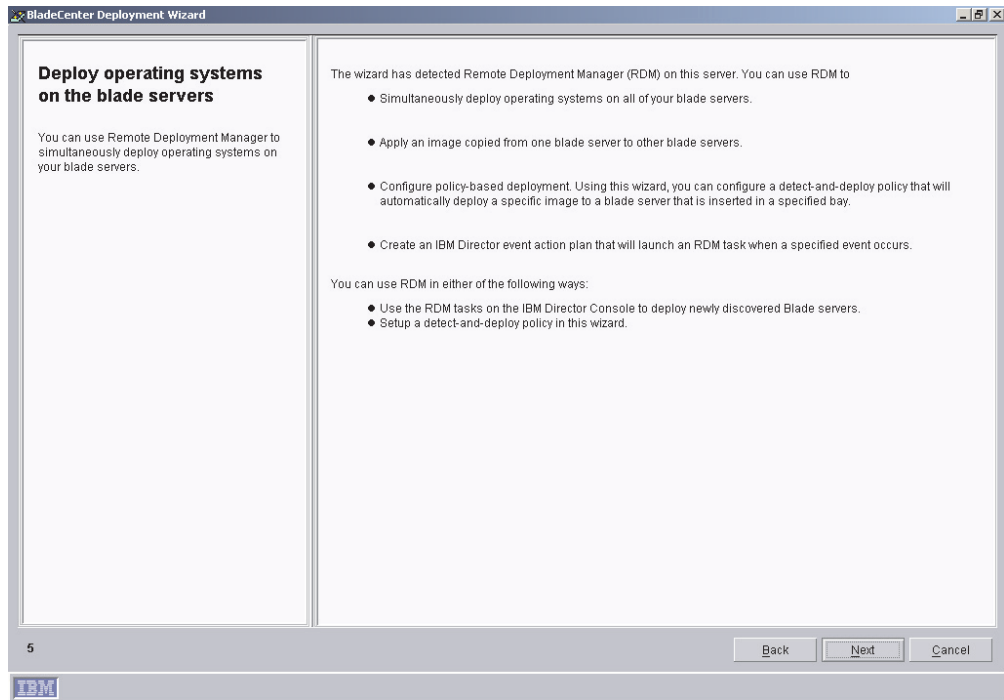


Figure 45. BladeCenter Deployment wizard: “Deploy operating systems on the blade servers” window

23. If you have IBM Remote Deployment Manager installed on your management server, go to step 24. Otherwise, go to step 27 on page 95.
24. Click **Next**. The “Configure the deployment policies” window opens.

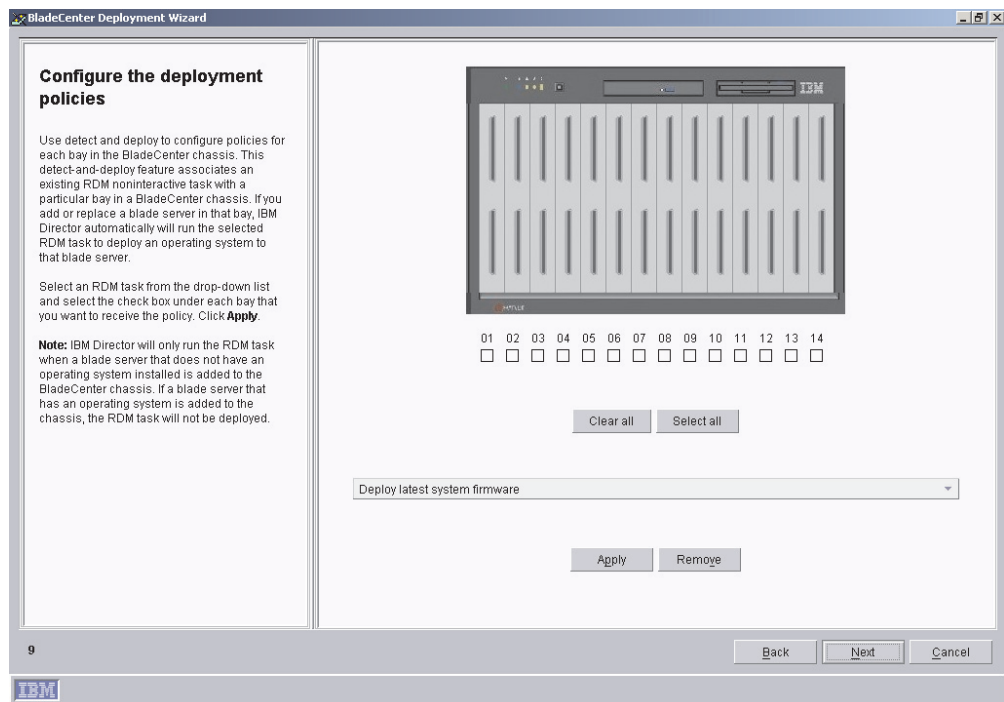


Figure 46. BladeCenter Deployment wizard: “Configure the deployment policies” window

25. 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**.
26. Repeat step 25 until you have configured all the deployment policies.
27. Click **Next**. The “Setup summary” window opens.

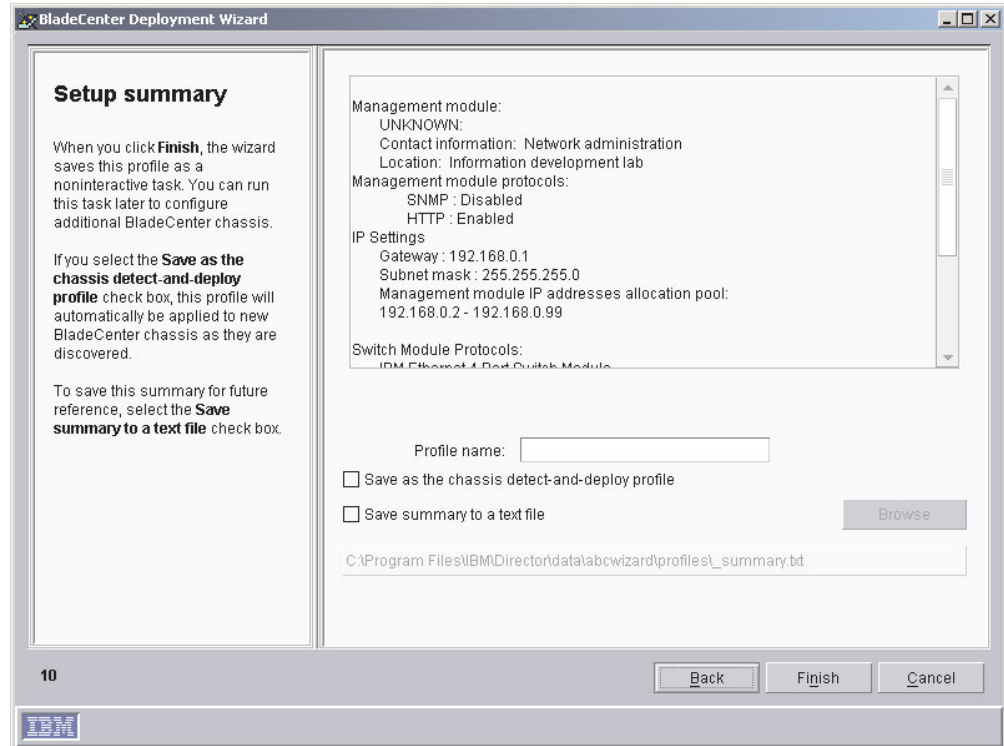


Figure 47. BladeCenter Deployment wizard: “Setup summary” window

28. Review the setup summary. The selected configuration options are displayed in the right pane.
 - a. To change the name, select the text in the **Profile name** field and type a new name for the profile. By default, the profile is given the name you assigned to the management module.
 - 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 setup summary for future reference, select the **Save summary to a text file** check box.
29. Click **Finish**. The profile is created. It appears as a subtask under Deployment Wizard in the Tasks pane of IBM Director Console.

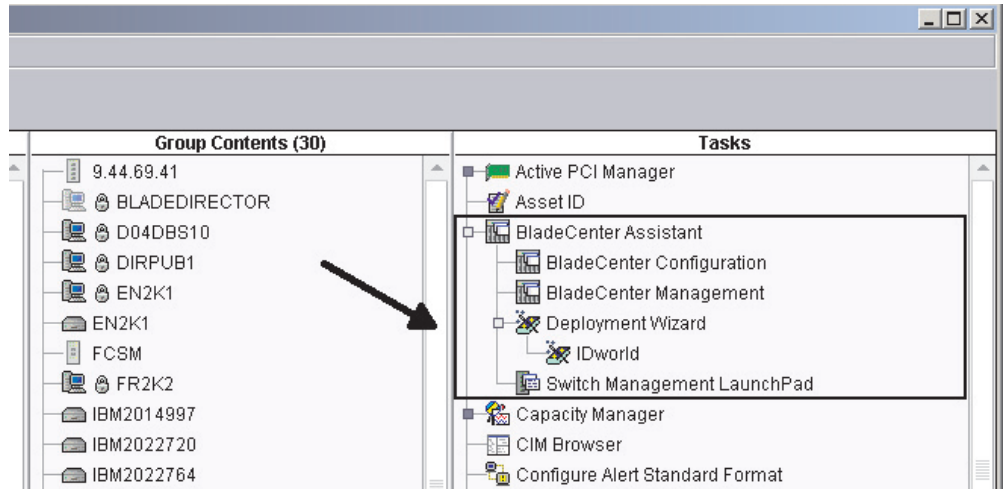


Figure 48. IBM Director Console Tasks pane: Deployment Wizard profile

30. When prompted, select when you want to run the profile. You can select to run the profile now, schedule a task, or cancel.

Chapter 8. Configuring IBM Director

This chapter contains information about using the Event Action Plan wizard, setting discovery preferences and creating management processor objects, authorizing IBM Director users, configuring security settings, and setting up software distribution.

Using the Event Action Plan wizard

The Event Action Plan wizard starts every time you log in to IBM Director Console, until you take one of the following actions:

- Use the Event Action Plan wizard to create an event action plan. You must go through the wizard and click **Finish** on the last window.
- Select the **Do not show this wizard again** check box and then close the Event Action Plan wizard.

If you take one of these actions, you are no longer able to access the Event Action Plan wizard. However, you can create or modify an event action plan using the Event Action Plan Builder. For more information, see the *IBM Director 4.11 Systems Management Guide*.

Note: You also can restrict access to the Event Action Plan wizard by removing users' access to the Event Action Plan Builder task. See "Creating user-account defaults" on page 107.

Complete the following steps to use the Event Action Plan wizard:

1. Start IBM Director Console. The Event Action Plan wizard starts, and the "Welcome to the Event Action Plan wizard" window opens.

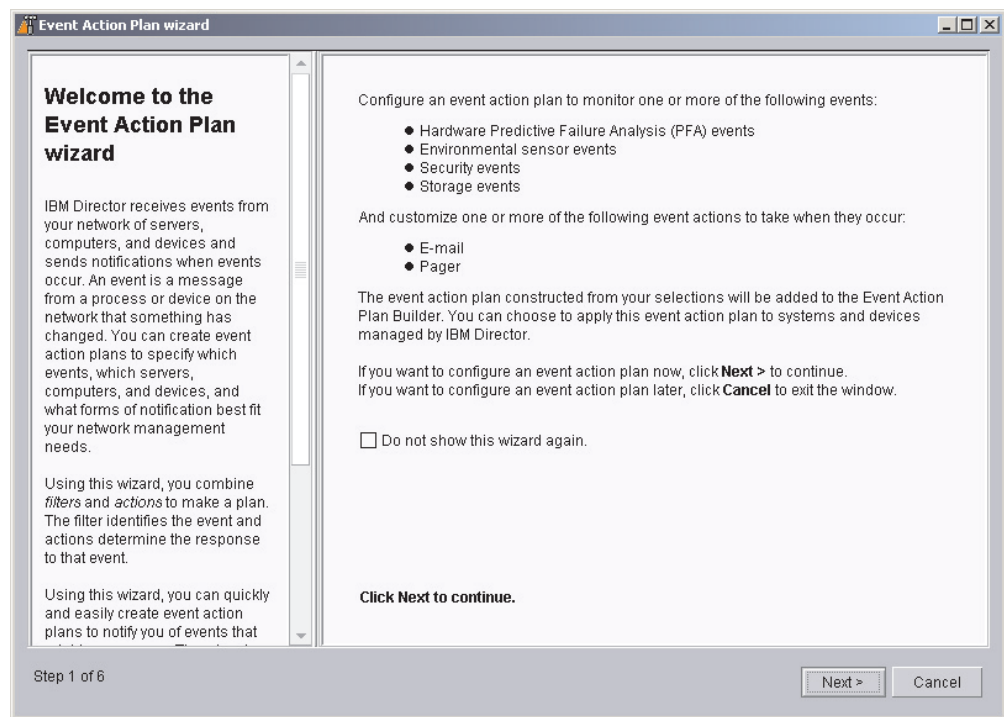


Figure 49. Event Action Plan wizard: "Welcome to the Event Action Plan wizard" window

2. Click **Next**. The “Select the event filters” window opens.

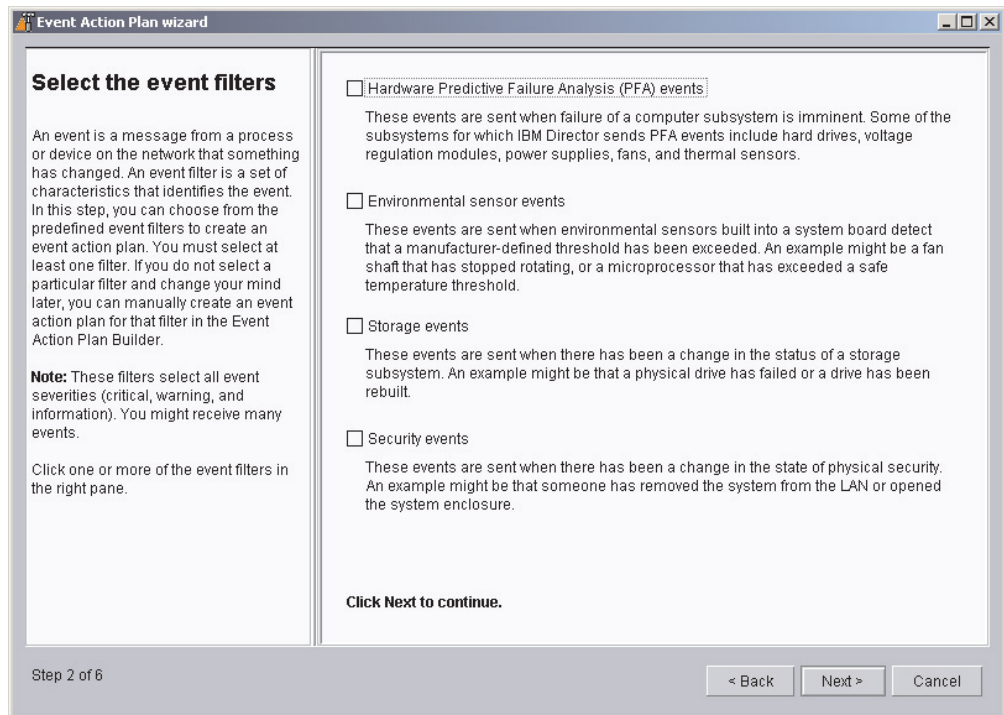


Figure 50. Event Action Plan wizard: “Select the event filters” window

3. Select the check boxes adjacent to the types of events you want to monitor. You can select the following event filters:

Hardware Predictive Failure Analysis® (PFA) events

These events are sent when failure of a computer subsystem is imminent. Some of the subsystems for which IBM Director sends PFA events include hard disk drives, voltage regulation modules, power supplies, and thermal sensors.

Environmental sensor events

These events are sent when environmental sensors built into a system board detect that a manufacturer-defined threshold has been exceeded. An example might be a microprocessor that has exceeded a safe temperature threshold.

Storage events

These events are sent when there has been a change in the status of a storage subsystem. An example might be that a physical drive has failed or a logical drive has been rebuilt.

Security events

These events are sent when there has been a change in the status of physical security. An example might be that someone has removed the system from the LAN or opened the system enclosure.

4. Click **Next**. The “Select the notification” window opens.

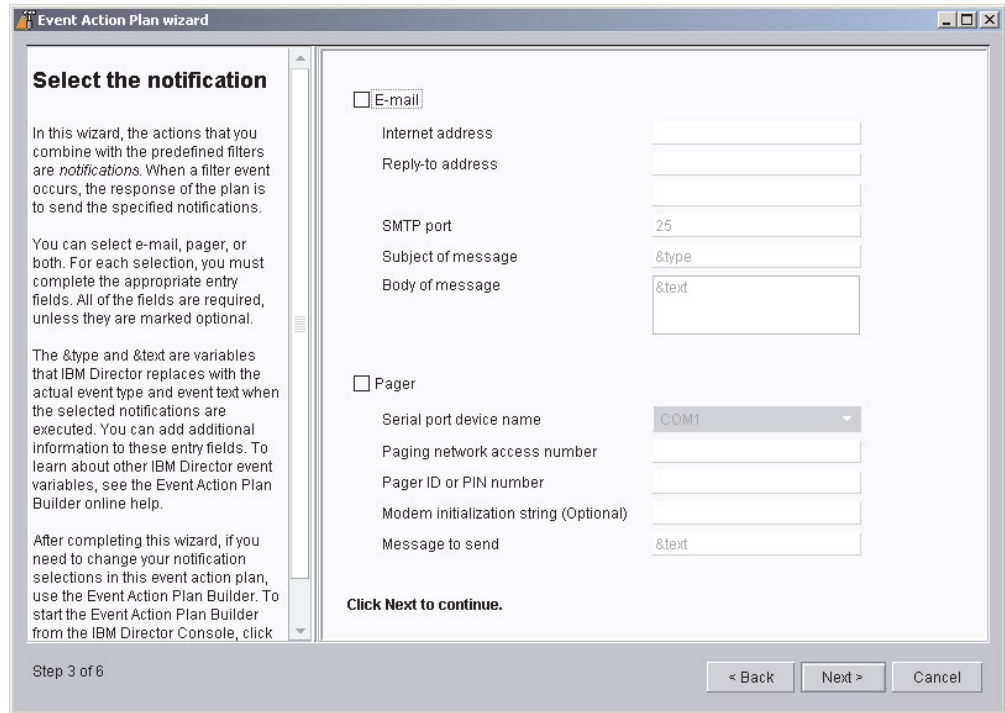


Figure 51. Event Action Plan wizard: “Select the notification” window

5. If you want to be notified by e-mail when an event occurs, select the **E-mail** check box. Then, configure the e-mail notification:
 - a. In the **Internet address** field, type the e-mail address to which the notification will be sent.
 - b. In the **Reply-to address** field, type the e-mail address that will be displayed in the reply-to field of the e-mail.
 - c. In the **SMTP port** field, type the port number of the SMTP server. By default, the SMTP port is set to 25.
 - d. In the **Subject of message** field, type the message that will be displayed in the subject-line of the e-mail. By default, this is set to &type.

You can add additional information to the entry field. For example, you might want to type the following string:

```
IBM Director alert: &system &type
```

When the e-mail is generated, the name of the managed system is substituted for &system, and the type of event that occurred is substituted for &type.

- e. In the **Body of message** field, type the message that will be displayed in the body of the e-mail. By default, this is set to &text.

You can add additional information to the entry field. For example, you might want to type the following string:

```
&time &date &text
```

When the e-mail is generated, the body will contain the time and date the event occurred, as well as details about the event.

Note: &type, &system, &time, &date, and &text are event-data substitution variables. For information about other event-data substitution variables, see the *IBM Director 4.11 Systems Management Guide*.

6. If you want to be notified by pager, select the **Pager** check box. Then, configure the pager notification:
 - a. From the **Serial port device name** list, select the name of the serial port device.
 - b. In the **Paging network access number** field, type the telephone number that will be dialed when an event occurs.
 - c. In the **Pager ID or PIN** field, type the pager ID or personal identification number (PIN).
 - d. In the **Modem initialization string (Optional)** field, type the modem initialization string.
 - e. In the **Message to send** field, type the message that will be sent when an event occurs.
7. Click **Next**. The “Apply the event action plan” window opens.

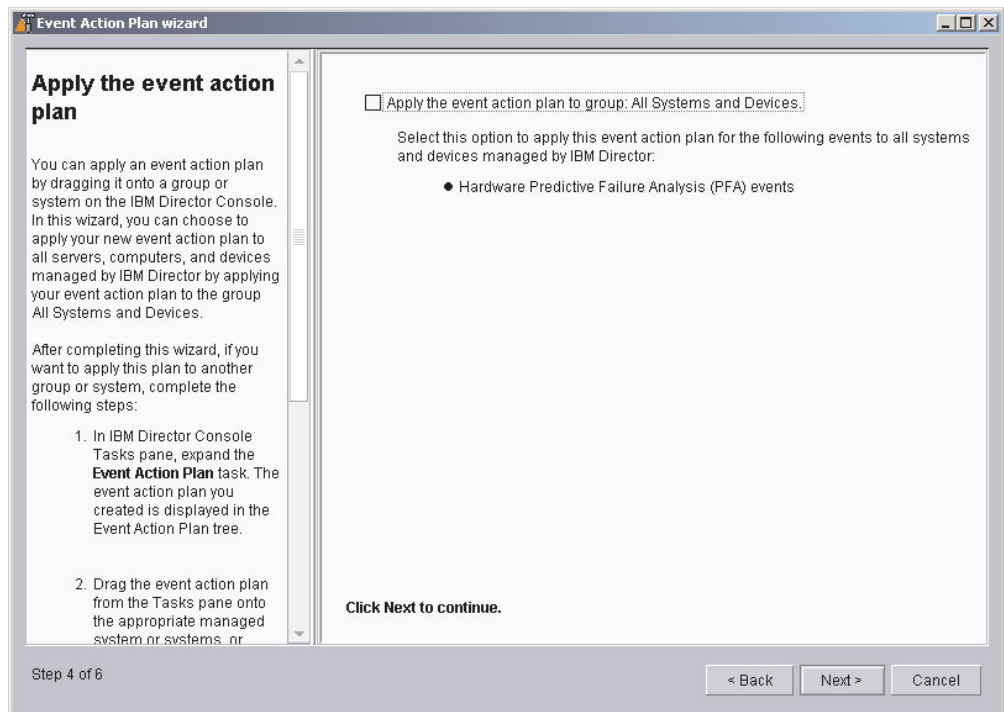


Figure 52. Event Action Plan wizard: “Apply the event action plan” window

8. If you want to apply the event action plan to all systems in the IBM Director environment, select the **Apply event action plan to group: All Systems and Devices** check box.
9. Click **Next**. The “Discover all systems and devices” window opens.

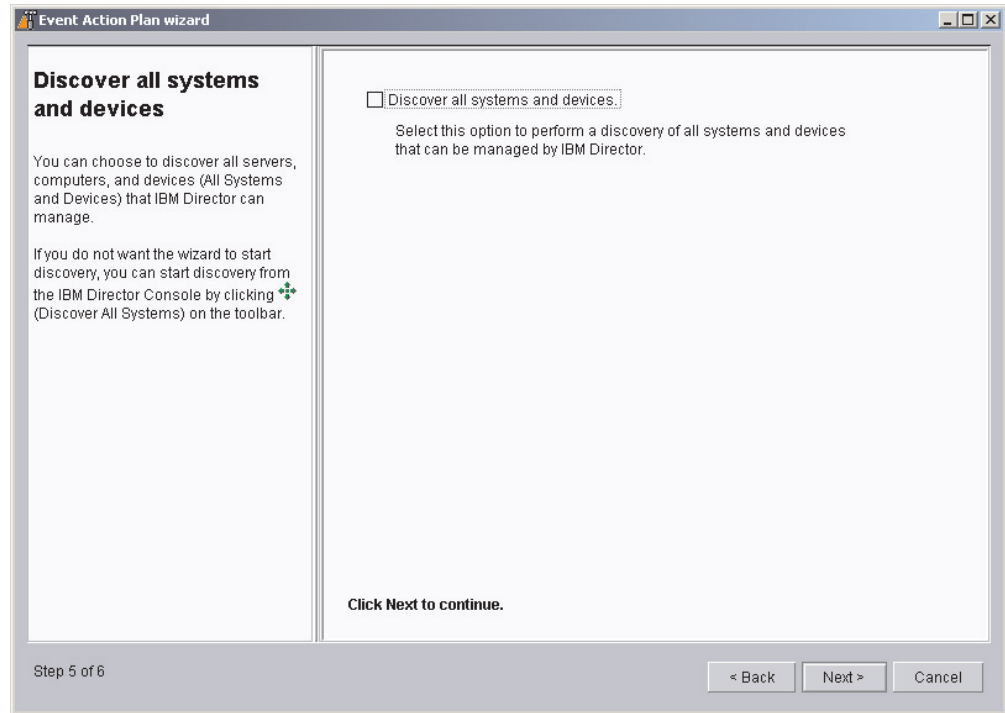


Figure 53. Event Action Plan wizard: “Discover all systems and devices” window

10. If you want IBM Director Server to discover all the managed systems and SNMP devices on the network, select the **Discover all systems and devices** check box.
11. Click **Next**. The “Review your selection summary” window opens.

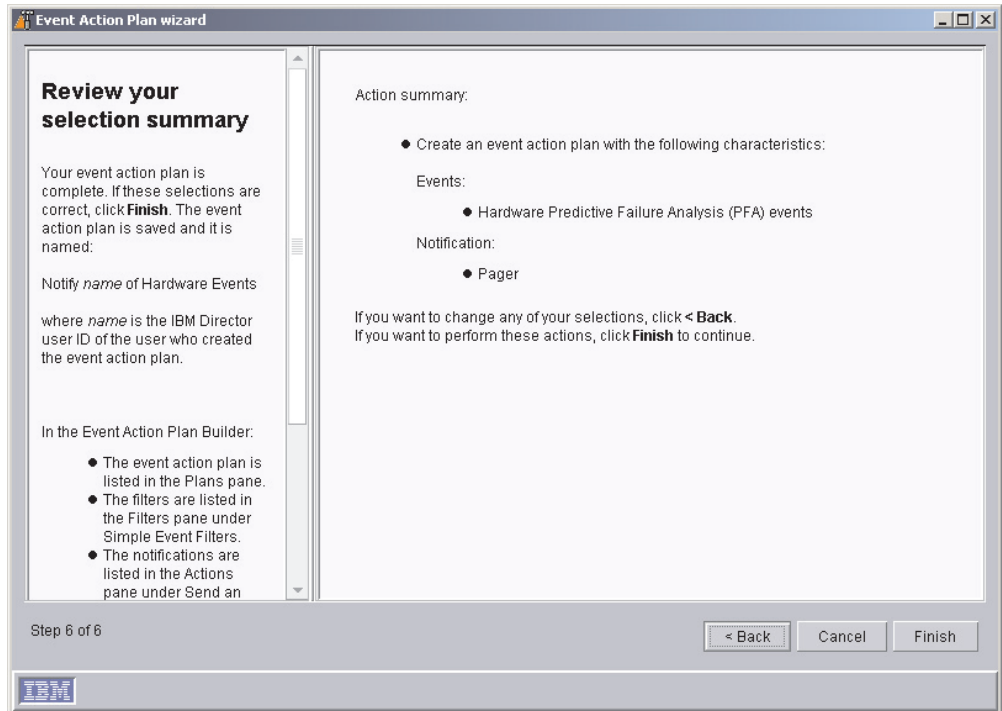


Figure 54. Event Action Plan wizard: “Review your selection summary” window

Review the selections. If you want to change any of your selections, click **Back**.

12. Click **Finish**. The event action plan is saved. It is named “Notify *name* of Hardware Events,” where *name* is the IBM Director user ID of the user who created the event action plan.

Discovering managed systems, devices, and objects

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

Types of discovery

IBM Director supports four types of discovery concerning managed systems and SNMP devices:

Broadcast discovery

Broadcast discovery sends out a general broadcast packet over the LAN. The destination address of this packet depends on the particular protocol used to communicate with the managed systems.

Broadcast discovery also can send out a broadcast packet to specific subnets. If you specify the IP address and subnet mask for a system (a discovery seed address), IBM Director sends a broadcast packet to that specific subnet and discovers all managed systems on that subnet.

Multicast discovery

Multicast discovery operates by sending a packet to the multicast address. By default, IBM Director uses 224.0.1.118 as the multicast address. Managed systems monitor this address and respond to the multicast from the management server. Multicasts are defined with maximum time to live (TTL), which is the number of times a packet is passed between subnets. After the TTL expires, the packet is discarded.

Multicasts are useful for networks that filter broadcasts but do not filter multicasts. Multicast discovery is available only for TCP/IP systems.

Unicast discovery

Unicast discovery sends a directed request to a specific address or range of addresses. This method generates a discovery request for each address in the range, but it is useful in networks where both broadcasts and multicasts are filtered. To discover certain types of managed systems (for example, dial-up systems), it might be necessary to use Unicast discovery. Unicast discovery is available only for TCP/IP systems.

Broadcast relay agents

Broadcast relay enables the server to discover TCP/IP and IPX systems when the systems are not directly reachable by broadcast packets because of network configuration. This situation can occur in networks where the management server and managed systems are in separate subnets and the network between them does not allow broadcast packets to pass from one subnet to the other.

This option generates less network traffic than unicast discovery and avoids many of the problems associated with filtered broadcasts. In broadcast relay, the management server sends a special discovery request message to a particular managed system, instructing the managed system to perform a discovery on the local subnet using a general broadcast. When managed systems on that subnet receive the discovery request, they reply to the management server that made the original request.

The management server performs all types of discovery simultaneously.

Setting discovery preferences

Complete the following steps to configure discovery preferences:

1. From IBM Director Console, click **Options** → **Discovery Preferences**. The “Discovery Preferences” window opens.

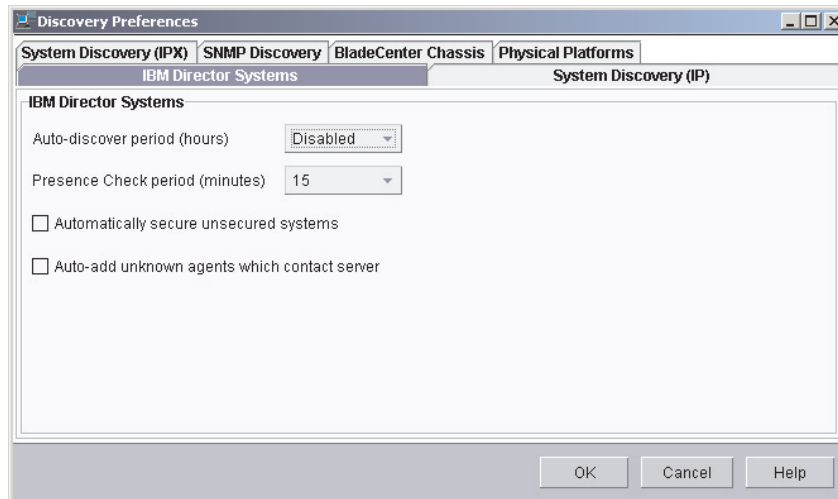


Figure 55. “Discovery Preferences” window

This window has six pages:

IBM Director Systems

Sets general discovery preferences

System Discovery (IP)

Defines how IBM Director discovers managed systems reachable through TCP/IP

System Discovery (IPX)

Defines how IBM Director discovers managed systems reachable through IPX

SNMP Discovery

Defines how IBM Director discovers SNMP devices

BladeCenter Chassis

Sets general discovery preferences for BladeCenter chassis

Physical Platforms

Sets general discovery preferences for physical platforms

- To move from one page to another, click the applicable tab. Click **OK** when you have finished configuring discovery preferences.

Discovering service processors

While IBM Director automatically discovers and creates physical platform managed objects for Remote Supervisor Adapters with updated firmware, IBM Director only discovers the following service processors when they are installed in servers on which IBM Director Agent is installed:

- ISMP
- ASM processor
- ASM PCI Adapter
- Remote Supervisor Adapter (without updated firmware)

For more information about which Remote Supervisor Adapters are automatically discovered, see “Updating Remote Supervisor Adapter firmware” on page 27.

In addition, if you add an ASM PCI Adapter or a Remote Supervisor Adapter to a server that contains an ASM processor, you must manually create a management processor object for the optional service processor.

Manually creating a management processor object

In the following situations, IBM Director does not discover service processors and make physical platform objects automatically:

- You add an ASM PCI Adapter to a server that contains an ASM processor.
- You add a Remote Supervisor Adapter to a server that contains an ASM processor.

In both of these scenarios, the ASM processor acts as the service processor for the server; the ASM PCI Adapter and the Remote Supervisor Adapter serve as a gateway to the ASM interconnect network.

For IBM Director to manage the ASM PCI Adapter or the Remote Supervisor Adapter, you must create a management processor object manually. After you create a management processor object, you can perform the following tasks:

- Configure the ASM PCI Adapter or Remote Supervisor Adapter using the Management Processor Assistant task
- Use out-of-band management to manage all ASM processors on the ASM interconnect network

Complete the following steps to create a management processor object manually:

1. Start IBM Director Console.
2. Right-click in the Group Contents pane; then, click **New → Management Processors**. The “Add Management Processors” window opens.

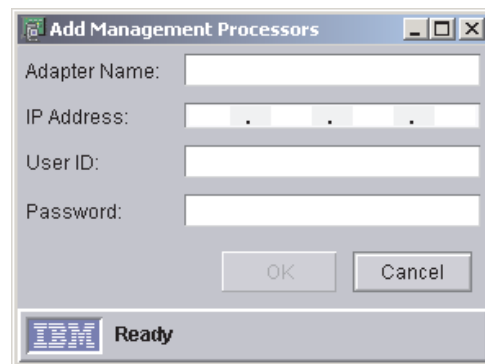


Figure 56. “Add Management Processors” window

3. In the **Adapter Name** field, type a name for the service processor.

Note: A best practice is assign the service processor a name that clearly identifies the service processor type and the server that it manages, for example, SystemName-ServiceProcessorType.

4. In the **IP Address** field, type the IP address of the service processor.
5. In the **User ID** field, type a valid user ID for the service processor.
6. In the **Password** field, type the password that corresponds to the user ID you typed in step 5.
7. Click **OK**.

8. The management processor object is displayed in the Group Contents pane.

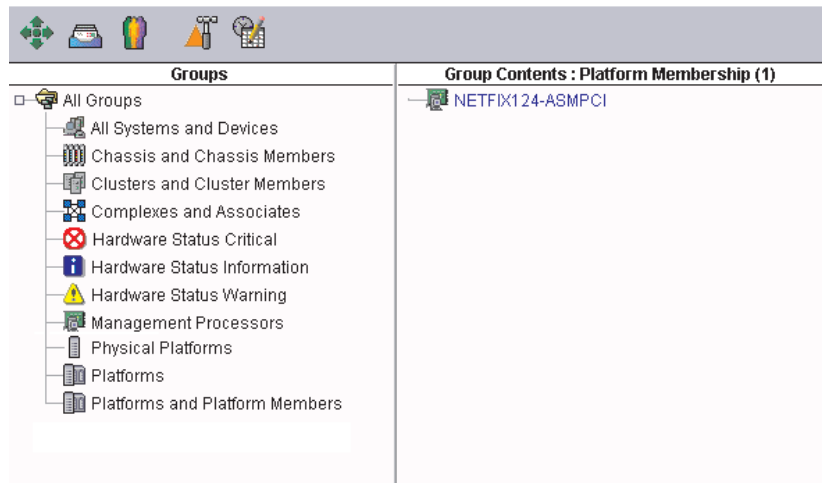


Figure 57. IBM Director Console: Group Contents pane

Authorizing IBM Director users

IBM Director Console uses the operating-system user accounts for user-logout security. When a user logs in to IBM Director, the user ID and password verification process used by the operating system is used to validate the user's authority to access IBM Director.

To use IBM Director, a user must have an operating-system account on the management server or the domain *and* be a member of either the DirAdmin or DirSuper group. When IBM Director Server is installed, these two groups are automatically created on the operating system. Members of the DirAdmin group have basic administrative privileges in the IBM Director environment; members of the DirSuper group have super user privileges.

On Windows, the IBM Director service account is assigned automatically to the DirSuper group, and all accounts with administrator privileges are assigned automatically to the DirAdmin group. On Linux, the diradmin and dirsUPER groups are not populated automatically; a user with root privileges must assign users to the groups.

Users' ability to perform tasks depends on which access privileges they have been assigned in the IBM Director environment. You can configure a default set of privileges for all user accounts, and you can edit user accounts on an individual basis.

Creating user-account defaults

You can use the User Defaults Editor to set the default access privileges for all members of the DirAdmin group. Complete the following steps to create user-account defaults:

1. In IBM Director Console, click **Options** → **User Administration**. The “User Administration” window opens.

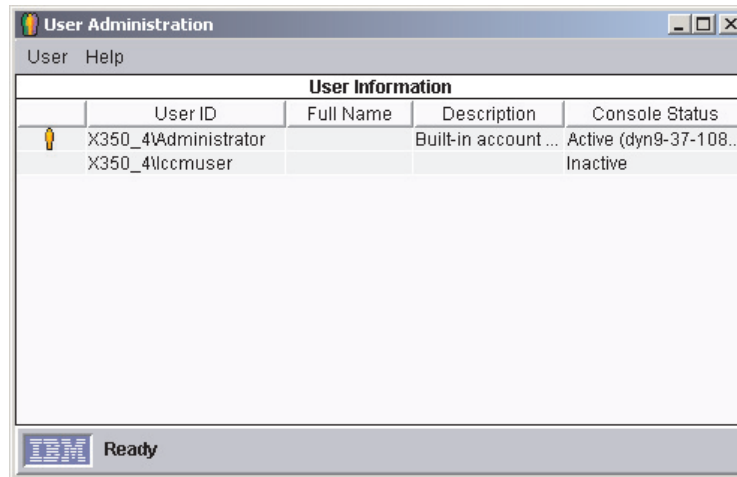


Figure 58. “User Administration” window

This window contains a list of all users authorized to access IBM Director.

2. Click **User** → **User Defaults**. The “User Defaults Editor” window opens.

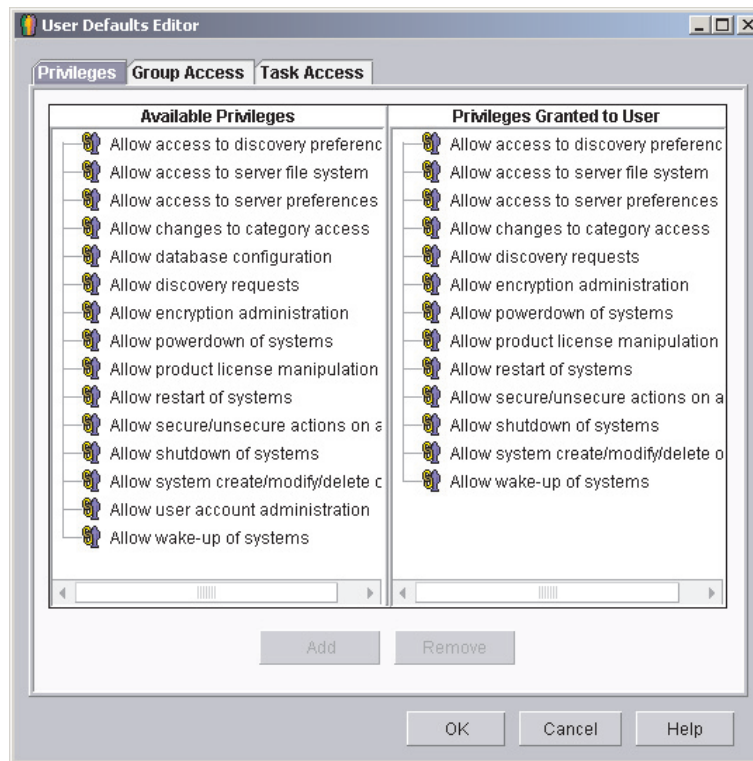


Figure 59. “User Defaults Editor” window

From this window, you can set the default access privileges for all members of the DirAdmin group.

Notes:

- a. For increased security, consider removing all default access privileges. You will have to set access levels for each user, but you can be sure that a user will not accidentally get access to restricted groups or tasks.
- b. You can restrict access to the Event Action Plan wizard by removing users' access to the Event Action Plan Builder task.

Editing an individual user's access privileges

Complete the following steps to edit a user's access privileges:

- 1. In IBM Director Console, click **Options** → **User Administration**. The "User Administration" window opens.

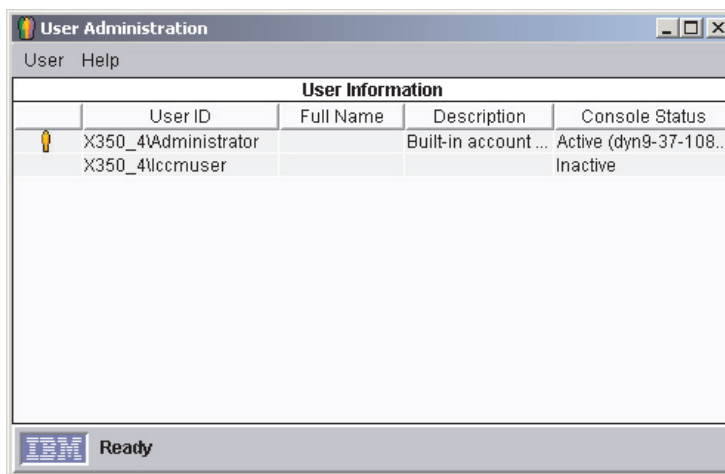


Figure 60. "User Administration" window

This window contains a list of all users authorized to access IBM Director.

- 2. Select the user whose access privileges you want to modify. Click **User** → **Edit**. The "User Editor" window opens.

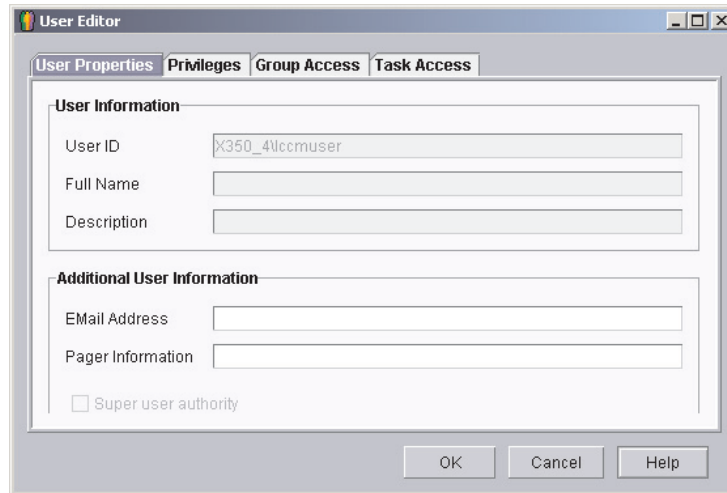


Figure 61. “User Editor” window: “User Properties” page

3. Click the **Privileges** tab. The “Privileges” page is displayed.

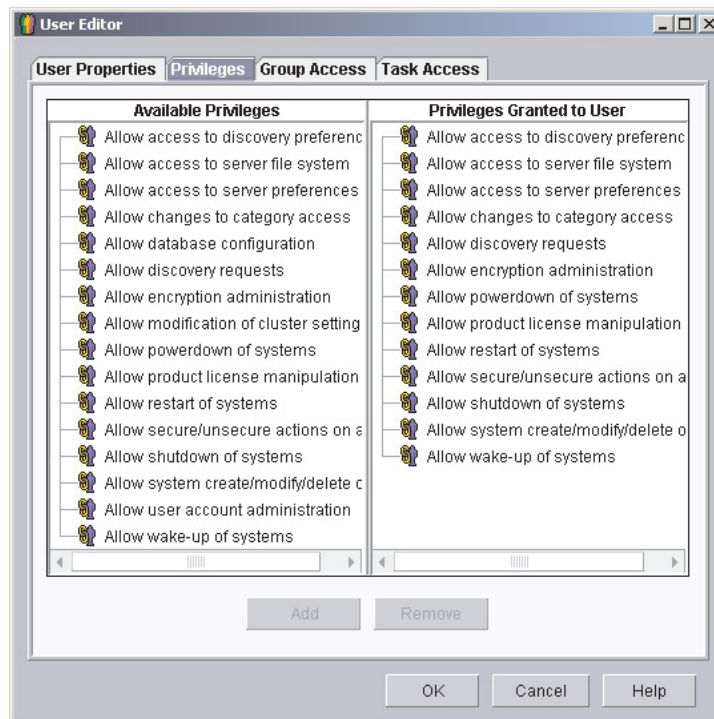


Figure 62. “User Editor” window: “Privileges” page

4. To add a privilege, click the privilege in the **Available Privileges** pane and then click **Add**.
To remove a privilege, click the privilege in the **Privileges Granted to User** pane and then click **Remove**.
5. To restrict the user’s access to groups, click the **Group Access** tab. The “Group Access” page is displayed.

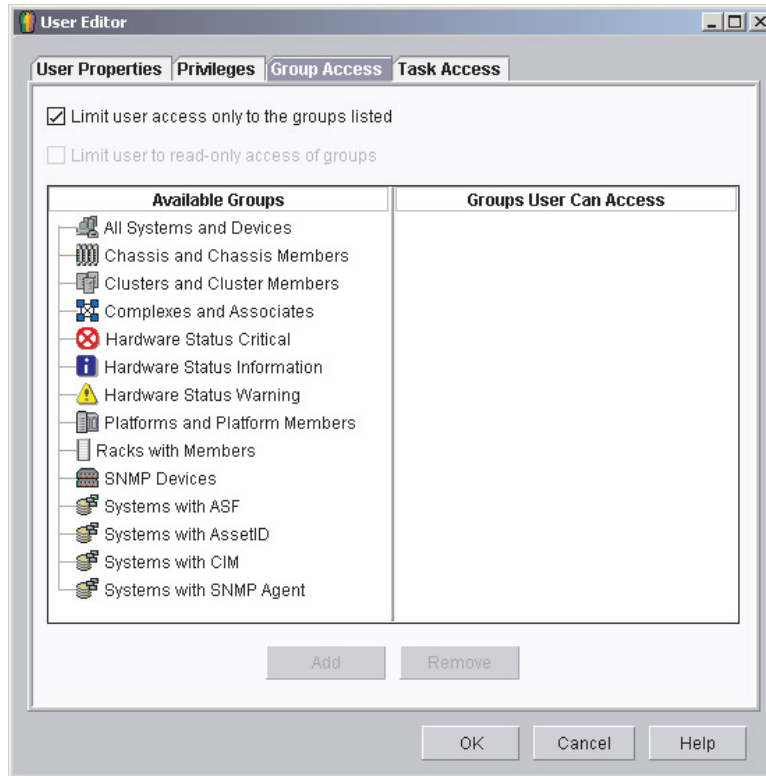


Figure 63. “User Editor” window: “Group Access” page

6. To permit the user to access specific groups only, select the **Limit user access only to the groups listed** check box. To add a group, click the group in the **Available Groups** pane and click **Add**. To remove a group, click the group in the **Groups User Can Access** pane and click **Remove**.

To prevent the user from creating new groups or modifying existing groups, select the **Limit user to read-only access of groups** check box.

7. To restrict the user’s access to tasks, click the **Task Access** tab. The “Task Access” page is displayed.

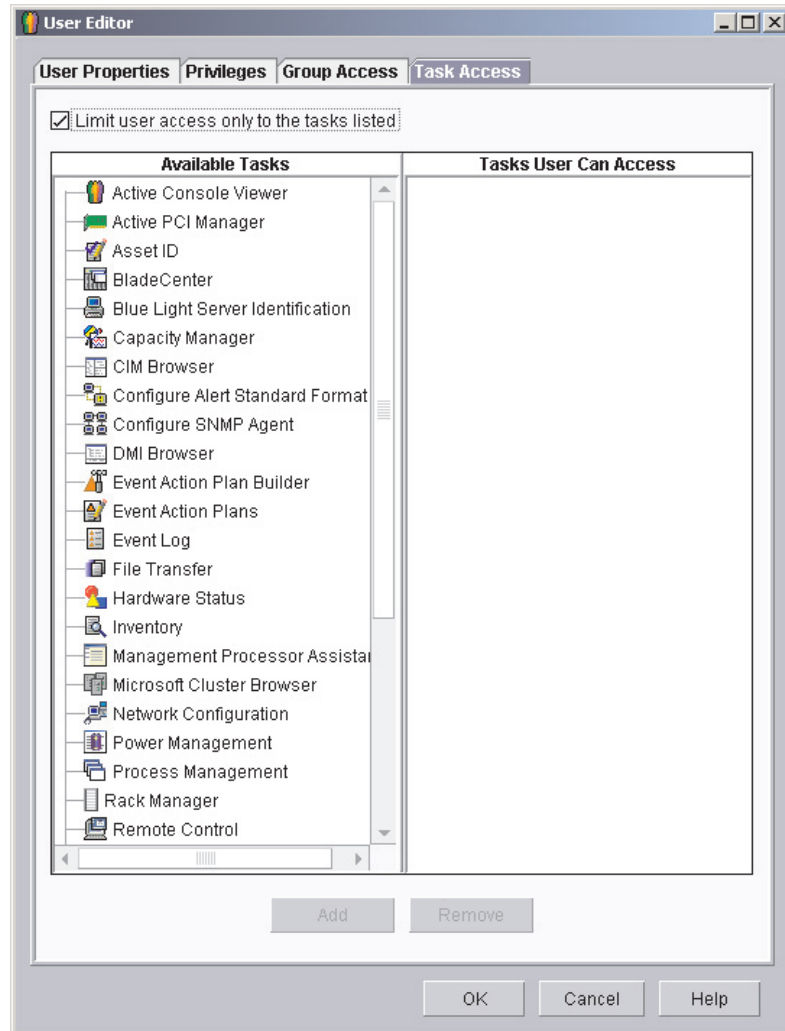


Figure 64. “User Editor” window: “Task Access” page

8. To restrict the user to performing certain tasks only, select the **Limit user access only to the tasks listed** check box. To add a task, click the task in the **Available Tasks** pane and click **Add**. To remove a task, click the task in the **Tasks User Can Access** pane and click **Remove**.

Note: You can restrict access to the Event Action Plan wizard by removing the user’s access to the Event Action Plan Builder task.

9. When you have finished editing the user’s privileges, click **OK**. The “User Editor” window closes.

Configuring security settings

This section contains information about enabling secure socket layers (SSL) and restricting IBM Director Console sessions to particular ports and session keys. It also includes information about configuring a custom access policy for Web-based Access.

Enabling SSL

You must modify the TWGConsole.prop and TWGServer.prop files to enable SSL. If you installed IBM Director in the default location, these files are located in the following directories:

For Windows	<code>d:\Program Files\IBM\Director\data</code>
For Linux	<code>/opt/IBM/director/data/</code>

where *d* is the hard disk on which IBM Director is installed.

Complete the following steps to enable SSL:

1. Open the TWGConsole.prop file in an ASCII text editor.
2. Modify the value of twg.gateway.link.1 to read as follows:
`twg.gateway.link.1=com.tivoli.twg.libs.TWGSSLLink`
3. Save and close the TWGConsole.prop file.
4. Open the TWGServer.prop file in an ASCII text editor.
5. Add the following line to the TWGServer.prop file:
`twg.gateway.link.1=com.tivoli.twg.libs.TWGSSLLink`
6. Save and close the TWGServer.prop file.

All supported cipher suites are enabled by default.

Enabling specific cipher suites

You can restrict IBM Director Console sessions to particular ports and session keys. For example, complete the following steps to restrict IBM Director Console sessions to using the default port (2033) and a 128-bit RC5 session key:

1. Open the TWGConsole.prop file in an ASCII text editor. If you installed IBM Director Console in the default location, this file is located in the following directory:

For Windows	<code>d:\Program Files\IBM\Director\data</code>
For Linux	<code>/opt/IBM/director/data/</code>

where *d* is the hard disk on which IBM Director is installed.

2. Modify the file so that it contains the following properties:

```
twg.gateway.link.1=com.tivoli.twg.libs.TWGSSLLink
twg.gateway.link.1.initparm=* -cipherSuites
SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA
```

Note: The specified cipher suites must be separated by a comma; do not add a space after the comma.

3. Save and close the PROP file.
4. Import the applicable RSA or SHA certificate into the following directory:

For Windows	<code>d:\Program Files\IBM\director\jre\lib\security\jssecacerts</code>
For Linux	<code>/opt/IBM/director/jre/lib/security/jssecacerts</code>

where *d* is the hard disk on which IBM Director is installed.

You can use the keytool program located in the following directory:

For Windows	<code>d:\Program Files\IBM\director\jre\bin</code>
For Linux	<code>/opt/IBM/director/jre/bin/keytool</code>

where *d* is the hard disk on which IBM Director is installed. You can download information about the keytool program from [http:// www.java.sun.com](http://www.java.sun.com).

5. Open the TWGServer.prop file in an ASCII text editor. If you installed IBM Director Server in the default location, this file is located in the following directory:

For Windows	<code>d:\Program Files\IBM\Director\data</code>
For Linux	<code>/opt/IBM/director/data/</code>

where *d* is the hard disk on which IBM Director is installed.

6. Repeat steps 2 through 4 on page 112.

To establish an SSL session without importing an RSA or SHA certificate, use an anonymous cipher suite.

Configuring a custom access policy for Web-based Access (Windows only)

If IBM Director Agent is installed on a Windows NT file system (NTFS) partition, you can configure a custom access policy for Web-based Access.

Note: Windows XP might hide the file permission editor. You must enable editing of file permissions before you can modify the access policy.

Complete the following steps to customize the access policy:

1. Using Windows Explorer, select the admin4.txt file. If you installed IBM Director Agent in the default location, this file is located in `d:/Program Files/IBM/Director/websrv/cgi-bin/`, where *d* is the hard disk on which IBM Director Agent is installed.
2. Edit the file access permissions. Grant read access to this file for users and groups that you want to be able to modify system settings.
3. Using Windows Explorer, select the user1.txt file. If you installed IBM Director Agent in the default location, this file is located in `d:/Program Files/IBM/Director/websrv/cgi-bin/`, where *d* is the hard disk on which IBM Director Agent is installed.
4. Edit the file access permissions. Grant read access to this file for users and groups that you want to be able to view but not modify the system settings

Note: Do *not* delete the admin4.txt and user1.txt files to restrict all Web-based Access to the managed system. Instead, remove the read-only permissions for administrators and users, and leave the files in the `Program Files/IBM/Director/websrv/cgi-bin/` directory.

Configuring software distribution

You can use the IBM Director Software Distribution task to import IBM software, build software packages using the Director Update Assistant wizard, and distribute the packages to managed systems.

If you purchase and install IBM Director 4.1 Software Distribution (Premium Edition), you have additional capabilities. You can accomplish the following additional tasks:

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

Note: Managed systems running NetWare or Caldera Open UNIX do not support the IBM Director Software Distribution task.

Methods of software distribution

IBM Director supports the following methods of software distribution:

- Streaming from the management server
- Redirected distribution

Streaming from the management server

Software-distribution packages are copied directly from the management server to the managed system.

This method of software distribution is resource-intensive. It can have a negative effect on the management server performance. In addition, a package distributed by this method requires that the target managed system has empty disk space twice the size of the package.

Streaming from the management server has one advantage, however. 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.

Because of the potential to resume distribution, you might prefer to stream a software package from the management server in the following situations:

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

Redirected distribution

Many software packages are tens or hundreds of megabytes in size. Distributing software of this size across a large network can cause bottlenecks in network data transmission. To avoid this problem, you can set up a universal naming convention (UNC) or FTP share on a network server. IBM Director Server streams software packages to the network share, where they are cached. From the share, they are either streamed to the managed systems or, in the case of software that uses the Microsoft Windows Installer or InstallShield as the installation utility, installed directly from the file-distribution server.

Redirected distribution greatly reduces the software-distribution traffic in your network. It uses fewer management server system resources. In addition, if you

install InstallShield or Microsoft Windows Installer (MSI) packages directly from the file-distribution server, redirected distribution requires less disk space on the managed systems.

Redirected distribution has one limitation: if a redirected distribution of a software package is interrupted (for example, if the network connection is lost), the installation must begin all over.

Setting up file-distribution servers

IBM Director supports UNC-based and FTP-based file distribution software. See your server documentation for information about setting up a shared subdirectory.

Note: You do not need to install IBM Director on the file-distribution server.

File-distribution server considerations

Consider the following issues when setting up file-distribution shares:

- In a Windows environment, the file-distribution server must either be a member of the same domain as the management server or have a trust relationship with that domain.
- The share must allow full read/write access to the management server. If the IBM Director service account does not have read/write access, software distribution defaults to streaming from the management server.
- The share must allow read access to all managed systems that you want to access the share.
- If the file-distribution server is configured as an FTP server, you can select to use FTP when transferring packages from the management server to the share. For managed systems running Windows, the home directory for the FTP login must be the same directory as the file-distribution server. For example, if `c:\stuff\swd_share` is mapped to `\\server\swd_share`, then `c:\stuff\swd_share` must be the home directory for the FTP user ID login used on the FTP file-distribution server configuration screen.
- If you want managed systems to access the share using null credentials, you must issue the `TWGshare` command. This alters a registry setting on the file-distribution server, which enables managed systems to access the share using null credentials. To issue the `TWGSHARE` command, complete the following steps:
 1. Copy the `twgshare.exe` file to the file-distribution server. This file is located in the `\IBM\director\bin\` directory.
 2. From a command prompt, type the following command:

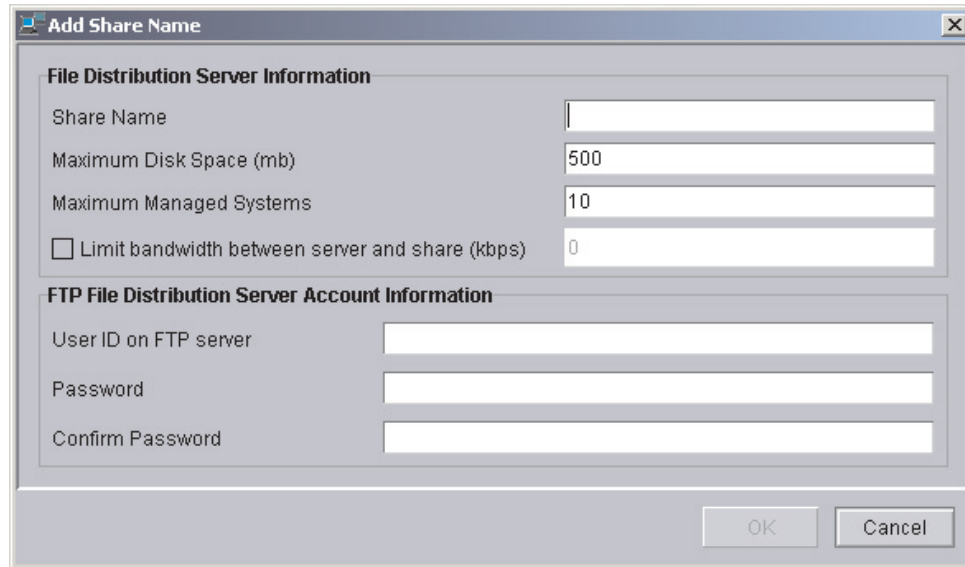
```
twgshare-a sharename
```

where *sharename* is the name of the share on the file-distribution server.
- If you do not want to use null credentials (which are a security risk), you must set up an operating-system account on the file-distribution server. Use the user ID and password for this account when you configure distribution preferences for managed systems. See “Configuring distribution preferences for managed systems” on page 118.

Configuring IBM Director to use a file-distribution server

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

1. Start IBM Director Console.
2. Click **Options** → **Server Preferences**. The “Server Preferences” window opens.
3. Click the **File Distribution Server** tab. A list is displayed of all configured file-distribution servers.
4. Click **Add**. The “Add Share Name” window opens.



The screenshot shows a dialog box titled "Add Share Name" with a close button (X) in the top right corner. It is divided into two main sections. The first section, "File Distribution Server Information", contains four input fields: "Share Name" (empty), "Maximum Disk Space (mb)" (500), "Maximum Managed Systems" (10), and "Limit bandwidth between server and share (kbps)" (0) with an unchecked checkbox. The second section, "FTP File Distribution Server Account Information", contains three input fields: "User ID on FTP server", "Password", and "Confirm Password", all of which are empty. At the bottom right, there are "OK" and "Cancel" buttons.

Figure 65. IBM Director Console: “Add Share Name” window

5. In the **Share Name** field, type the name of the file-distribution server using UNC notation. To specify FTP as the transport protocol, begin the share-name entry with ftp:, for example ftp:\\ServerName\\AccountName.
6. In the **Maximum Disk Space** field, type the maximum amount of disk space (in MB) that can be allocated on the file-distribution server for software distribution.
7. In the **Maximum Managed Systems** field, type the maximum number of managed systems that can receive a software package at the same time.
8. To limit the bandwidth that can be used to send packages between IBM Director Server and the file-distribution server, select the **Limit bandwidth between server and share (kbps)** check box. In the entry field, type the maximum bandwidth, in kilobytes per second (KBps), that can be used to send packages between IBM Director and the file-distribution server.

Note: You might want to limit the bandwidth when a dedicated connection, such as integrated services digital network (ISDN), is used for copying the files from IBM Director Server to the share.

9. If you specified an FTP-based server in step 5 on page 116, you must provide information about the FTP server:
 - a. In the **User ID on FTP server** field, type a user ID authorized to access the FTP server installed on the share.
 - b. In the **Password** field, type the password associated with the user ID.
 - c. In the **Confirm password** field, retype the password associated with the user ID.
10. Press **OK**. The “Server Preferences” window reopens. The data you entered in the “Add Share” window is displayed.

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

Configuring software-distribution preferences

Complete the following steps to configure software-distribution preferences:

1. If necessary, start IBM Director Console.
2. Click **Options** → **Server Preferences**. The “Server Preferences” window opens.
3. Click the **Software Distribution** tab. The “Software Distribution” page is displayed.

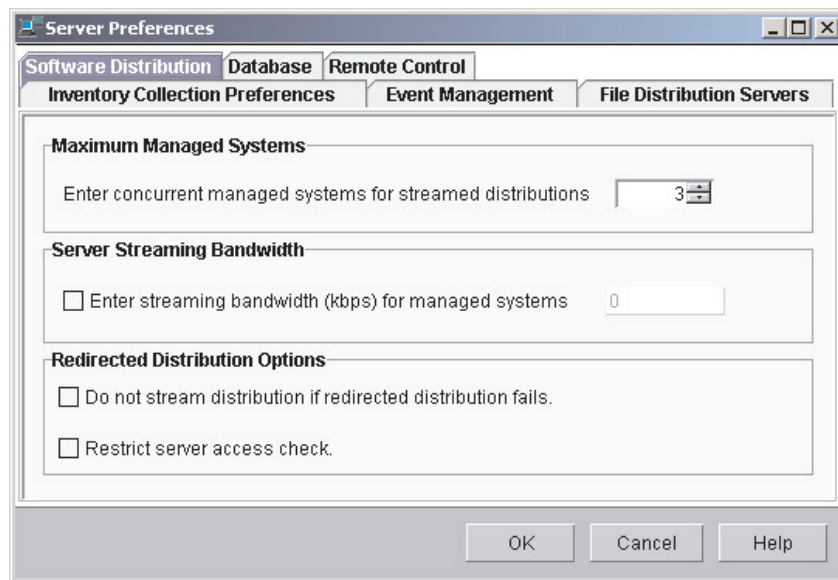


Figure 66. IBM Director Console: “Software Distribution” page

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

Note: To specify values less than 1 KBps, type a decimal. The minimum acceptable value is 0.25 (256 bytes per second).

6. To avoid streaming a package in the event that a redirected distribution fails, select the **Do not stream distribution if redirected distribution fails** check box.

7. To prevent IBM Director Server from performing an access check of *all* of the file-distribution shares, select the **Restrict server access check** check box. This restricts the access check to *only* the file-distribution shares you configure for a specific managed system or group. See “Configuring distribution preferences for managed systems” for more information about restricting access to specific file-distribution shares.
8. Click **OK**.

Configuring distribution preferences for managed systems

After you configure IBM Director to use a file-distribution server, you can assign unique policies to a managed system and groups. By default, a managed system attempts to access all shares that have been defined to the management server. You can configure the following software-distribution preferences for a managed system or group:

- Restrict access to specific shares
- Specify whether software distribution occurs through streaming or redirected distribution
- Limit the bandwidth used for software distribution

Complete the following steps to define distribution preferences:

1. If necessary, start IBM Director Console.
2. In the Group Contents pane, right-click the managed system or group.
3. Click **Distribution Preferences**. The “Set Managed System Distribution Preferences” window opens.

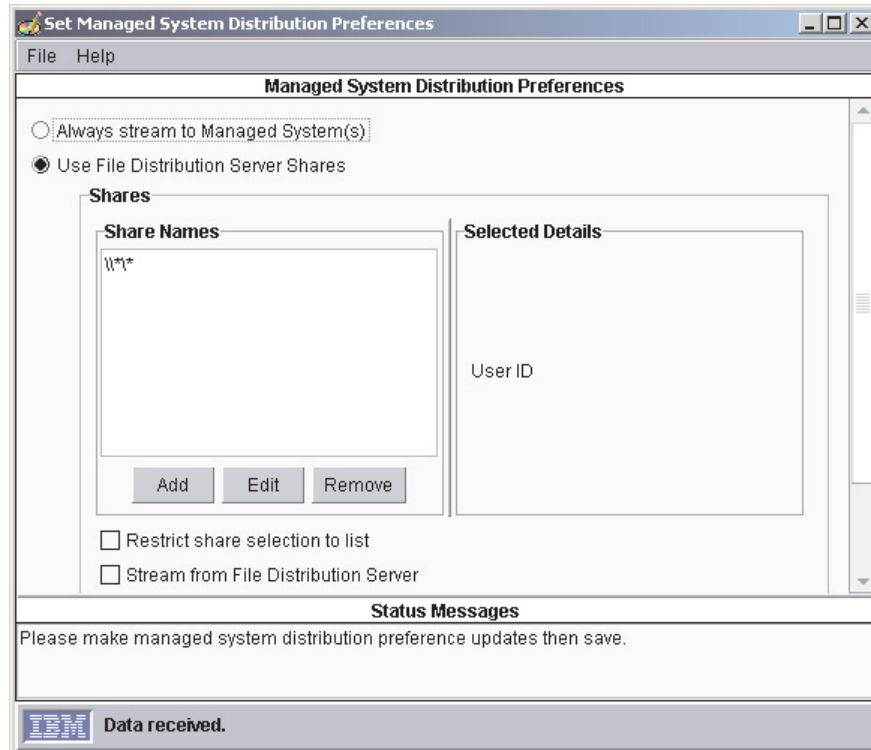


Figure 67. IBM Director Console: “Managed System Distribution Preferences” window

4. Select the method of software distribution:
 - If you want to copy packages directly from IBM Director Server to the managed system or group, click **Always stream to the Managed System(s)**.
 - If you want to copy packages from a share to the managed system or group, click **Use File Distribution Server Shares**.
5. To add a share, click **Add**. The “Add Share Name” window opens.

Figure 68. IBM Director Console: “Add Share Name” window

In the **Share Name** field, type the name of the share using UNC notation. To specify FTP as the transport protocol, begin the share-name entry with ftp:, for example, ftp:\\ServerName\AccountName.

In the **File Distribution Server Account Information** group box, type the information necessary to access the share.

Click **OK**.

6. Repeat step 5 until you have added all the shares that you want the managed system or group to access.
7. If you want to limit the shares that the managed system or group can access to only those displayed, select the **Restrict share selection to list** check box.

Note: If you do not select this option, other defined shares can be used for software distribution if the shares displayed are not available. In this situation, UNC-based shares are accessed using null credentials and FTP-based shares are accessed anonymously.

8. To ensure that software packages are always streamed rather than installed remotely, select the **Stream from File Distribution Server** check box.

Note: Software packages that contain applications that use Microsoft Windows Installer (MSI) or InstallShield as their installation mechanism are installed directly from the file-distribution share *unless* the **Stream from File Distribution Server** check box is selected.

9. To limit the bandwidth used when copying packages from the file-distribution server to the managed system or group, select the **Enter streaming bandwidth (kbps) for managed systems** check box. In the entry field, type the bandwidth, in kilobytes per second (KBps), used for copying packages to the managed system or group. This value also determines the bandwidth used to copy packages from IBM Director Server and the managed system or group.

Chapter 9. Installing IBM Director extensions

This chapter contains procedures for installing the IBM Director Server Plus Pack extensions located on the *IBM Director Server Plus Pack CD*.

For an overview of the IBM Director Server Plus Pack, see “IBM Director Server Plus Pack” on page 8.

Completing the Rack Manager installation on the management server

Note: If you did not install Rack Manager when you installed IBM Director Server, do so before continuing with this procedure. For information about modifying an IBM Director Server installation to add Rack Manager, see “Modifying an IBM Director installation” on page 173.

To complete the Rack Management installation on the management server, you must install the Rack Management component located on the *IBM Director Server Plus Pack CD*. This section contains procedures for installing this component on management servers running either Windows or Linux.

Completing the Rack Manager installation on Windows

Complete the following steps to finish installing Rack Manager on a management server running Windows:

1. Insert the *IBM Director Server Plus Pack CD* into the CD-ROM drive.
2. Start Windows Explorer, and open the `\rackmgr\server\windows\i386` directory located on the *IBM Director Server Plus Pack CD*.
3. Double-click **setup.exe**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
4. Click **Next**. A window that contains the license agreement opens.
5. Click **Yes** to accept the license agreement. The “Start Copying Files” window opens.
6. Click **Next**. The “InstallShield Wizard Complete” window opens.
7. Click **Finish**.
8. Remove the *IBM Director Server Plus Pack CD* from the CD-ROM drive.
9. Shut down and restart the management server.

Completing the Rack Manager installation on Linux

Complete the following steps to finish installing Rack Manager on a management server running Linux:

1. Stop IBM Director. From a command prompt, type the following command and press Enter:
`/opt/IBM/director/bin/twgstop`
2. Insert the *IBM Director Server Plus Pack CD* into the CD-ROM drive.
3. If the CD does not automount, go to step 4 on page 122. If the CD automounts, type the following command and press Enter:
`umount /mnt/cdrom`

where `mnt/cdrom` is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

5. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/rackmgr/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

6. Type the following command and press Enter:

```
./dirinstall
```
7. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```
8. To unmount the CD-ROM drive, complete the following steps:
 - a. Type `cd /` and press Enter.
 - b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

9. Remove the *IBM Director Server Plus Pack* CD from the CD-ROM drive.

Installing Software Distribution (Premium Edition)

You can install Software Distribution (Premium Edition) on management servers running Windows and Linux.

Installing Software Distribution on Windows

Complete the following steps to install Software Distribution on the management server:

1. Insert the *IBM Director Software Distribution (Premium Edition)* CD into the CD-ROM drive.
2. Start Windows Explorer, and open the `\swdist\server\windows\i386` directory located on the *IBM Director Software Distribution (Premium Edition)* CD.
3. Double-click **setup.exe**. The InstallShield wizard starts and the “Welcome to the InstallShield Wizard” window opens.
4. Click **Next**. A window that contains the license agreement opens.
5. Click **Yes** to accept the license agreement. The “Start Copying Files” window opens.
6. Click **Next**. The “InstallShield Wizard Complete” window opens.
7. Click **Finish**.
8. Remove the *IBM Director Software Distribution (Premium Edition)* CD from the CD-ROM drive.
9. Shut down and restart the management server.

Installing Software Distribution on Linux

Complete the following steps to install Software Distribution on the management server:

1. Stop IBM Director. From a command prompt, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstop
```

2. Insert the *IBM Director Software Distribution (Premium Edition)* CD into the CD-ROM drive.
3. If the CD does not automount, go to step 4. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

5. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/swdist/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

6. Type the following command and press Enter:

```
./install
```

7. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

8. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.

- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

9. Remove the CD from the CD-ROM drive.

Installing the Server Plus Pack extensions on managed systems

The *IBM Director Server Plus Pack* CD contains the Server Plus Pack extensions. They can be installed on managed systems either by using standard installation procedures or by using the IBM Director Software Distribution task.

For a list of Server Plus Pack extensions that can be installed on managed systems and the operating systems on which they are supported, see Table 3 on page 15.

Using standard installation procedures

You can use standard installation procedures to install the Server Plus Pack extensions on managed systems. This is useful for managed systems running operating systems that do not support software distribution, such as Novell NetWare.

Installing the Server Plus Pack extensions on Windows

Complete the following steps to install Server Plus Pack extensions on a managed system running Windows:

1. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive.
2. Using Windows Explorer, locate the setup.exe file for the Server Plus Pack extension you want to install. This file is located on the *IBM Director Server Plus Pack* CD in the `\extension\agent\windows\i386` directory, where *extension* is one of the following strings:
 - activpci
 - capmgt
 - swrejuv
 - sysavail
3. Double-click the setup.exe file. The IBM Director installation program starts.
4. Follow the instructions on the screen.

Installing the Server Plus Pack extensions on Red Hat Linux, SuSE Linux, and VMware ESX Server

Complete the following steps to install the Server Plus Pack extensions on a managed system running Linux:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstop
```

2. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive.
3. If the CD does not automount, go to step 4. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

5. Change to the directory where the RPM files are located. Type the following command and press Enter:

```
cd /mnt/cdrom/extension/agent/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive, and *extension* is one of the following strings:

- capmgt
- swrejuv
- sysavail

6. Install the Server Plus Pack extension. Type one of the following commands and press Enter:

For Capacity Manager	<code>rpm -U CapMgtAgent-4.10-1.i386.rpm</code>
-----------------------------	---

For Software Rejuvenation	<code>rpm -U SwRejuvAgent-4.10-1.i386.rpm</code>
----------------------------------	--

For System Availability	<code>rpm -U SysAvailAgent-4.10-1.i386.rpm</code>
--------------------------------	---

7. Repeat steps 5 and 6 until you have installed all the Service Plus Pack extensions that you want to install.

8. To start IBM Director Agent, type the following command and press Enter:
`/opt/IBM/director/bin/twgstart`
9. To unmount the CD-ROM drive, complete the following steps:
 - a. Type `cd /` and press Enter.
 - b. Type the following command and press Enter:
`umount /mnt/cdrom`

where `mnt/cdrom` is the mount point of the CD-ROM drive.

10. Remove the *IBM Director Server Plus Pack* CD from the CD-ROM drive.

Installing the Server Plus Pack extensions on NetWare

Notes:

1. To install Capacity Manager, you must log on to the server running NetWare from a Windows workstation running the NetWare Client for Windows.
2. The SYS volume must be mapped as a drive to the system running Windows.
3. You must have administrator or supervisor access on the NetWare server.

Complete the following steps to install Capacity Manager on NetWare:

1. Stop IBM Director Agent. From the server running NetWare, change to the console screen. Type the following command and press Enter:
`unload twgipc`
2. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive of the system running Windows. If the autorun window opens, close it.
3. Start Windows Explorer and open the `\capmgt\agent\netware` directory.
4. Double-click **setup.exe**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
5. Click **Next**. The “Choose Destination Location” window opens.

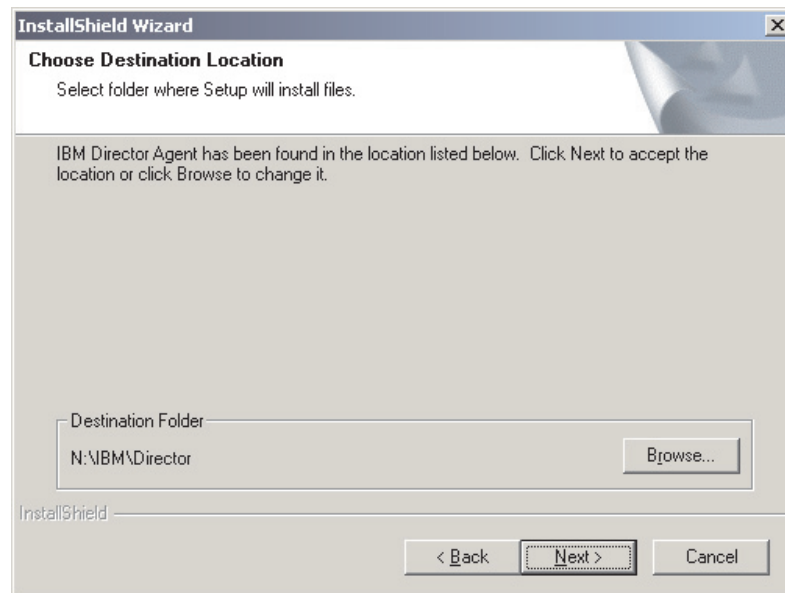


Figure 69. Installing Capacity Manager on NetWare: “Choose Destination Location” window

6. Click **Next**. The “Start Copying Files” window opens.

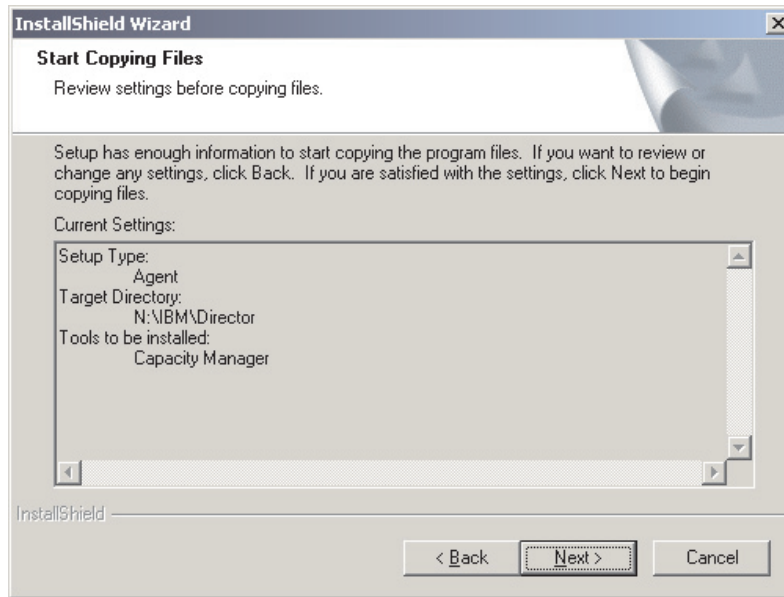


Figure 70. Installing Capacity Manager on NetWare: “Start Copying Files” window

7. Click **Next**. When the installation is completed, the “InstallShield Wizard Complete” window opens.
8. Click **Finish**.
9. Remove the *IBM Director Server Plus Pack* CD from the CD-ROM drive.
10. On the server running NetWare, change to the console screen.
11. To start IBM Director Agent, type the following command and press Enter:

```
load twgipc
```

Using the IBM Director Software Distribution task (Windows and Linux only)

The *IBM Director Server Plus Pack* CD contains XML files that describe the Server Plus Pack extensions. The following files are located at the root of the CD:

- pluspack_all.xml
- pluspack_linux.xml
- pluspack_windows.xml

Each XML file describes a group of a software packages. For example, the pluspack_all.xml file describes *all* the Server Plus Pack software packages, and the pluspack_linux.xml file describes the Server Plus Pack packages for managed systems running Linux.

When you import the XML files into the IBM Director, the Director Update Assistant creates software packages. Then, you can use the IBM Director Software Distribution task to distribute the packages to the managed systems.

The names of the non-English-language XML files are similar to those listed, with the addition of language codes. For example, the package that describes all the German-language Server Plus Pack software packages is named pluspack_all_de.xml.

In addition, XML files that describe the individual Server Plus Pack extensions are located in the applicable directories on the *IBM Director Server Plus Pack* CD.

Creating a software package

You can create software packages that contain the entire Server Plus Pack, packages that contain a single component, or packages that contain several Server Plus Pack components. Complete the following steps to create a software package:

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

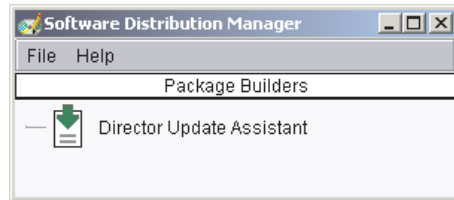


Figure 71. Creating a software package: “Software Distribution Manager” window (Standard Edition)

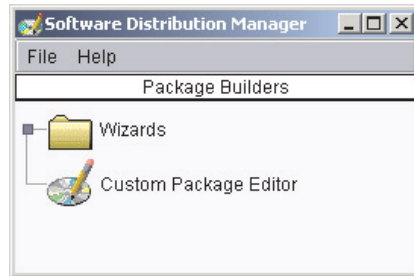


Figure 72. Creating a software package: “Software Distribution Manager” window (Premium Edition)

3. If you have not installed IBM Director 4.1 Software Distribution (Premium Edition), go to step 4. Otherwise, expand the **Wizards** tree.
4. Double-click **Director Update Assistant**. The “Director Update Assistant” window opens.

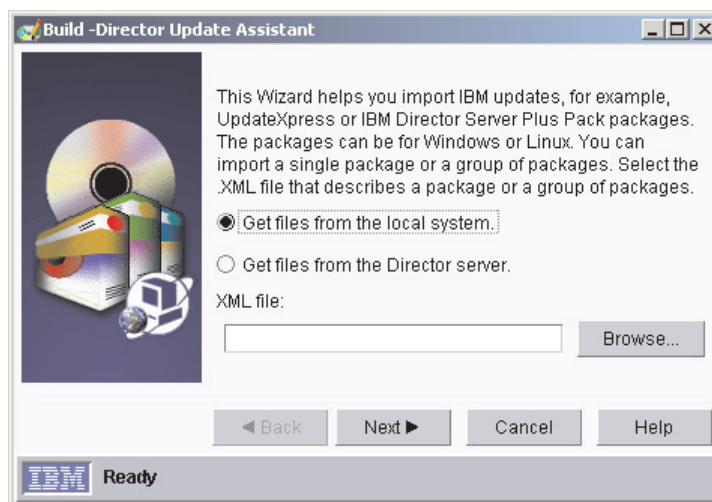


Figure 73. Creating a software package: “Director Update Assistant” window

5. By default, **Get files from the local system** is selected. If you want to get files from the management server, click **Get files from the Director server**.
6. To select a file, click **Browse**. The “IBM Update Package/Root Directory Location” window opens.

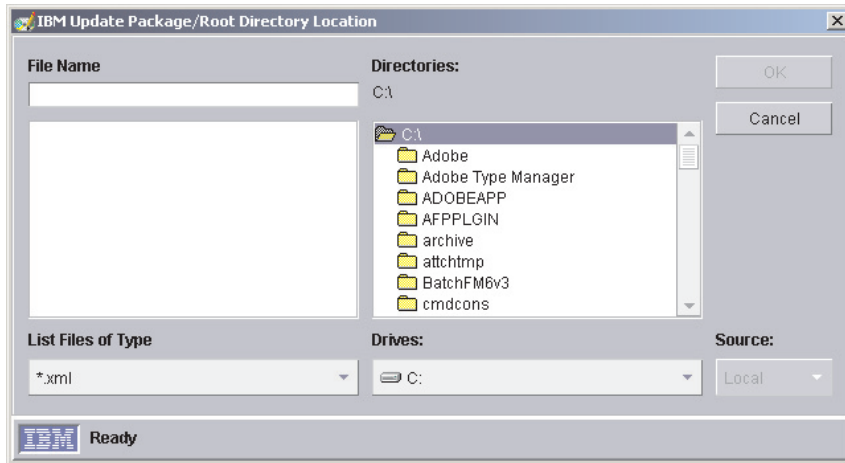


Figure 74. Creating a software package: “IBM Update Package/Root Directory Location” window

7. Locate the XML file and click it. The name of the XML file is displayed in the **File Name** field.

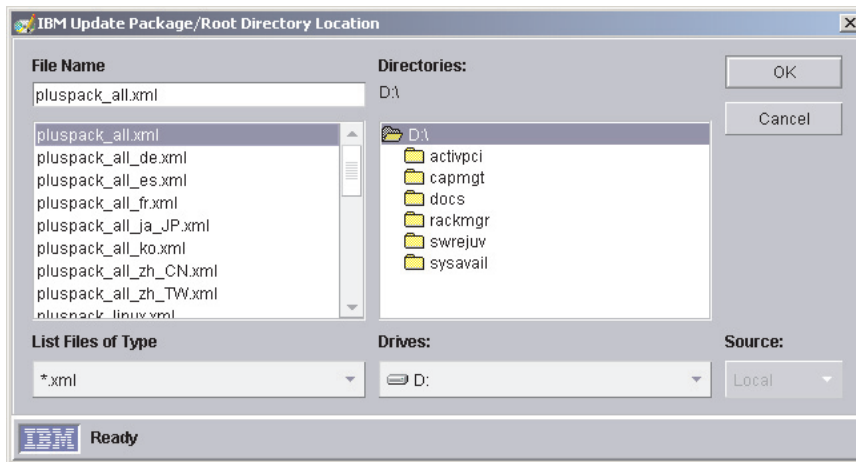


Figure 75. Creating a software package: “IBM Update Package/Root Directory Location” window

8. Click **OK**. The “Director Update Assistant” window reopens.

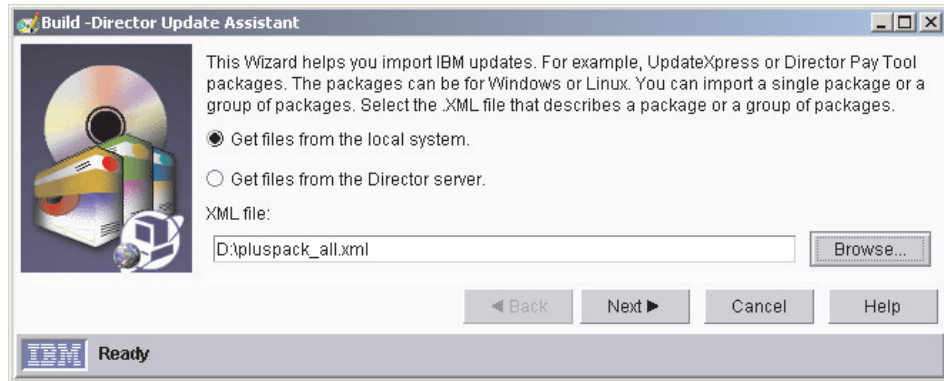


Figure 76. Creating a software package: “Director Update Assistant” window

9. Click **Next**. The second “Director Update Assistant” window opens.

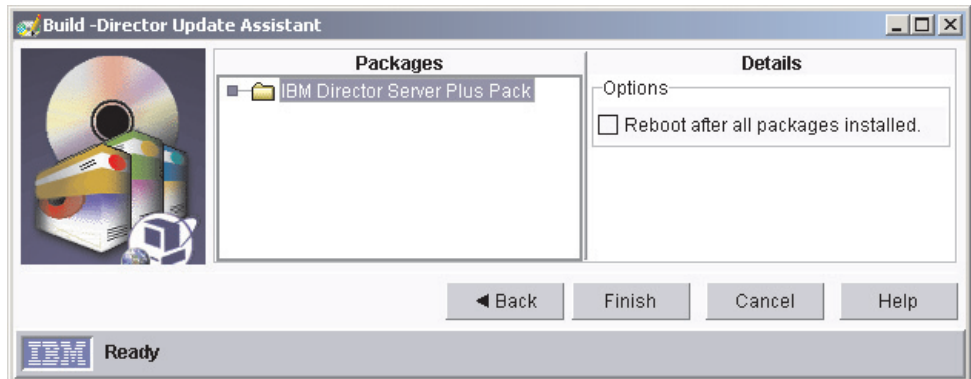


Figure 77. Creating software packages: “Director Update Assistant” window

10. If you selected an XML file that contains more than one update, expand the tree in the Packages pane. A green check mark (✓) is displayed beside the packages selected for installation; a red X is displayed beside the update packages that are not selected. To select an update package, double-click the package name.

It is not necessary to select the **Reboot after all packages installed** check box. Installing the Server Plus Pack extension forces a restart of IBM Director Agent, if needed.

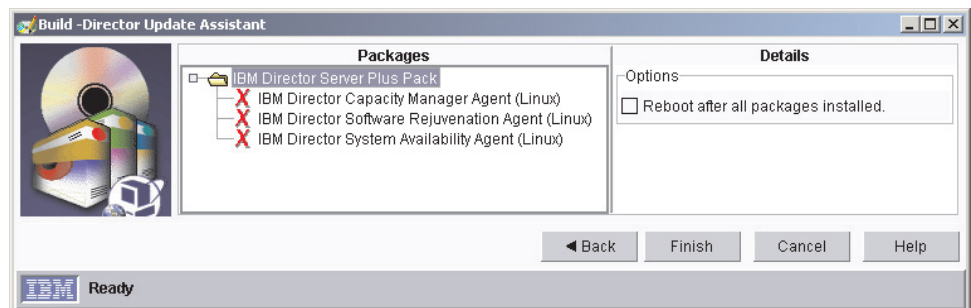


Figure 78. Creating software packages: “Director Update Assistant” window

- Click **Finish**. As the packages are processed, a status message is displayed at the bottom of the window. When the processing is completed, the software packages are displayed in the Tasks pane of IBM Director Console.

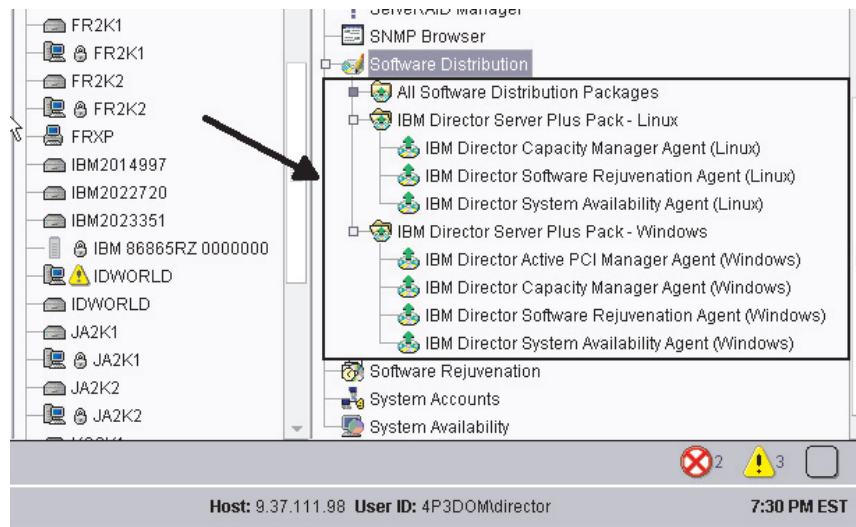


Figure 79. All Software Distribution Packages: IBM Director Server Plus Pack

Installing a software package

Complete the following steps to install a software package:

- Start IBM Director Console.
- In the Tasks pane, expand the **Software Distribution** task.
- Click the software package that you want to distribute. Then, drag it into the Group Contents pane and drop it onto the icon displayed for the system on which you want to install the software package. A window opens.

Note: To distribute software to several systems at once, you can drag the software package into the Groups pane and drop it onto the icon for the group. Alternatively, you can select multiple managed systems in the Group Contents pane.

- When prompted Do you wish to create a scheduled job for this task or execute immediately?, click **Schedule** or **Execute Now**. If you click **Execute Now**, the software package is distributed immediately. If you click **Schedule**, the “New Scheduled Job” window opens.

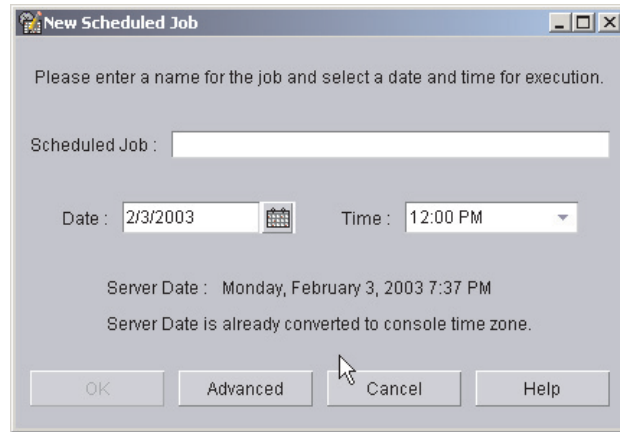


Figure 80. Scheduling the installation of a software package: “New Scheduled Job” window

5. Schedule the job:
 - a. In the **Scheduled Job** field, type a unique name for the job. This name is displayed in the Jobs pane of the Scheduler window.
 - b. In the **Date** field, type the day you want the software package to be installed (MM/DD/YYYY format).
 - c. In the **Time** field, type the time you want the software package to be installed.

For more information about the Scheduler task, see the *IBM Director 4.11 Systems Management Guide*.

6. Click **OK**. The “Save Job Confirmation” window opens.
7. Click **OK**.

After installing Active PCI Manager, be sure to restart (reboot) the managed system. If you do not restart the managed system, the Slot Manager subtask might fail.

Part 4. Upgrading IBM Director

Chapter 10. Upgrading IBM Director Server

This chapter contains instructions for upgrading IBM Director Server. When you upgrade IBM Director Server, IBM Director Console and IBM Director Agent are upgraded automatically.

You can upgrade IBM Director Server on servers running the following operating systems:

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

Upgrading IBM Director Server on Windows

Notes:

1. IBM Director is certified to run with the Oracle *9i* JDBC Thin Driver, version 9.0.1 for use with JDK 1.2 and 1.3 *only*. During the upgrade to IBM Director Server 4.1, the Oracle JDBC driver built into IBM Director 3.x will be removed; if the Oracle *9i* JDBC driver is not installed, IBM Director will not start.
2. Earlier versions of Active PCI Manager are not compatible with IBM Director. Before you install IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
3. All user-defined temperature thresholds are lost when upgrading from IBM Director Server 3.x to IBM Director Server 4.11. To avoid losing threshold settings, make a note of the temperature thresholds and then reset the thresholds after upgrading to IBM Director Server 4.11.

Complete the following steps to upgrade IBM Director Server on Windows:

1. If you use Oracle Server as the IBM Director database application, verify that you have installed the Oracle *9i* JDBC Thin Driver, version 9.0.1. See “Oracle Server” on page 32 for information about downloading the JDBC driver and setting the CLASSPATH statement.
2. Stop IBM Director Server. From a command prompt, type the following command and press Enter:

```
net stop twgipc
```
3. Close all applications, including any command-prompt windows.
4. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
5. If the installation program starts automatically and the InstallShield wizard starts, go to step 7. Otherwise, click **Start** → **Run**.
6. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

7. Click **Install IBM Director**. The “IBM Director Installation” window opens.
8. Click **IBM Director Server installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.

If you are upgrading from IBM Director 3.x, the window is updated with the following message: IBM Director 3.x has been detected. The InstallShield Wizard might be slower than usual during the upgrade of the installation files.

9. Click **Next**. The “License Agreement” window opens.
10. Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.

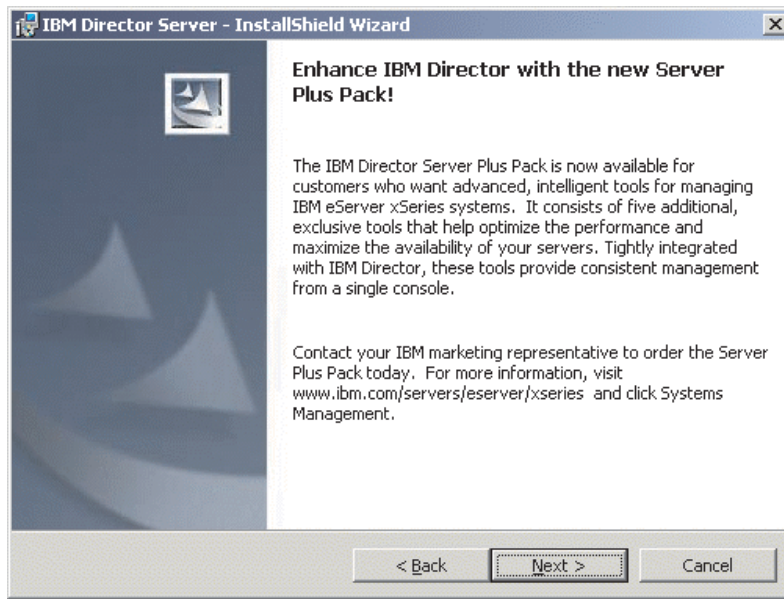


Figure 81. Upgrading IBM Director Server on Windows: “Server Plus Pack” window

11. Click **Next**. The “Feature and installation directory selection” window opens.

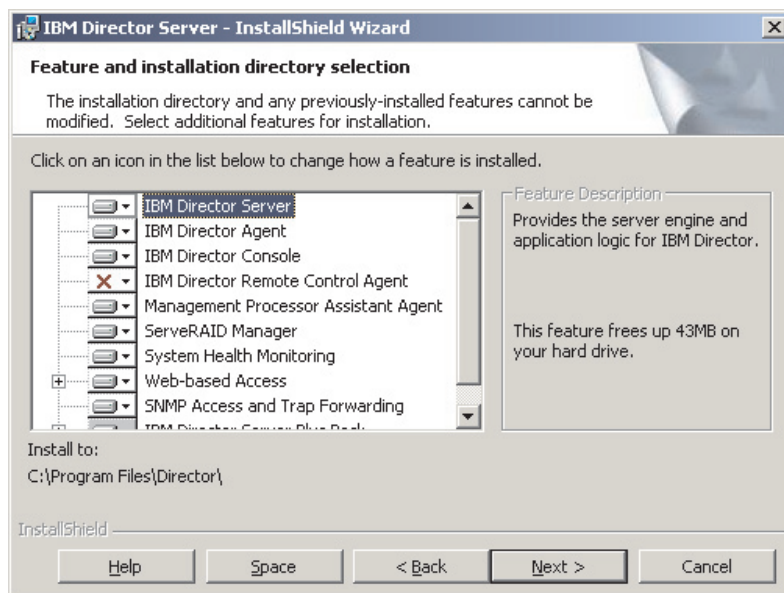




Figure 82. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window

IBM Director Server, IBM Director Agent, IBM Director Console, and any previously-installed features are selected automatically for installation; a hard disk drive icon  is displayed to the left of each component.

 is displayed to the left of the uninstalled features. If they were not installed previously, you can install the following features:

IBM Director Remote Control Agent

Enables a system administrator to perform remote desktop functions on a managed system.

Management Processor Assistant Agent

Enables communication with service processors in IBM xSeries and Netfinity servers.

ServeRAID Manager

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities.

System Health Monitoring


Monitors the status of hardware components, produces and relays hardware alerts, and facilitates upward integration.

Web-based Access

Enables a system administrator to access the managed-system data through a Web browser or the Microsoft Management Console (MMC).

SNMP Access and Trap Forwarding

Enables access to managed-system data and alerts through SNMP.

12. To select a feature, click  to the left of the feature name. A menu opens.

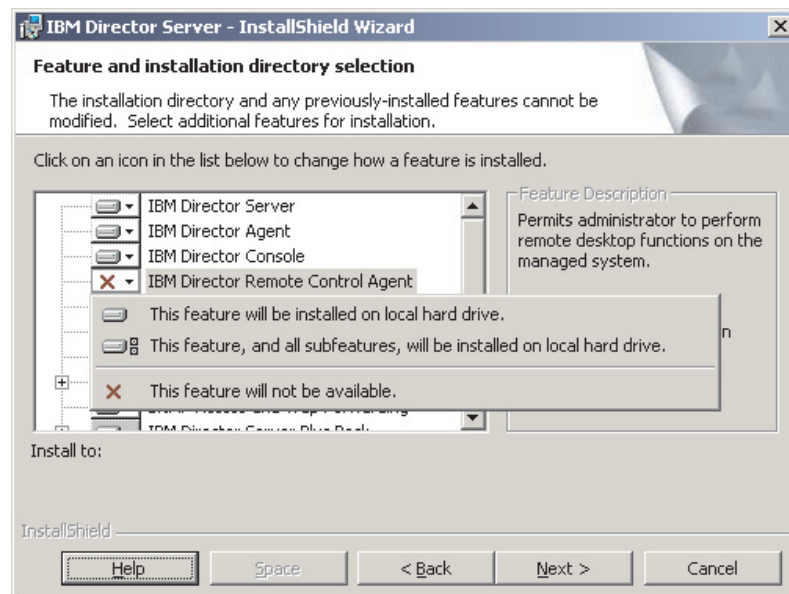


Figure 83. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window

To select the feature, click **This feature will be installed on local hard drive** or **This feature, and all its subfeatures, will be installed on local hard drive**.

13. Select the Server Plus Pack extensions that you want to install. Any previously-installed Server Plus Pack extensions are selected automatically for installation. If they were not installed previously, you can select the following extensions:

Capacity Manager

Tracks system resource utilization, identifies bottlenecks, and provides performance information.

Rack Manager

Manages IBM servers, storage devices, and other components located in an IBM enclosure.

Active PCI Manager

Manages PCI and PCI-X adapters in managed systems.

Software Rejuvenation

Schedules restarts of managed systems.

System Availability

Determines availability of managed systems and provides statistical data.

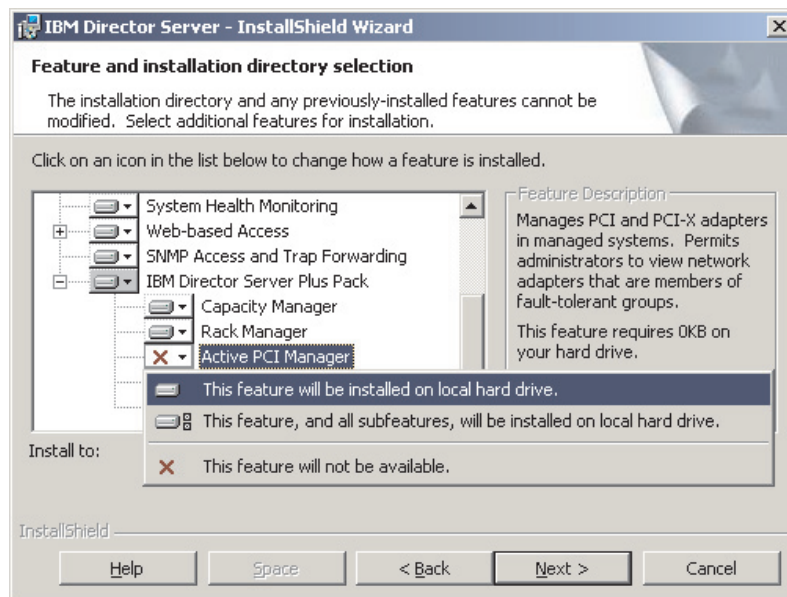


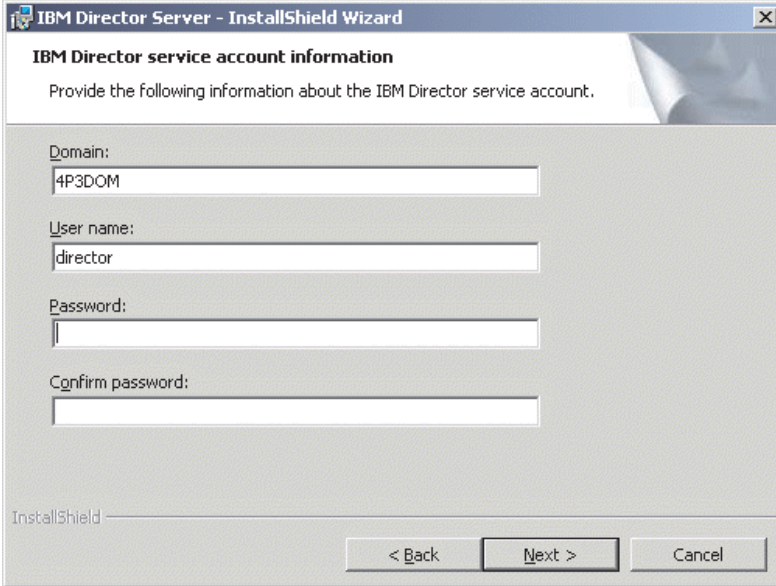
Figure 84. Upgrading IBM Director Server on Windows: Installing the Server Plus Pack

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all its subfeatures, will be installed on local hard drive**. Otherwise, select the Server Plus Pack extensions individually.

Notes:

- a. Rack Manager will not function until the Rack Manager component located on the *IBM Director Server Plus Pack* CD is installed on the management server.
- b. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.

14. Click **Next**. The “IBM Director service account information” window opens. (For more information about the IBM Director service account, see “IBM Director security” on page 33.)



The screenshot shows a Windows dialog box titled "IBM Director Server - InstallShield Wizard". The main heading is "IBM Director service account information". Below the heading is the instruction: "Provide the following information about the IBM Director service account." There are four text input fields: "Domain:" with the value "4P3DOM", "User name:" with the value "director", "Password:" which is empty, and "Confirm password:" which is empty. At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted), and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

Figure 85. Upgrading IBM Director Server on Windows: “IBM Director service account information” window

15. The **User Name**, **Domain**, **Password**, and **Confirm password** fields are filled in automatically with the information for the service account used for the existing IBM Director Server installation.

Note: Do not change the service account information. If you do, the installation will fail.

16. Click **Next**. The “Encryption settings” window opens.

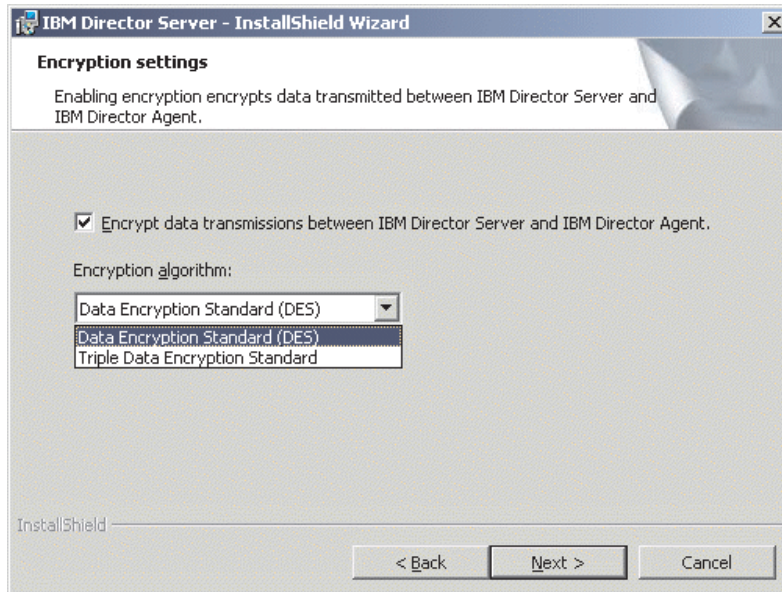


Figure 86. Installing IBM Director Server on Windows: “Encryption settings” window

17. To encrypt data transmitted between IBM Director Server and IBM Director Agent, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box; then, select the encryption algorithm.
18. Click **Next**. The “Software-distribution settings” window opens.

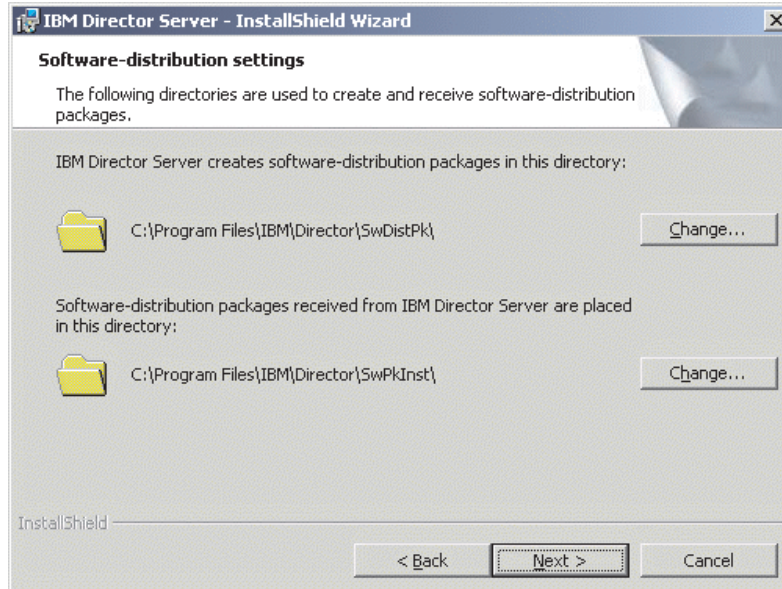


Figure 87. Upgrading IBM Director Server on Windows: “Software-distribution settings” window

19. Click **Next**. If you did not select to install the Web-based Access feature, the “Ready to Install the Program” window opens; go to step 21 on page 141. Otherwise, the “Web-based Access information” window opens.

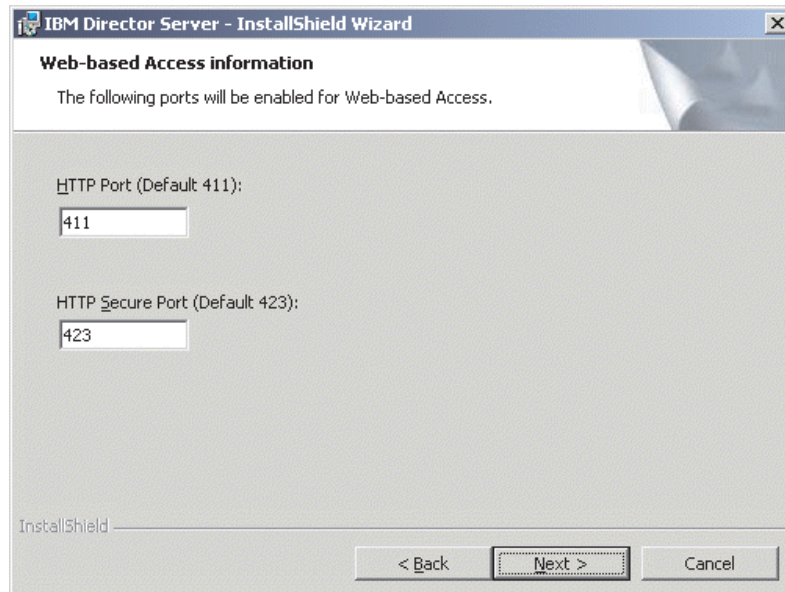


Figure 88. Upgrading IBM Director Server on Windows: “Web-based Access information” window

20. Change the default HTTP ports (if necessary); then, click **Next**. The “Ready to Install the Program” window opens.
21. Click **Install**. The “Installing IBM Director Server” window opens. The progress of the installation is displayed in the **Status** field. When the installation is completed, the “Network driver configuration” window opens.

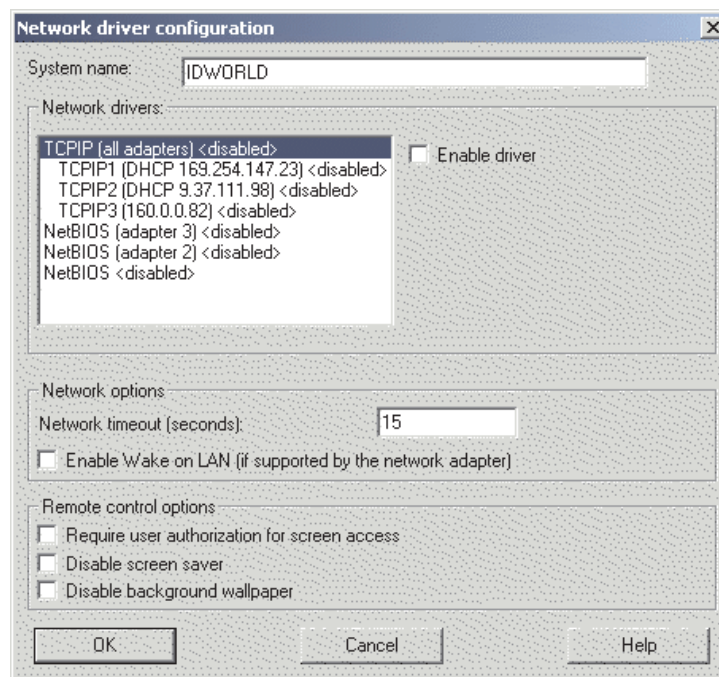


Figure 89. Upgrading IBM Director Server on Windows: “Network driver configuration” window

22. In the **System name** field, type the name that you want displayed in IBM Director Console. By default, this is the NetBIOS name of the management server.
23. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent:
 - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

Note: If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Server will receive data packets addressed to the individual adapter *only*.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
- c. Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN feature.

Note: To determine whether your server supports the Wake on LAN feature, see your server documentation.

24. If you selected to install the IBM Director Remote Control Agent, the following options are available:

Require user authorization for system access

Select this check box to request authorization from the local user before controlling a managed system remotely.

Disable screen saver

Select this check box to disable the screen saver on the managed system being controlled remotely.

Disable background wallpaper

Select this check box to disable desktop wallpaper on the managed system being controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

25. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
26. Click **Finish**. A window opens, asking you if you want to restart the server.
27. Remove the *IBM Director 4.11* CD from the CD-ROM drive.
28. Click **Yes** to restart the server.

For instructions on how to install IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 121 and “Installing Software Distribution (Premium Edition)” on page 122.

Upgrading IBM Director Server on Linux

When you upgrade IBM Director Server, IBM Director automatically upgrades all previously-installed IBM Director features and extensions. You can also choose to install additional features and extensions.

Important: (PostgreSQL only) If you modified the TWGDatabase.TWGExt file to point to a PostgreSQL JDBC driver, you must create a symbolic link before upgrading to IBM Director Server. Complete the following steps to create a symbolic link:

1. From a command prompt, type the following command and press Enter:

```
ln -s realname path/postgresql.jar
```

where *realname* is the fully qualified name of the PostgreSQL JDBC driver, for example, /opt/postgres/lib/jdbc7.1-1.2.jar, and *path* is the path of the symbolic link, for example, /opt/postgres/lib/.

2. Update the /etc/TWGserver/setup_env file. Change the classpath statement to read as follows:

```
CLASSPATH=path/postgresql.jar  
export CLASSPATH
```

where *path* is the path of the symbolic link.

Complete the following steps to upgrade IBM Director Server on Linux:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3 on page 51. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. If you want to customize the installation, go to step 6 on page 51. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 18 on page 53.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the dirinstall script. This file is fully commented.

You can specify the location of the Red Hat Package Manager (RPM) files, select previously-uninstalled IBM Director extensions and features that you want to install, and select log file options.

8. Save the modified installation script.

9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```

11. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

12. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.

- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

13. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

For instructions on how to install IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 121 and “Installing Software Distribution (Premium Edition)” on page 122.

Chapter 11. Upgrading IBM Director Console

This chapter contains instructions for upgrading IBM Director Console. You can upgrade IBM Director Console on systems running the following operating systems:

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

Upgrading IBM Director Console on Windows

This section provides instructions for upgrading IBM Director Console using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

Notes:

1. Earlier versions of Active PCI Manager are not compatible with IBM Director. Before you install IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
2. If you have both IBM Director Console and IBM Director Agent installed on a system, you *must* upgrade both components. After you upgrade IBM Director Console, upgrade IBM Director Agent. See “Upgrading IBM Director Agent on Windows” on page 151.

Upgrading IBM Director Console using the InstallShield wizard

Complete the following steps to upgrade IBM Director Console on Windows:

1. If IBM Director Agent is installed, from a command prompt, type the following command and press Enter:

```
net stop twgipc
```
2. Close all open applications, including command-prompt sessions.
3. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
4. If the installation program starts automatically and the InstallShield wizard starts, go to step 6. Otherwise, click **Start** → **Run**.
5. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

6. Click **Install IBM Director**. The “IBM Director Installation” window opens.
7. Click **IBM Director Console installation**. The “Welcome to the InstallShield Wizard” window opens.

If you are upgrading from IBM Director 3.x, the window is updated with the following message: IBM Director 3.x has been detected. The InstallShield Wizard might be slower than usual during the upgrade of the installation files.

8. Click **Next**. The “License Agreement” window opens.

- Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.

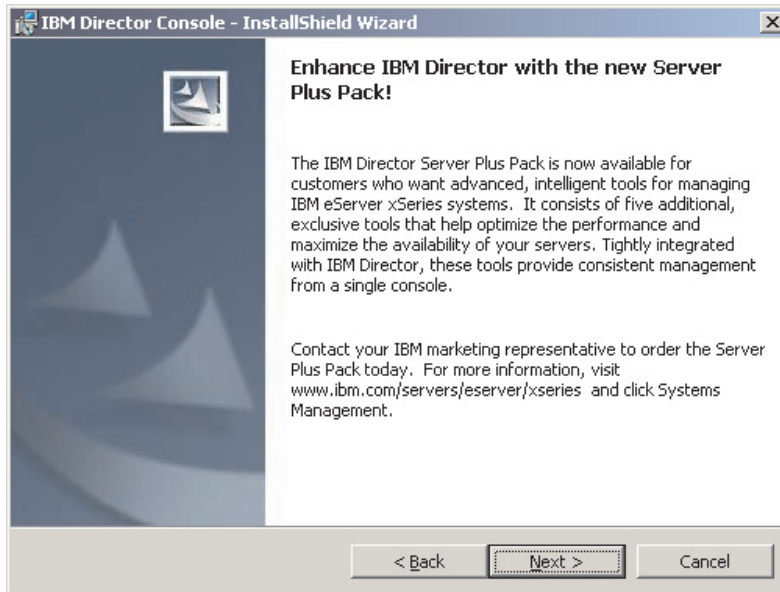


Figure 90. Upgrading IBM Director Console: “Server Plus Pack” window

- Click **Next**. The “Feature and installation directory selection” window opens.

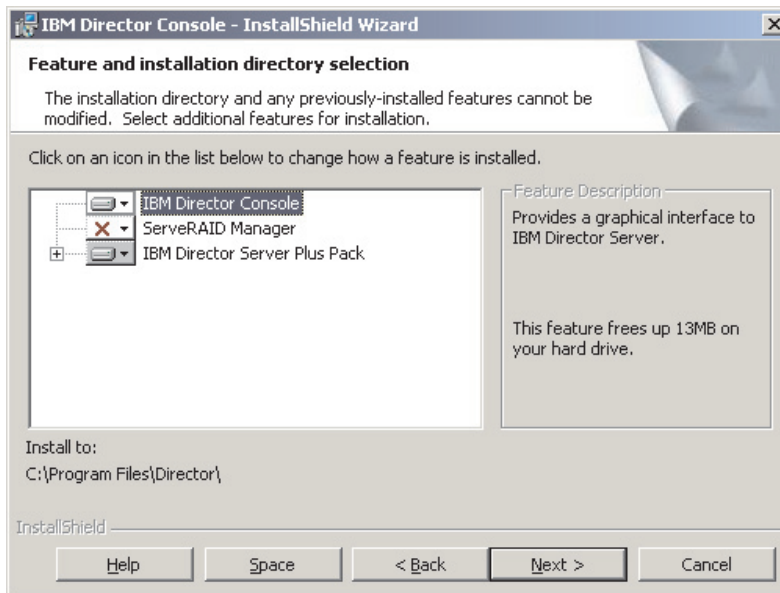




Figure 91. Upgrading IBM Director Console: “Feature and destination directory selection” window

IBM Director Console and any previously-installed features are selected automatically for installation; a hard disk drive icon  is displayed to the left of the component.

 is displayed to the left of the uninstalled features. If it was not installed previously, you can install ServeRAID Manager, a feature that manages and monitors IBM ServeRAID adapters.

11. To select ServeRAID Manager, click  to the left of the feature name. A menu opens. Click **This feature will be installed on local hard drive.**

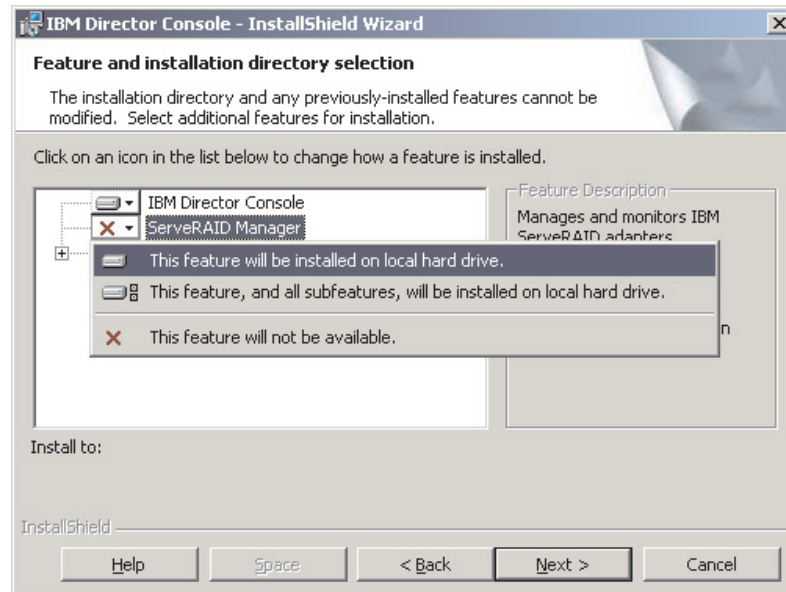


Figure 92. Upgrading IBM Director Console: Installing ServeRAID Manager

12. Select the Server Plus Pack extensions that you want to install:

Capacity Manager

Tracks system resource utilization, identifies bottlenecks, and provides performance information.

Rack Manager

Manages IBM servers, storage devices, and other components located in an IBM enclosure.

Active PCI Manager

Manages PCI and PCI-X adapters in managed systems.

Software Rejuvenation

Schedules restarts of managed systems.

System Availability

Determines availability of managed systems and provides statistical data.

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all its subfeatures, will be installed on local hard drive.** Otherwise, select the Server Plus Pack extensions individually.

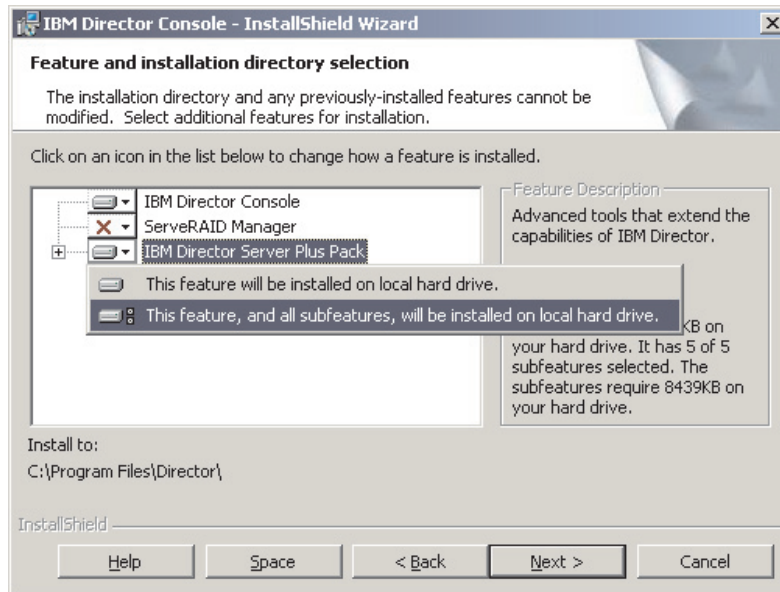


Figure 93. Upgrading IBM Director Console: Installing the Server Plus Pack

Notes:

- a. Rack Manager will not function until the Rack Manager component, located on the *IBM Director Server Plus Pack* CD, is installed on the management server.
 - b. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.
13. Click **Next**. The “Ready to Install the Program” window opens.
 14. Click **Install**. The “Installing IBM Director Console” window opens. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
 15. Click **Finish**. A window opens, asking if you want to restart the system.
 16. Remove the *IBM Director 4.11* CD from the CD-ROM drive.
 17. Click **Yes** to restart the system.

Performing an unattended upgrade of IBM Director Console

You can perform an unattended upgrade of IBM Director Console using a response file, which provides answers to the questions posed by the InstallShield wizard.

Complete the following steps to upgrade IBM Director Console on Windows:

1. If IBM Director Agent is installed, from a command prompt, type the following command and press Enter:

```
net stop twgipc
```
2. Close all open applications, including command-prompt sessions.
3. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
4. Copy the `dircon.rsp` file to a local directory. This file is located in the `director\console\windows\i386` directory on the *IBM Director 4.11* CD.
5. From Windows Explorer, right-click the copy of the `dircon.rsp` file and then click **Properties**. The “`dircon.rsp` Properties” window opens. Clear the **Read-Only** check box and click **OK**.

6. Open the copy of the `dircon.rsp` file in an ASCII text editor.
7. Modify and save the `dircon.rsp` file. This file follows the Windows INI file format and is fully commented.

Note: Windows automatically detects and upgrades the IBM Director features that were part of the existing IBM Director installation. However, you can select features that were not installed previously.

8. Change to the directory that contains the IBM Director Console installation file (`ibmsetup.exe`). This file is located in the `director\console\windows\i386` directory on the *IBM Director 4.11* CD.
9. From the command prompt, type the following command and press Enter:
`ibmsetup.exe installationtype rsp="responsefile.rsp"`

where:

- `installationtype` is one of the following commands:
 - UNATTENDED shows the progress of the installation but does not require any user input.
 - SILENT suppresses all output to the screen during installation.
 - `responsefile.rsp` is the path and name of the response file that you created in step 7.
10. When the installation is completed, remove the *IBM Director 4.11* CD from the CD-ROM drive.

Upgrading IBM Director Console on Linux

This section contains instructions for upgrading IBM Director Console using the *IBM Director 4.11* CD. It also contains instructions for upgrading IBM Director Console and IBM Director Agent simultaneously.

Note: If the management console also has IBM Director Agent installed, you must perform the upgrade using the instructions outlined in “Upgrading IBM Director Console and IBM Director Agent simultaneously” on page 150.

Upgrading IBM Director Console

When you upgrade IBM Director Console, IBM Director automatically upgrades all previously-installed IBM Director features and extensions. You also can choose to install additional features and extensions.

Complete the following steps to upgrade IBM Director Console on Linux:

1. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where `mnt/cdrom` is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where `dev/cdrom` is the specific device file for the CD-ROM block device and `mnt/cdrom` is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/console/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. Copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

6. Open an ASCII text editor and modify the “User configuration” section of the *dirinstall* script. This file is fully commented.

You can specify the location of the RPM files, select previously-uninstalled IBM Director extensions and features that you want to install, and select log file options.

7. Save the modified installation script.

8. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

9. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.

- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

10. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

Upgrading IBM Director Console and IBM Director Agent simultaneously

When you install the IBM Director Agent and IBM Director Console for Linux patch, all previously-installed IBM Director features and extensions are upgraded.

Complete the following steps to upgrade IBM Director Console and IBM Director Agent at the same time:

1. Download `IBMDirectorAgentConsoleLinuxPatch4.11-1.tar.gz` from the IBM Systems Management Software: Download/Electronic Support page at http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html.

2. Gunzip and untar the package. It contains the following file:
`IBMDirectorAgentConsolePatch4.11-1.sh`.

3. From a command prompt, type the following command and press Enter:

```
./IBMDirectorAgentConsolePatch4.11-1.sh -x directory
```

where `-x directory` is an optional parameter that saves the RPM files, and *directory* is the fully qualified file name of the directory to which the RPM files are written.

Chapter 12. Upgrading IBM Director Agent

This chapter contains instructions for upgrading IBM Director Agent using either standard installation procedures or the IBM Director Software Distribution task.

You can upgrade IBM Director Agent on systems running the following operating systems:

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

IBM Director Agent is no longer supported on the following operating systems:

- Windows 95, 98, and Millennium Edition (Me)
- NetWare, version 5.x
- OS/2 WARP Server for e-business
- Caldera Linux, versions 2.3.1 and 3.1
- Turbolinux, versions 6.0.5 and 6.5
- SCO UnixWare, version 7.1.1

If you want to manage systems running these operating systems, do not upgrade from IBM Director Agent 3.x. IBM Director 4.11 can manage systems running IBM Director Agent 3.x.

Upgrading IBM Director Agent using standard installation procedures

This section contains information about upgrading IBM Director Agent using standard installation procedures.

Upgrading IBM Director Agent on Windows

This section provides information about installation prerequisites and instructions for upgrading IBM Director Agent using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

Preparing to upgrade IBM Director Agent on Windows

Before you install IBM Director Agent, make sure that you have uninstalled any incompatible files and installed any necessary prerequisites and device drivers.

Consider the following information:

1. Earlier versions of Active PCI Manager are not compatible with IBM Director. Before you upgrade IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
2. If you have both IBM Director Agent and IBM Director Console installed on a system, you *must* upgrade both components. If you have not done so already, upgrade to IBM Director Console 4.1 before upgrading to IBM Director Agent 4.1. See Chapter 11, “Upgrading IBM Director Console”, on page 145.
3. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

Upgrading IBM Director Agent using the InstallShield wizard

Note: (Windows XP only) During the installation, message windows might open behind the installation window. These message windows stop the installation process. To check for hidden message windows, press Alt+Tab to cycle through the active windows.

Complete the following steps to upgrade IBM Director Agent on Windows:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
net stop twgipc
```
2. Close all applications, including any command-prompt sessions.
3. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
4. If the installation program starts automatically and the InstallShield wizard starts, go to step 6. Otherwise, click **Start** → **Run**.
5. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

6. Click **Install IBM Director**. The “IBM Director Installation” window opens.
7. Click **IBM Director Agent installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.

If you are upgrading from IBM Director 3.x, the window is updated with the following message: IBM Director 3.x has been detected. The InstallShield Wizard might be slower than usual during the upgrade of the installation files.

8. Click **Next**. The “License Agreement” window opens.
9. Click **I accept the terms in the license agreement** and click **Next**. The “Feature and installation directory selection” window opens.

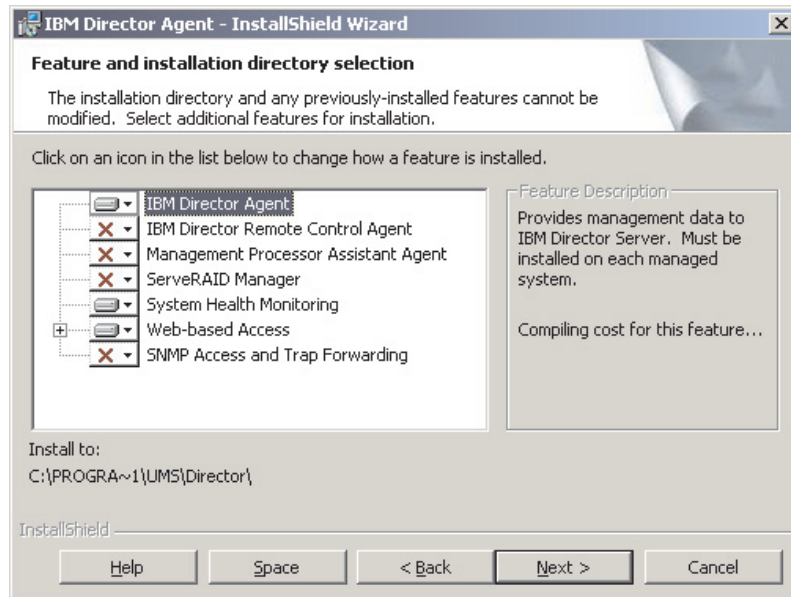




Figure 94. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window

IBM Director Agent and any previously-installed features are selected automatically for installation; a hard disk drive icon  is displayed to the left of the component.

 is displayed to the left of uninstalled features. If they were not installed previously, you can select to install the following features:

IBM Director Remote Control Agent

Enables a system administrator to perform remote desktop functions on a managed system.

Management Processor Assistant Agent

Enables communication with service processors in IBM xSeries and Netfinity servers.

ServeRAID Manager

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities.

System Health Monitoring


Monitors the status of hardware components, produces and relays hardware alerts, and facilitates upward integration.

Web-based Access

Enables system administrator to access managed-system data through a Web browser or the Microsoft Management Console (MMC).

SNMP Access and Trap Forwarding

Enables access to managed-system data and alerts through SNMP.

- To select a feature, click  to the left of the feature name. A menu opens.

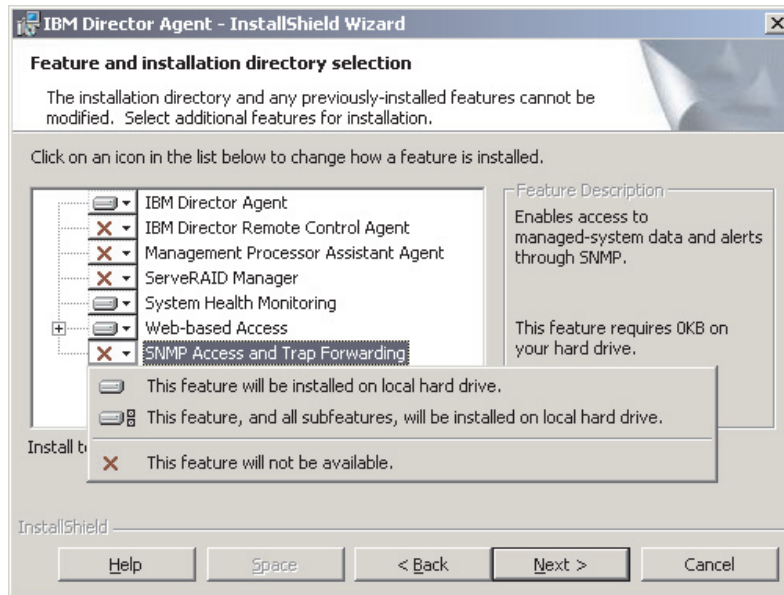


Figure 95. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window

To install the feature, click **This feature will be installed on local hard drive** or **This feature, and all its subfeatures, will be installed on local hard drive**.

11. When you have selected the features you want to install, click **Next**. The “Security settings” window opens.

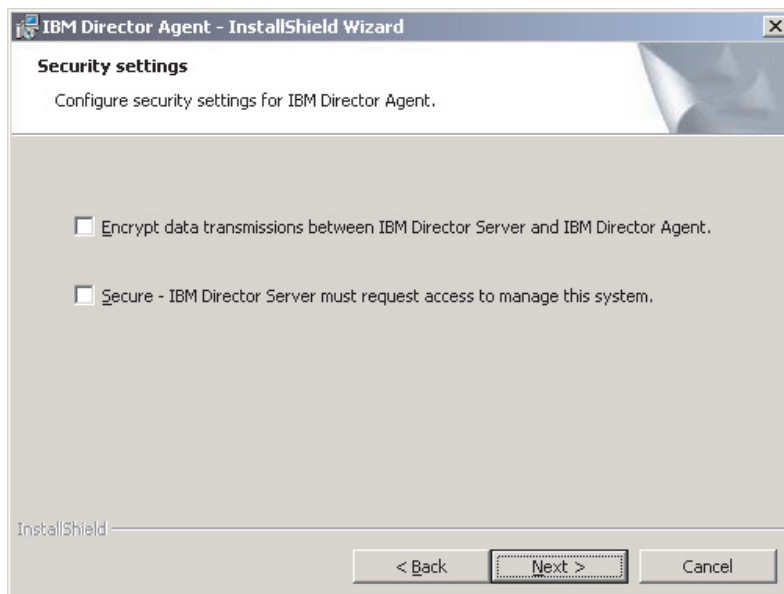


Figure 96. Upgrading IBM Director Agent on Windows: “Security settings” window

12. If you do not want to encrypt transmissions between IBM Director Server and IBM Director Agent, go to step 13 on page 155. Otherwise, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box.

- Note:** If encryption is enabled, the following conditions apply:
- The managed system is automatically secured, and the **Secure – IBM Director Server must request access to manage this system** check box is unavailable.
 - Only management servers with encryption enabled are able to communicate with the managed system.
- To set IBM Director Agent to the secured state, select the **Secure – IBM Director Server must request access to manage this system** check box. This ensures that only authorized instances of IBM Director Server can manage this system.
 - Click **Next**. The “Software Distribution settings” window opens.

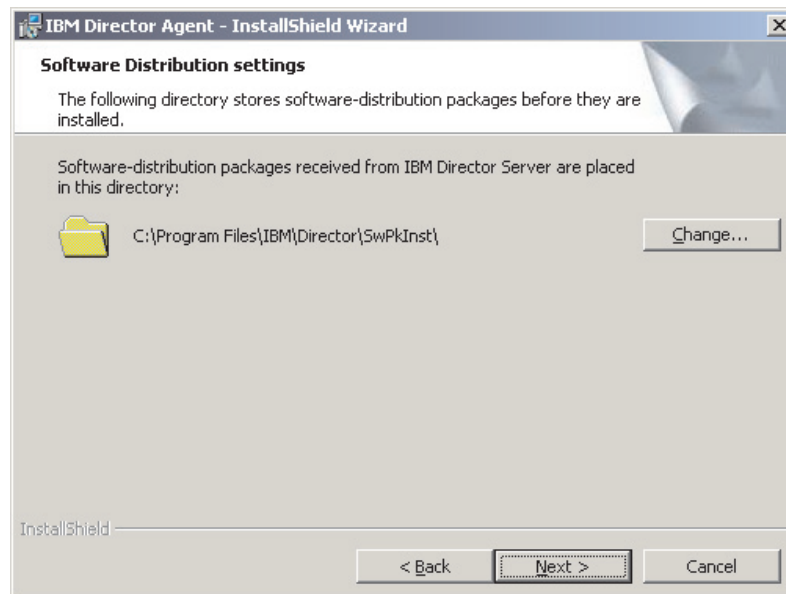


Figure 97. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window

- To select an alternative location where software-distribution packages are stored before being applied to IBM Director Agent, click **Change** and select another directory.
- Click **Next**. If you did not select to install the Web-based Access feature, go to step 17 on page 156. Otherwise, the “Web-based Access information” window opens.

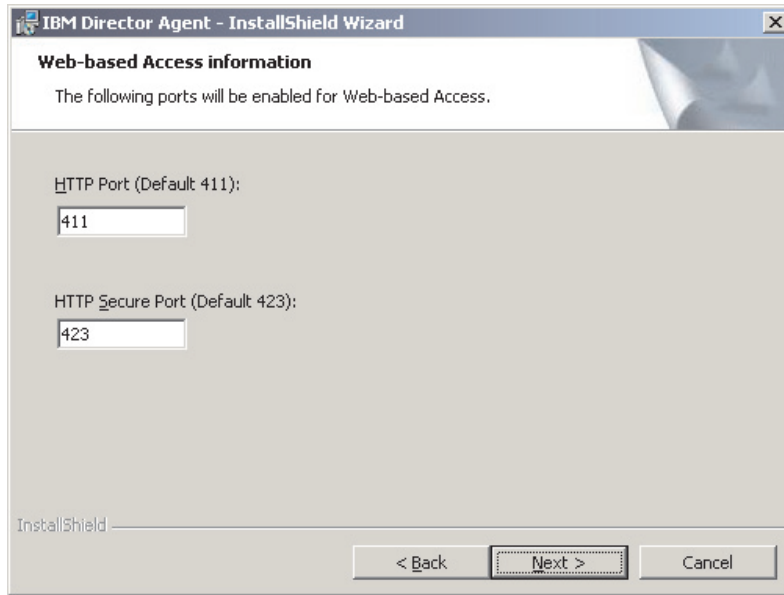


Figure 98. Upgrading IBM Director Agent on Windows: “Web-based Access information” window

16. Change the default HTTP port numbers (if necessary), and click **Next**. The “Ready to Install the Program window” opens.
17. Click **Install**. The “Installing IBM Director Agent” window opens. The status bar indicates the progress of the installation. When the installation is completed, the “Network driver configuration” window opens.

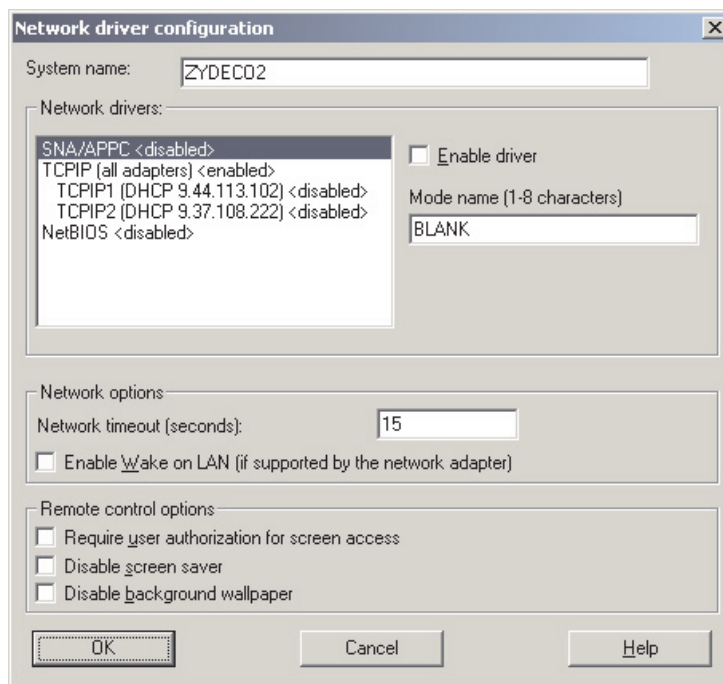


Figure 99. Upgrading IBM Director Agent on Windows: “Network driver configuration” window

18. In the **System Name** field, type the name that you want displayed in IBM Director Console. By default, this is the NetBIOS name of the managed system.
19. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
 - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

Note: If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive data packets addressed to the individual adapter *only*.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
 - c. Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN feature.
- Note:** To determine whether your server supports the Wake on LAN feature, see your server documentation.
20. If you selected to install the IBM Director Remote Control Agent, the following options are available:

Require User Authorization for System Access

Select this check box to request authorization from the local user before accessing a managed system remotely.

Disable Screen Saver

Select this check box to disable the screen saver on the managed system being controlled remotely.

Disable Background Wallpaper

Select this check box to disable desktop wallpaper on the managed system being controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

21. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the "InstallShield Wizard Completed" window opens.
22. Click **Finish**. The "IBM Director Agent Installer" Information window opens.
23. Remove the *IBM Director 4.11* CD from the CD-ROM drive.
24. Click **Yes** to restart your system.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, "Installing IBM Director extensions", on page 121.

Performing an unattended upgrade of IBM Director Agent

Note: You cannot perform a silent installation of IBM Director Agent on Windows XP.

You can perform an unattended upgrade of IBM Director Agent using a response file, which provides answers to the questions posed by the InstallShield wizard.

Complete the following steps to upgrade IBM Director Agent on Windows:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
net stop twgipc
```
2. Close all open applications.
3. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
4. Copy the `diragent.rsp` file to a local directory. This file is located in the `director\agent\windows\i386` directory on the *IBM Director 4.11* CD.
5. From Windows Explorer, right-click the copy of the `diragent.rsp` file and then click **Properties**. The “`diragent.rsp` Properties” window opens. Clear the **Read-Only** check box and click **OK**.
6. Open the copy of the `diragent.rsp` file in an ASCII text editor.
7. Modify and save the `diragent.rsp` file. This file follows the Windows INI file format and is fully commented

Note: Windows automatically detects and upgrades the IBM Director Agent features that were part of the existing IBM Director installation. However, you can select features that were not installed previously.

8. Change to the directory that contains the IBM Director Agent installation file (`ibmsetup.exe`). This file is located in the `director\agent\windows\i386` directory on the *IBM Director 4.11* CD.
9. From the command prompt, type the following command and press Enter:

```
ibmsetup.exe installationtype rsp="responsefile.rsp" waitforme
```

where:

- *installationtype* is one of the following commands:
 - UNATTENDED shows the progress of the installation but does not require any user input.
 - SILENT suppresses all output to the screen during installation.
 - *responsefile.rsp* is the path and name of the response file that you created in step 7.
 - *waitforme* is an optional parameter that ensures that `ibmsetup.exe` process will not end until the installation of IBM Director Agent is completed.
10. If prompted to do so, restart the operating system.

Note: If you installed ServeRAID Manager or MPA Agent for the first time, you must restart the managed system after the installation is completed. This ensures that the new features are detected.

11. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions”, on page 121.

Upgrading IBM Director Agent on Red Hat Linux or SuSE Linux

This section provides information about installation prerequisites and instructions for upgrading IBM Director Agent.

Note: If the managed system also has IBM Director Console installed, you must perform the upgrade using the instructions outlined in “Upgrading IBM Director Console and IBM Director Agent simultaneously” on page 150.

Preparing to upgrade IBM Director Agent on Linux

Before you upgrade IBM Director Agent, make sure you have installed any necessary prerequisites and device drivers. Consider the following information:

1. (IBM servers only) Determine the type of service processor installed in the server. If the server does not contain a Remote Supervisor Adapter or a Remote Supervisor Adapter II, you must install the IBM SMBus device driver for Linux before you install IBM Director Agent. The IBM SMBus device driver ensures that the Asset ID and Management Processor Assistant tasks function properly. See “Downloading, building, and installing the IBM SMBus device driver” for more information.
2. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

3. Verify that the operating-system password-encryption method is set to message digest 5 (MD5) or DES.
4. (SuSE Linux 7.x only) Verify that the following libraries and packages are upgraded to level 2.2.4-64 or later:
 - glibc libraries
 - glibc-devel package (if installed)
 - glibc-profile package (if installed)
5. If you want to use the Remote Session task on the managed system, verify that the package containing telnetd is installed and configured. This is usually in the `telnet_server_version.i386.RPM` package, where *version* is the code level of your Linux distribution.

Downloading, building, and installing the IBM SMBus device driver

You must download the IBM SMBus device driver source files:

- `ibmsmb-src-redhat-4.10-1.i386.rpm`
- `ibmsmb-src-suse-4.10-1.i386.rpm`

You can download the files from the IBM Systems Management Software: Download/Electronic Support page at http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html.

Before installing the IBM SMBus device driver, you must install the source RPM file, which builds the binary RPM file. You must build the binary RPM file on a system with the same kernel version and hardware configuration as the target system. Be sure that hardware configuration is similar in regard to the number of processors.

Complete the following steps to build and install the IBM SMBus device driver:

1. Configure a system with the appropriate operating system. Verify that the Linux kernel source is installed and properly configured.
2. To install the source RPM file, from a command prompt, type one of the following commands and press Enter:

Red Hat Linux and VMware ESX Server	<code>rpm -ivh ibmsmb-src-redhat-4.10-1.i386.rpm</code>
SuSE Linux	<code>rpm -ivh ibmsmb-src-suse-4.10-1.i386.rpm</code>

This creates a binary RPM file in the `/usr/local/ibmsmb` directory.

3. Change to the `/usr/local/ibmsmb` directory.
4. To install the IBM SMBus device driver, type the following command and press Enter:

```
rpm -ivh ibmsmb-4.10-1.i386.rpm
```

Issuing this command accomplishes the following tasks:

- Uncompresses and untars the archive into the `/usr/local/ibmsmb` directory
- Copies the driver, shared library, and all configuration files to their appropriate locations
- Loads the device driver

Upgrading IBM Director Agent on Red Hat Linux or SuSE Linux

When you upgrade IBM Director Agent, IBM Director automatically upgrades all previously-installed IBM Director features. You can also choose to install additional features.

Note: (Upgrading from IBM Director 3.x only) The installation directory has changed. During the upgrade, the installation process migrates old user data from `/opt/tivoliwg` to `/opt/IBM/director` automatically.

Complete the following steps to upgrade to IBM Director Agent on Linux:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
/opt/tivoliwg/bin/twgstop
```

2. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
3. If the CD does not automount, go to step 4. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where `mnt/cdrom` is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where `dev/cdrom` is the specific device file for the CD-ROM block device and `mnt/cdrom` is mount point of the CD-ROM drive.

5. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/agent/linux/i386/
```

where `mnt/cdrom` is the mount point of the CD-ROM drive.

6. Copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the dirinstall script. This file is fully commented.

You can specify the location of the RPM files, select previously-uninstalled IBM Director Agent features you want to install, and select log file options.

8. Save the modified installation script.
9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```

11. To start IBM Director Agent, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

12. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.
- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

13. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable the Wake on LAN feature. See “Enabling Wake on LAN” on page 178.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions”, on page 121.

Upgrading IBM Director Agent on NetWare

When you upgrade IBM Director Agent, IBM Director automatically upgrades all previously-installed IBM Director features. You also can choose to install additional features.

Notes:

1. If the managed system running NetWare 5.x includes any of the following service processors, IBM Director Server *cannot* manage the system out-of-band:
 - ASM processor
 - ASM PCI adapter

To manage these systems out-of-band using a management server running IBM Director Server, you must upgrade to NetWare 6.0 and IBM Director Agent 4.1 or later.

2. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you upgrade IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

Complete the following steps to upgrade IBM Director Agent on NetWare:

1. On the NetWare server, change to the console screen.
2. Stop IBM Director Agent. From the console, type the following command and press Enter:
`unload twgipc`
3. Insert the *IBM Director 4.11* CD into the CD-ROM drive of the system running Windows. If the autorun window opens, close it.
4. Start Windows Explorer and open the `\director\agent\netware` directory.
5. Double-click **setup.exe**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
6. Click **Next**. The “Installing IBM Director Agent” window opens.
7. Click **Yes** to accept the license agreement. A warning window opens, stating that an existing version of IBM Director has been detected.
8. Click **OK**. The “Choose destination location” window opens.
9. Click the drive that is mapped to the SYS volume on the NetWare server; then, click **Next**. The “Select Components” window opens.

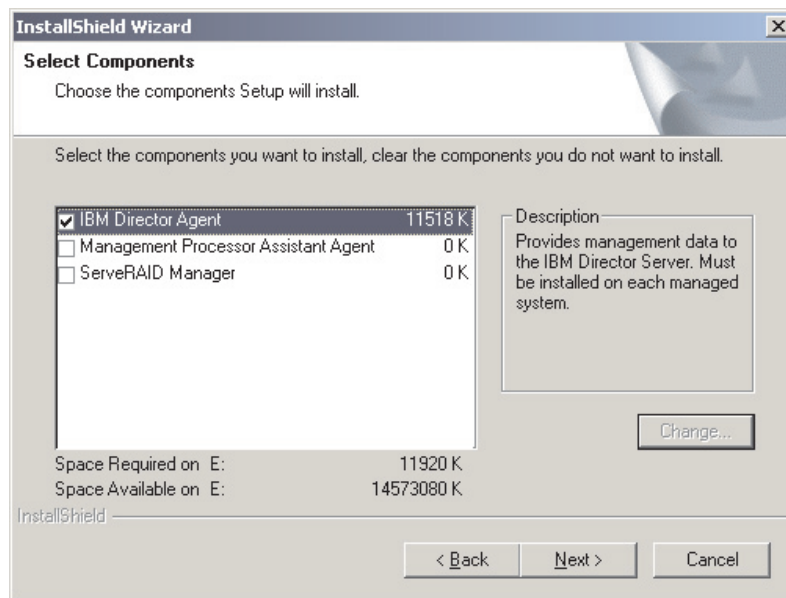


Figure 100. Upgrading IBM Director Agent on NetWare: “Select Components” window

10. Select the check boxes for the previously-uninstalled features you want to install; then, click **Next**. A status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Complete” window opens.
11. Click **Finish**.
12. Remove the *IBM Director 4.11* CD from the CD-ROM drive.
13. On the server running NetWare, start IBM Director Agent. Type the following command and press Enter:
`load twgipc`

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions”, on page 121.

Upgrading IBM Director Agent on Caldera Open UNIX

When you upgrade IBM Director Agent, IBM Director automatically upgrades all previously-installed IBM Director features. You also can choose to install additional features.

Notes:

1. Before upgrading IBM Director Agent, verify that the operating-system password encryption method is set to MD5 or DES.
2. (IBM servers only) If the server contains one of the following service processors, verify that the service processor device driver has been installed:
 - Advanced System Management processor
 - Advanced System Management PCI Adapter
 - Remote Supervisor Adapter
 - Remote Supervisor Adapter II

If the device driver is not installed before you upgrade IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

3. The installation directory has not changed. Program files and user data remain in the `/opt/tivoliwg` directory.

Complete the following steps to upgrade IBM Director Agent on Caldera Open UNIX:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
/opt/tivoliwg/bin/twgstop
```

2. Insert the *IBM Director 4.11* CD into the CD-ROM drive.
3. To mount the CD-ROM drive, type the following command and press Enter:

```
mount -F cdfs -o ro,nmconv=c,fperm=+x /dev/cdromdevicefile /mountpoint
```

where *cdromdevicefile* is the specific device file for the CD-ROM block device and *mountpoint* is the mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mountpoint/director/agent/openunix/i386
```

where *mountpoint* is the mount point of the CD-ROM drive.

5. Copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

6. Open an ASCII text editor and modify the “User configuration” section of the installation script. This file is fully commented. You can specify the location of the PKG files, select previously-uninstalled IBM Director features that you want to install, and select log file options.
7. Save the modified installation script.

8. To install IBM Director Agent, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

9. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/tivoliwg/bin/cfgsecurity
```

10. To start IBM Director Agent, type the following command and press Enter:

```
/opt/tivoliwg/bin/twgstart
```

11. To unmount the CD-ROM drive, type the following command and press Enter:

```
umount /mountpoint
```

where *mountpoint* is the mount point of the CD-ROM drive.

12. Remove the *IBM Director 4.11* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable the Wake on LAN feature. See “Enabling Wake on LAN” on page 178.

Upgrading IBM Director Agent using the Software Distribution task

You can use the IBM Director Software Distribution task to upgrade IBM Director Agent on managed systems running Windows or Linux.

The following files describe IBM Director Agent and the IBM SMBus device driver:

- diragent_linux.xml
- diragent_windows.xml
- smbdriver_linux.xml

You can download the files from the IBM Systems Management Software: Download/Electronic Support page at http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html.

When you import the XML files into IBM Director, the Director Update Assistant creates software packages. Then, you can use the IBM Director Software Distribution task to distribute the packages to the managed systems.

To install the IBM SMBus device driver using the Software Distribution task, you first must build the binary RPM file and copy it to the same directory as the smbdriver_linux.xml file. See “Downloading, building, and installing the IBM SMBus device driver” on page 159 for more information.

Make sure you have installed any necessary prerequisites and device drivers on the managed systems before upgrading IBM Director Agent. Be sure to read “Preparing to upgrade IBM Director Agent on Windows” on page 151 and “Preparing to upgrade IBM Director Agent on Linux” on page 159 for more information.

Creating a software package

Complete the following steps to create a software package:

1. Download the IBM Director Agent upgrade packages.
2. If you want to accept the default settings for the installation, go to step 3. Otherwise, open a copy of the dirinstall script or response file in an ASCII text editor. Modify the script or response file as needed; then, save the modified script or file.
3. Start IBM Director Console.
4. In the Tasks pane, double-click **Software Distribution**. The “Software Distribution Manager” window opens.

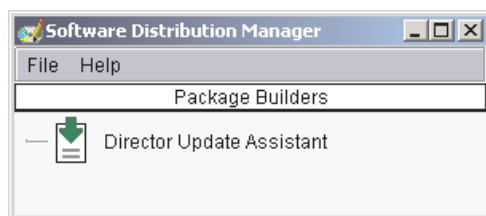


Figure 101. Creating a software package: “Software Distribution Manager” window (Standard Edition)

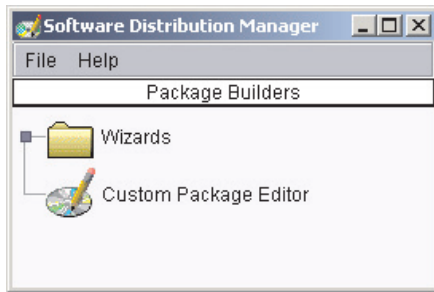


Figure 102. Creating a software package: “Software Distribution Manager” window (Premium Edition)

5. If you have not installed IBM Director 4.1 Software Distribution (Premium Edition), go to step 6. Otherwise, expand the **Wizards** tree.
6. Double-click **Director Update Assistant**. The “Director Update Assistant” window opens.



Figure 103. Creating a software package: “Director Update Assistant” window

7. By default, **Get files from the local system** is selected. If you want to get files from the management server, click **Get files from the Director server**.
8. To select a file, click **Browse**. The “IBM Update Package/Root Directory Location” window opens.

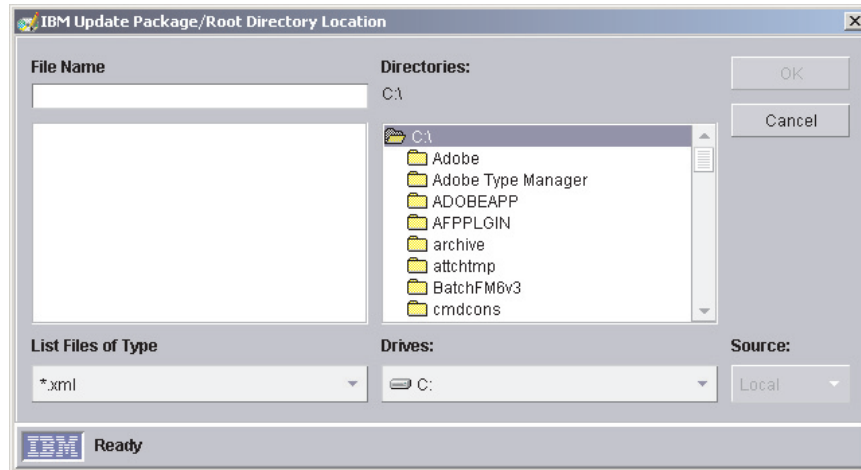


Figure 104. Creating a software package: “IBM Update Package/Root Directory Location” window

9. Locate the XML file and click it. The name of the XML file is displayed in the **File Name** field.

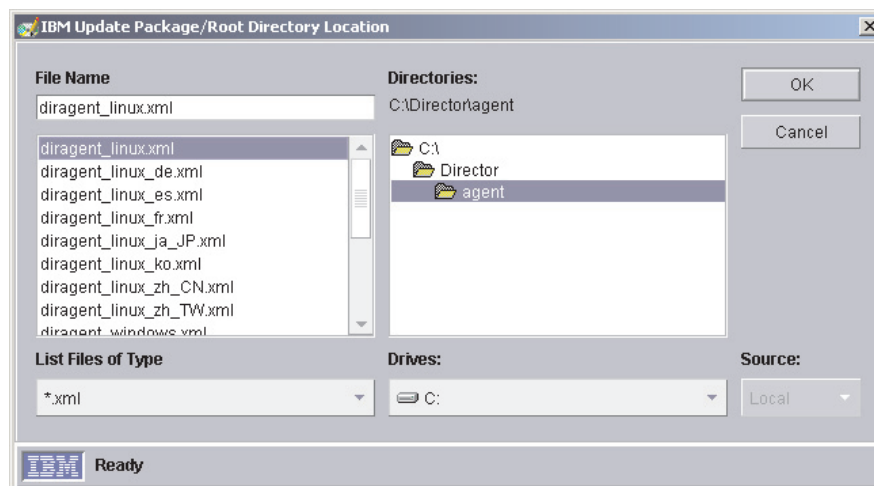


Figure 105. Creating a software package: “IBM Update Package/Root Directory Location” window

10. Click **OK**. The “Director Update Assistant” window reopens.

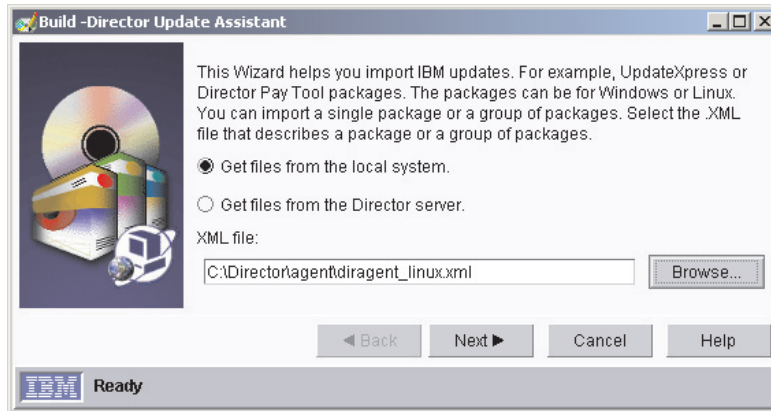


Figure 106. Creating a software package: “Director Update Assistant” window

11. Click **Next**. The second “Director Update Assistant” window opens.

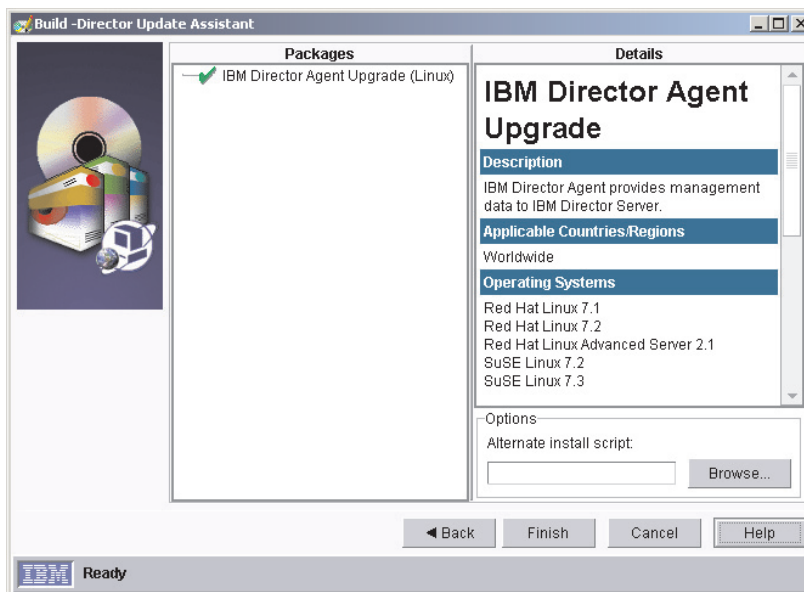


Figure 107. Creating software packages: “Director Update Assistant” window

12. To specify an alternative installation script or response file, click **Browse** and locate file you modified in step 2 on page 165.

Note: If you do not specify an alternative installation script or response file, IBM Director Agent is installed with the default settings specified in the diragent.rsp file or dirinstall script.

13. Click **Finish**. As the packages are processed, a status message is displayed at the bottom of the window.

14. When the processing is completed, the software-distribution packages are displayed in the Tasks pane of IBM Director Console.

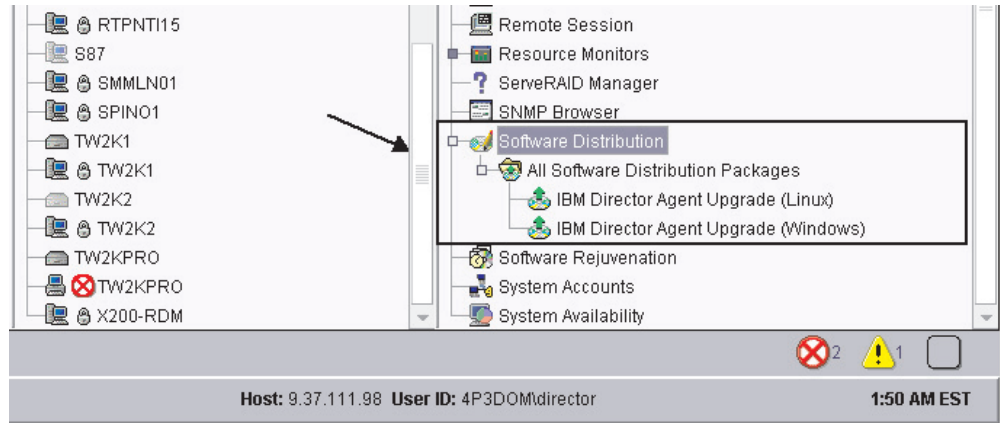


Figure 108. All Software Distribution Packages: IBM Director Agent Upgrade

Installing a software package

Complete the following steps to install a software package:

1. Start IBM Director Console.
2. In the Tasks pane, expand the **Software Distribution** task.
3. Click the software package that you want to distribute. Then drag it into the Group Contents pane and drop it onto the icon displayed for the system on which you want to install the software package. A window opens.

Note: To distribute software to several systems at once, you can drag the software package into the Groups pane and drop it onto the icon for the group. Alternatively, you can select multiple managed systems in the Group Contents pane.

4. When prompted Do you wish to create a scheduled job for this task or execute immediately?, click **Schedule** or **Execute Now**. If you click **Execute Now**, the software package is distributed immediately. If you click **Schedule**, the “New Scheduled Job” window opens.

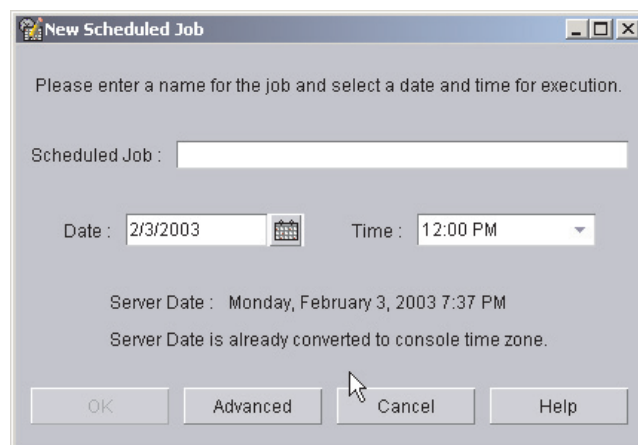


Figure 109. Scheduling the installation of a software package: “New Scheduled Job” window

5. Schedule the job:
 - a. In the **Scheduled Job** field, type a unique name for the job. This name is displayed in the Jobs pane of the Scheduler window.
 - b. In the **Date** field, type the day you want the software package to be installed (MM/DD/YYYY format).
 - c. In the **Time** field, type the time you want the software package to be installed.

For more information about the Scheduler task, see the *IBM Director 4.11 Systems Management Guide*.

6. Click **OK**. The “Save Job Confirmation” window opens.
7. Click **OK**.

Part 5. Maintenance and problem solving

Chapter 13. Modifying and uninstalling IBM Director

This chapter contains procedures for modifying and uninstalling IBM Director.

Modifying an IBM Director installation

This section provides instructions for modifying an IBM Director installation on the following operating systems:

- Windows
- Linux
- Caldera Open UNIX
- NetWare

You cannot use the Software Distribution task to modify an existing installation of IBM Director Agent.

Modifying IBM Director running on Windows

After you install IBM Director, you can modify the installation. You can configure the IBM Director database, install a previously uninstalled feature, or remove a feature.

Notes:

1. Before you configure a database for use with IBM Director, verify that you have completed any necessary preinstallation tasks. See “Database management” on page 29 for more information.
2. If both System Health Monitoring and MPA Agent are installed, you cannot remove System Health Monitoring only. To remove System Health Monitoring, you first must uninstall MPA Agent. When the uninstallation process is completed, then uninstall System Health Monitoring.

Configuring the database after IBM Director Server is installed

Complete the following steps to configure a database after you have installed IBM Director Server:

1. Stop IBM Director Server. From a command prompt, type the following command and press Enter:

```
net stop twgipc
```

2. Type the following command and press Enter:

```
cfgdb
```

The “IBM Director database configuration” window opens.

3. Follow the instructions on the screen. For more information, see “Installing IBM Director Server on Windows” on page 39. Steps 25 through 32 detail the process of selecting and configuring a database for use with IBM Director Server.

Installing or uninstalling an IBM Director feature

Complete the following steps to add a previously uninstalled feature to or remove a feature from IBM Director Server, IBM Director Console, or IBM Director Agent:

1. Click **Start** → **Settings** → **Control Panel**. The “Control Panel” window opens.
2. Double-click **Add/Remove Programs**. The “Add/Remove Programs” window opens.

3. Click the IBM Director software component you want to modify; then, click **Change**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
4. Click **Next**. The “Program Maintenance” window opens.

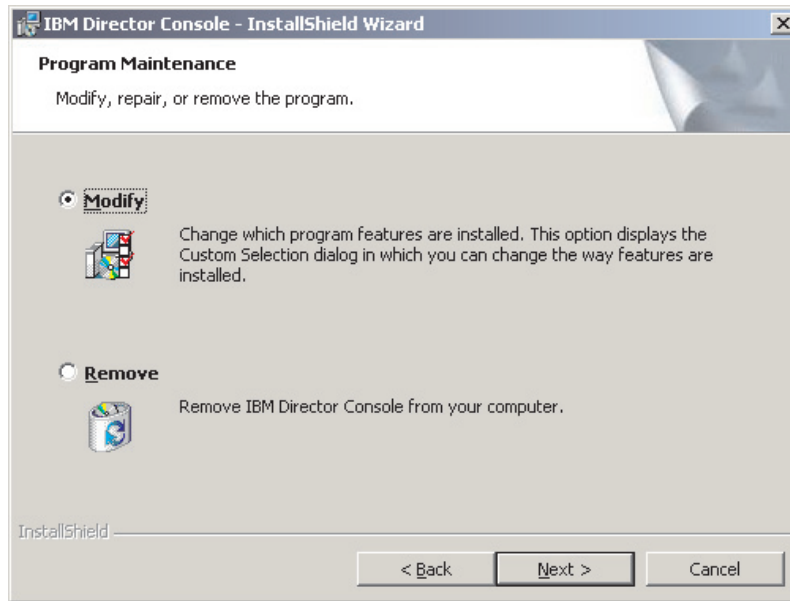


Figure 110. “Program Maintenance” window

5. Click **Modify**; then, click **Next**.
6. Continue through the wizard, making changes as necessary. For more information, see “Installing IBM Director Server on Windows” on page 39, “Installing IBM Director Console on Windows” on page 55, or “Installing IBM Director Agent on Windows” on page 61.

If you modify an IBM Director Agent installation by adding either ServeRAID Manager or MPA Agent, be sure to restart the managed system after the installation is completed. This ensures that the new components are detected.

You also can remove Server Plus Pack extensions by issuing the `dirunins` command from a command-line prompt. See “Uninstalling IBM Director using the `dirunins` command” on page 180 for more information.

Modifying IBM Director running on Linux

After you install IBM Director, you modify the installation. You can configure the IBM Director database, enable Wake on LAN for IBM Director Agent, install a previously uninstalled feature, or remove a feature.

Note: Before you configure a database for use with IBM Director, verify that you have completed any necessary preinstallation tasks. See “Database management” on page 29 for more information.

Installing the database after IBM Director Server is installed

Complete the following steps to install and configure a database after you have installed IBM Director Server:

1. Stop IBM Director Server. From a command prompt, type the following command and press Enter:
`/opt/IBM/director/bin/twgstop`
2. Type the following command and press Enter:
`/opt/IBM/director/bin/cfgdb`
3. Follow the instructions on the screen.
4. To restart IBM Director Server, type the following command and press Enter:
`/opt/IBM/director/bin/twgstart`

Enabling the Wake on LAN feature

Complete the following steps to enable Wake on LAN for IBM Director Agent:

1. Stop IBM Director Agent. Type the following command and press Enter:
`/opt/IBM/director/bin/twgstop`
2. Open an ASCII text editor and edit the ServiceNodeLocal.properties file. This file is located in the `/opt/IBM/director/data` directory.
3. Modify the value of `ipc.wakeonlan` to read as follows:
`ipc.wakeonlan=1`
4. Save and close the ServiceNodeLocal.properties file.
5. Start IBM Director Agent. Type the following command and press Enter:
`/opt/IBM/director/bin/twgstart`

Installing an IBM Director feature

Complete the following steps to add a previously uninstalled feature to IBM Director Server, IBM Director Console, and IBM Director Agent:

1. Make a copy of the `dirinstall` script. This file is located in the `/director/component/linux/i386` directory on the *IBM Director 4.11* CD, where *component* is `server`, `console`, or `agent`.
2. Open an ASCII text editor and modify the “User configuration” section of the `dirinstall` script.
3. Save the modified installation script.
4. Stop IBM Director. Type the following command and press Enter:
`/opt/IBM/director/bin/twgstop`
5. Run the `dirinstall` script. Type the following command and press Enter:
`/SourceDirectory/dirinstall`

where *SourceDirectory* is the directory to which you copied the modified installation script

6. Start IBM Director. Type the following command and press Enter:
`/opt/IBM/director/bin/twgstart`

You also can use the standard RPM commands.

Uninstalling an IBM Director feature

Complete the following steps to remove a feature from IBM Director Server, IBM Director Console, and IBM Director Agent:

1. Modify the `diruninstall` script, which is located in the `IBM/director/bin` directory. By default, this script removes all detected IBM Director components.
2. Save the modified uninstallation script.

3. Stop IBM Director. Type the following command and press Enter:
`/opt/IBM/director/bin/twgstop`
4. Run the `diruninstall` script. Type the following command and press Enter:
`/SourceDirectory/diruninstall`

where *SourceDirectory* is the directory to which you copied the modified uninstallation script.
5. Start IBM Director. Type the following command and press Enter:
`/opt/IBM/director/bin/twgstart`

You also can use the standard RPM commands.

Note: (KDE environment only) If you plan to use `kpackage`, ensure that the **Use scripts** check box is cleared.

Modifying IBM Director running on NetWare

Notes:

1. You cannot use this procedure to uninstall ServeRAID Manager or the MPA Agent. However, you can use this procedure to add either component to an existing IBM Director Agent installation.
2. To modify an IBM Director Agent installation, you must log on to the NetWare server from a Windows workstation running the NetWare Client for Windows.
3. The SYS volume must be mapped as a drive to the system running Windows.
4. You must have administrator or supervisor access on the NetWare server.

Complete the following steps to add a previously uninstalled feature to IBM Director Agent:

1. Stop IBM Director Agent. From the server running NetWare, change to the console screen. Type the following command and press Enter:
`unload twgipc`
2. Insert the *IBM Director 4.11* CD into the CD-ROM drive of the system running Windows. If the autorun window opens, close it.
3. Start Windows Explorer, and open the `\director\agent\netware` directory.
4. Double-click **setup.exe**. The InstallShield wizard starts.
5. Click **Next**. The “Installing IBM Director Agent” window opens.
6. Click **Next** to accept the license agreement. The “Choose destination location” window opens.

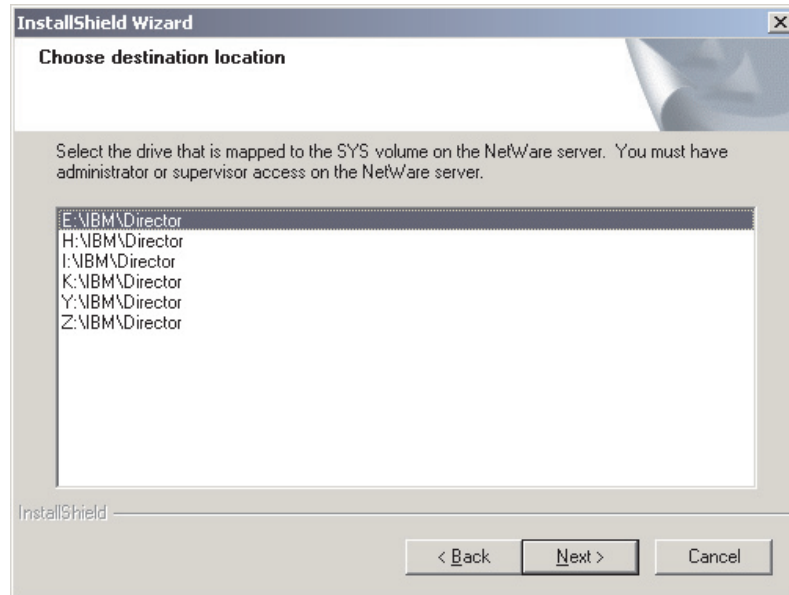


Figure 111. Modifying IBM Director Agent on NetWare: “Choose destination location” window

7. Click the drive that is mapped to the SYS volume on the NetWare server; then, click **Next**. The “Select Components” window opens.

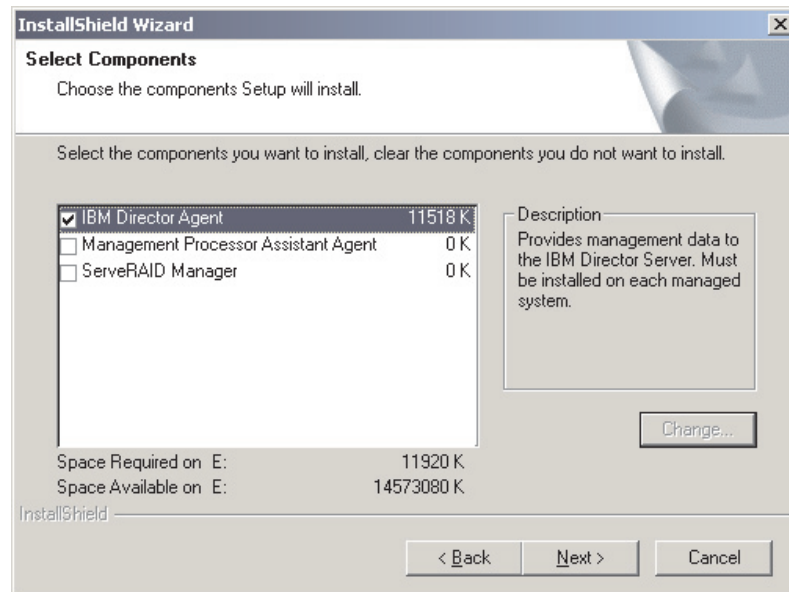


Figure 112. Modifying IBM Director Agent on NetWare: “Select Components” window

8. Select the check boxes for the components you want to add.
9. Click **Next**. The Setup Status window opens, and the IBM Director Agent installation begins. When the installation is completed, the “InstallShield Wizard Complete” window opens.
10. Click **Finish**.
11. On the NetWare server, change to the console screen.
12. Type the following command and press Enter:


```
load twgipc
```

Modifying IBM Director running on Caldera Open UNIX

After you install IBM Director Agent, you can enable the Wake on LAN feature, install a previously uninstalled feature, or remove a feature.

Enabling Wake on LAN

Complete the following steps to enable Wake on LAN for IBM Director Agent:

1. Stop IBM Director Agent. Type the following command and press Enter:

```
/opt/location/bin/twgstop
```

where *location* is IBM/director for a new installation of IBM Director Agent and tivoliwg if you upgraded from IBM Director Agent 3.x.

2. Open an ASCII text editor and edit the ServiceNodeLocal.properties file. This file is located in */opt/location/data*, where *location* is IBM/director for a new installation of IBM Director Agent and tivoliwg if you upgraded from IBM Director Agent 3.x.
3. Modify the value of ipc.wakeonlan to read as follows:

```
ipc.wakeonlan=1
```

4. Save and close the ServiceNodeLocal.properties file.
5. Start IBM Director Agent. Type the following command and press Enter:

```
/opt/location/bin/twgstart
```

where *location* is IBM/director for a new installation of IBM Director Agent and tivoliwg if you upgraded from IBM Director Agent 3.x.

Installing an IBM Director feature

Complete the following steps to add a previously uninstalled feature to IBM Director Agent:

1. Make a copy of the dirinstall script. This file is located in the */director/agent/openunix/* directory on the *IBM Director 4.11* CD.
2. Open an ASCII text editor and modify the “User configuration” section of the dirinstall script.
3. Save the modified installation script.
4. Stop IBM Director Agent. Type the following command and press Enter:

```
/opt/location/bin/twgstop
```

where *location* is IBM/director for a new installation of IBM Director Agent and tivoliwg if you upgraded from IBM Director Agent 3.x.

5. Run the dirinstall script. Type the following command and press Enter:

```
/SourceDirectory/dirinstall
```

where *SourceDirectory* is the directory to which you copied the modified installation script

6. Start IBM Director Agent. Type the following command and press Enter:

```
/opt/location/bin/twgstart
```

where *location* is IBM/director for a new installation of IBM Director Agent and tivoliwg if you upgraded from IBM Director Agent 3.x.

You also can use the standard pkgadd commands.

Important: If you plan to modify a Caldera Open UNIX installation by issuing a `pkgadd` command, be aware of the following consideration. If you have upgraded from IBM Director Agent 3.x, you must issue the following command:

```
pkgadd -a /SourceDirectory/admin.tivoliwg -d /SourceDirectory/  
PackageName
```

where *SourceDirectory* is the location of the `admin.tivoliwg` file and the Caldera Open UNIX packages, and *PackageName* is the name of the specific package. This ensures that the new feature is installed in the same directory as IBM Director Agent.

Uninstalling an IBM Director feature

Complete the following steps to remove a feature from IBM Director Agent:

1. Modify the `diruninstall` script, which is located in the `IBM/director/bin` directory. By default, this script removes all detected IBM Director components.
2. Save the modified uninstallation script.
3. Stop IBM Director Agent. Type the following command and press Enter:

```
/opt/location/bin/twgstop
```

where *location* is `IBM/director` for a new installation of IBM Director Agent and `tivoliwg` if you upgraded from IBM Director Agent 3.x.

4. Run the `diruninstall` script. Type the following command and press Enter:

```
/SourceDirectory/diruninstall
```

where *SourceDirectory* is the directory to which you copied the modified uninstallation script.

5. Start IBM Director Agent. Type the following command and press Enter:

```
/opt/location/bin/twgstart
```

where *location* is `IBM/director` for a new installation of IBM Director Agent and `tivoliwg` if you upgraded from IBM Director Agent 3.x.

You also can use the standard `pkgrm` commands.

Uninstalling IBM Director

You can use the following procedures to uninstall IBM Director.

Uninstalling IBM Director on Windows

You can uninstall IBM Director either by using the Windows Add/Remove Programs feature or from a command-line prompt.

Uninstalling IBM Director using the Windows Add/Remove Programs feature

Complete the following steps to uninstall IBM Director:

1. Shut down all applications.
2. Click **Start** → **Settings** → **Control Panel**. The “Control Panel” window opens.
3. Double-click **Add/Remove Programs**. The “Add/Remove Programs” window opens.
4. Click the IBM Director software component you want to remove; then, click **Remove**.
5. Follow the instructions on the screen.

Uninstalling IBM Director using the dirunins command

From a command-line prompt, type the following command and press Enter:

```
dirunins option directorcomponent
```

The following table contains information about the possible values for *option* and *directorcomponent*.

Table 12. Diruns parameters

Variable	Parameter	What it does
<i>option</i>	debug	Logs all messages sent by the Windows Installer log engine, including status and information messages
	deletedata	Deletes all configuration data
	<i>logfile</i>	Specifies the fully qualified name of an alternate installation log file, for example, XXX
	silent	Suppresses all output to the screen
	unattended	Shows the progress of the uninstallation but does not require any user input
<i>directorcomponent</i>	server	Uninstalls IBM Director Server and any installed Server Plus Pack extensions
	console	Uninstalls IBM Director Server and any installed Server Plus Pack extensions
	agent	Uninstalls IBM Director Agent
	capmgt	Uninstalls Capacity Manager
	swrejuv	Uninstalls Software Rejuvenation
	sysavail	Uninstalls System Availability
	activepci	Uninstalls Active PCI Manager

Note: If you are uninstalling IBM Director Agent, be sure to uninstall any installed Server Plus Pack extensions before uninstalling IBM Director Agent.

Uninstalling IBM Director on Linux

Use the `diruninstall` script located in the `IBM/director/bin` directory. Running this script removes all IBM Director components, including the Server Plus Pack extensions. To uninstall IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/diruninstall
```

You also can use standard RPM commands. Consider the following information:

- You must uninstall MPA, ServeRAID Manager, and the Server Plus Pack extensions *before* uninstalling IBM Director Server, IBM Director Console, or IBM Director Agent.
- If an IBM Director database is configured, you must delete the tables and remove the IBM Director database configuration. Perform this task *after* all other packages are removed but *before* uninstalling IBM Director Server. From a command prompt, type the following command and press Enter:

```
/opt/IBM/director/bin/uncfgdb
```

When you uninstall packages on Linux, the following files are retained to make it possible to restore persistent data:

- `/opt/IBM/director.save.1/saveddata.tar`
- `/etc/TWGagent/TWGagent.uid`

Uninstalling IBM Director Agent on NetWare

Complete the following steps to uninstall IBM Director Agent on NetWare:

1. From the server running NetWare, change to the console screen.
2. Type the following command and press Enter:
`unload twgipc`
3. Using an ASCII text editor, open the `autoexec.ncf` file and remove the following lines:

```
:*****IBM Director Agent*****  
Search add sys:IBM\Director  
load twgipc  
:*****IBM Director agent*****
```
4. Save the modified `autoexec.ncf` file.
5. Shut down and restart the server running NetWare.
6. From a Windows workstation running the NetWare Client for Windows, map a drive to the SYS volume and delete the `IBM\Director` directory.

Uninstalling IBM Director on Caldera Open UNIX

Use the `diruninstall` script located in the `IBM/director/bin` directory. Running this script removes all IBM Director components, including the Server Plus Pack extensions. To uninstall IBM Director, type the following command and press Enter:

```
/opt/location/bin/diruninstall
```

where *location* is `IBM/director` for a new installation of IBM Director Agent and `tivoliwg` if you upgraded from IBM Director Agent 3.x. You also can use standard PKGRM commands. Consider the following information:

- You must uninstall MPA, ServeRAID Manager, and the Server Plus Pack extensions *before* uninstalling IBM Director Agent.
- To uninstall MPA, issue the `pkgrm IBMMPAA` command from the command prompt.

Chapter 14. 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 4.1 or later:

- Installation, upgrades, and uninstallation (see page 183)
- IBM Director Server (see page 185)
- IBM Director Console (see page 188)
- IBM Director Agent (see page 191)
- Managed systems running Windows (see page 192)
- IBM Director tasks (see page 193)
- Software Distribution (see page 194)
- Web-based Access (see page 195)

Installation, upgrades, and uninstallation

This section describes problems that are found when installing, upgrading, or uninstalling IBM Director.

Installation

Table 13 describes problems that are found when installing IBM Director.

Table 13. Installation problems

Symptom	Suggested action
When you are installing IBM Director Server, the following message is displayed: Error 1722. There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor.	A possible reason for this error is that the display for a system running IBM Director Server or IBM Director Console must support at least 256 colors. Increase the display color palette to more than 256 colors, uninstall the previous partial installation and reinstall IBM Director Server.
Canceling the installation of IBM Director Agent left files in directories.	Safely 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 drive directory you designated for the installation.
When modifying the installation of IBM Director Agent or IBM Director Console, you are prompted for the location of the installation page "IBM Director Agent.msi" or "IBM Director Console.msi", as applicable.	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" or "IBM Director Console.msi" file, specify the directory where the extracted files are located.

Upgrades

Table 14 describes problems that are found while upgrading IBM Director.

Table 14. Upgrade problems

Symptom	Suggested action
Error message 1306 is displayed when upgrading.	<p>Complete the following steps:</p> <ol style="list-style-type: none"> 1. Access the “Windows Administrative Tools” window. 2. Double-click Services. The “Services” window opens. 3. Double-click Director Support Program. The “Properties” window opens. 4. In the Startup type list, click Manual. 5. Click OK. 6. Restart (reboot) the system. 7. Restart the IBM Director upgrade.
Error message 1921 is displayed for the UMSHTTPD service when upgrading.	<p>Complete the following steps:</p> <ol style="list-style-type: none"> 1. Access the “Windows Administrative Tools” window. 2. Double-click Services. The “Services” window opens. 3. Double-click UMS HTTPServ. The “Properties” window opens. 4. In the Service Status group, click Stop.
<p>(Japanese, Simplified and Traditional Chinese, and Korean only)</p> <p>Upgrading from IBM Director 3.1 to IBM Director 4.1 or IBM Director 4.11 resulted in distorted characters in the Description field of the Alert Forwarding Profiles in the Management Processor Assistant task.</p>	<p>To avoid this, make a note of your Description field contents before upgrading. After installing IBM Director 4.1 or IBM Director 4.11 you must reenter the information in English because all of the input fields that are interpreted by the service processor must be provided in US ASCII.</p>
Error message 1921 or 1922 is displayed when upgrading from IBM Director Server 2.2 to 3.1, 3.1.1, 4.1 or 4.11.	<p>Complete the following steps:</p> <ol style="list-style-type: none"> 1. Access the “Windows Administrative Tools” window. 2. Double-click Services. The “Services” window opens. 3. Double-click Director Support Program. The “Properties” window opens. 4. In the Startup type list, click Manual. 5. Click OK. 6. Restart the system. 7. Restart the upgrade of IBM Director Server.

Uninstallation

Table 15 describes problems that are found while uninstalling IBM Director.

Table 15. Uninstallation problems

Symptom	Suggested action
The following message is displayed: Error 1306: Another application has exclusive access to the C:\Program Files\IBM\Director\log\esntevt.dat	Shut down all other applications; then, click Retry . Cancel the uninstallation and restart the server. Then, start the uninstallation again.
Error message 1306 is displayed during an uninstallation.	Complete the following steps: <ol style="list-style-type: none"> 1. Access the “Windows Administrative Tools” window. 2. Double-click Services. The “Services” window opens. 3. Double-click Director Support Program. The “Properties” window opens. 4. In the Startup type list click Manual. 5. Click OK. 6. Repeat steps 3-5 for the Director Web Server if applicable. 7. Restart (reboot) the system. 8. Restart the uninstallation.
(Windows 2000 and Windows XP only) If you uninstall IBM Director Server, the following Web server log files might be locked by a process that is assumed to have ended. These files are: <ul style="list-style-type: none"> • apache_log • date.txt • stderr.log where <i>date</i> is the date the file was created.	If this occurs, a message is displayed stating that the file cannot be deleted. Clicking Retry only redisplay the message. This is a Windows timing issue with locked files and it should occur very infrequently.

IBM Director Server

Table 16 describes general problems that are found on management servers.

Table 16. IBM Director Server problems

Symptom	Suggested action
Databases	
The Microsoft Jet database is full.	Migrate to a larger database such as IBM DB2, Oracle, or Microsoft SQL.
Errors occur during the Database Configuration process when an Oracle database is used.	Configure and start the Oracle TCP/IP listener before starting the Database Configuration task. If a failure occurs, the database administrator must check the configuration of the TCP/IP listener.
When you are using Telnet to access a Linux environment through a Windows operating system and then running the cfgdb utility, messages overlay.	Complete the following steps to solve this problem: <ol style="list-style-type: none"> 1. Set the environmental variable term to vt100 before running the cfgdb utility. 2. Maximize the Telnet window to its largest possible size.

Table 16. IBM Director Server problems (continued)

Symptom	Suggested action
<p>The database application failed, generally with inventory errors, on a BladeCenter unit.</p>	<p>To solve this problem, use one of the following procedures:</p> <ul style="list-style-type: none"> • Use the TWGRESET command and change the database application before configuring the IBM Director database. Then, reconfigure the BladeCenter unit. • Uninstall IBM Director and delete any remaining files. Next, reinstall IBM Director and use a new database application. Then, reconfigure the BladeCenter unit. <p>In all cases, you must reconfigure the BladeCenter unit after changing the database application.</p>
Discovery	
<p>A BladeCenter discovery does not function correctly when multiple network interface cards (NICs) are enabled.</p>	<p>To solve this problem, use one of the following procedures:</p> <ul style="list-style-type: none"> • Change the NIC that is attached to the BladeCenter unit network. You might have to search to find the working NIC. • Disable the NICs that are not connected to the management module and then perform the discovery. When the discovery is complete, enable the NICs. You must do this each time you perform a discovery.
Encryption	
<p>Certain managed systems cannot be managed.</p>	<ul style="list-style-type: none"> • If encryption keys or encryption algorithms are changed using the “Encryption Administration” window, some systems might not be able to be managed. When new keys or a new cipher algorithm are requested, a presence check is forced by IBM Director. The presence check might not be completed immediately. There might be some delay between the requested operation and the time the managed system receives the new key. • If encryption is disabled on the management server, encrypted managed systems can no longer be managed. These systems will relock after a short period of time. Request a presence check to force the managed system to relock.
Event actions	
<p>Certain event actions fail because an incorrect adapter name is used.</p>	<p>If the configuration of a network adapter on a management server has been changed, IBM Director Server loses contact with IBM Director Agent for those managed systems that were discovered before the configuration change. To solve this problem, reestablish communication between IBM Director Server and IBM Director Agent on the affected managed systems. To do so, from IBM Director Console, click Tasks → Discover Systems → System Discovery to rediscover the managed systems.</p>
SNMP devices	
<p>An attribute value for a MIB file cannot be changed.</p>	<p>Make sure that:</p> <ul style="list-style-type: none"> • IBM Director is using a community name that allows write access to the MIB file that has a value that you want to change. • The MIB file is writable. • The MIB file has a value that you can set to be displayed in the SNMP Browser. • The compiled MIB file is associated with the value to change.

Table 16. IBM Director Server problems (continued)

Symptom	Suggested action
SNMP devices are not being discovered.	<p>Make sure that:</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 and must be added as a seed device. Remove the management server as the seed device. • The seed devices or other devices to be discovered are running an SNMP agent. • The community names that are specified in the IBM Director "Discovery Preferences" window allow IBM Director to read the mib-2.system table of the devices to be discovered and the mib-2.ip.ipNetToMediaTable on seed devices. • The correct network masks have been configured for all managed systems that must be discovered. • The correct addresses have been entered for the seed devices. The most effective seed devices are routers and domain name servers. To configure these devices, from IBM Director Console, click Options → Discovery Preferences. SNMP discovery does not discover all of the devices. If a device has not communicated with other managed systems, the device might not be discovered.
When a 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.
Starting	
(Linux only) Shortly after starting IBM Director Server, 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.
SNMP traps	
Trap destinations are missing from the SNMP agent table. Note: IBM Director sends and receives SNMP traps using TCP/IP only.	A table displays only the first trap destination in the SNMP configuration interface when 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).
Unexpected shut down	
(Linux only) IBM Director Server might shut down with an unrecoverable error under the following circumstances: <ul style="list-style-type: none"> • The management server is running a Linux operating system and using IBM DB2 as the IBM Director database. • The ServeRAID Manager is not installed. • Another management server discovers or inventories this system. 	Modify the IBM Director Server installation to include ServeRAID Manager.

IBM Director Console

Table 17 describes general problems that are found on the management console.

Table 17. IBM Director Console problems

Symptom	Suggested action
BladeCenter unit	
After inserting a blade server in a BladeCenter chassis, a physical platform managed object (PPMO) is not displayed in IBM Director Console.	Run the Inventory task on the BladeCenter chassis.
Dialog boxes	
Tables appear too small in a pane.	Change the table settings to enlarge the table in the pane. Note that modified table settings are not saved.
Discovered systems	
(Linux only) When no default router is configured or a nonroutable private network is used, IBM Director might not add any discovered systems on these networks to the IBM Director Console Group Contents pane.	<p>Use 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. <ol style="list-style-type: none"> In IBM Director Console, click Options → Discovery Preferences. Click the System Discovery pane. <p>Setting System Discovery seeds enables discovery of managed systems. For more information on seeding, see the online help for the System Discovery (IP) pane or the <i>IBM Director 4.11 Installation and Configuration Guide</i>.</p> Set a default router using 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 “route” man page. Setting a default router enables discovery of systems that are accessible using the specified router.</p>
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 that criterion 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>

Table 17. IBM Director Console problems (continued)

Symptom	Suggested action
Event action plans	
Group event action plans are not displayed.	<p>Complete the following steps to make sure that a managed system or group has an event action plan assigned to it:</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. <p>Event action plan associations are not displayed in the Groups pane, nor are event action plans that have been applied to a group that is displayed as being associated with each individual managed system that is a part of that group. The event action plan is displayed as being applied to the group only.</p>
Java Runtime Environment (JRE) Exceptions	
Intermittent JRE exceptions occur	<p>Make sure that you have sufficient memory. Intermittent JRE exceptions might occur when you run IBM Director Console on systems that are memory constrained. Sun Microsystems previously identified that this is a problem in some products. For more information about memory requirements, see the <i>IBM Director 4.11 Installation and Configuration Guide</i>.</p>
Managed system	
Managed systems are unavailable on the management console.	<ul style="list-style-type: none"> • Make sure that: <ul style="list-style-type: none"> – The system is turned on. – IBM Director Agent is running. – The network connection is reliable. • Check or modify the network timeout value. Click Start → Programs → IBM Director → Network → Configuration. • Check the network timeout value for the management server or the managed system. To change the network timeout value, use one of the following procedures: <ul style="list-style-type: none"> – Windows: Edit the twgipccf.exe file by changing the timeout value. – Linux: In the data directory, under the <i>products install</i> root, edit the ServiceNodeLocal.properties file. Add <code>ipc.timeouts=x</code> where <i>x</i> is the specified number of seconds. The default setting is 15 seconds. <p>If you are using UNIX or Linux and IBM Director Agent is installed in the default directory, you must restart IBM Director Agent. At a command prompt, type</p> <pre>/opt/IBM/director/bin/twgend -r</pre> <p>to stop and restart IBM Director Agent.</p>
A request for access fails, and the managed systems remain locked.	<p>Make sure that:</p> <ul style="list-style-type: none"> • You are using the correct user ID and password. • The managed system and management server accept encrypted communications only. • The server has encryption enabled through the “Encryption Administration” window. • If the managed system is running UNIX or Linux, the password encryption is set to Message Digest 5 (MD5) or Data Encryption Standard (DES).

Table 17. IBM Director Console problems (continued)

Symptom	Suggested action
<p>Through the use of imaging, a system was added and is displayed on the management console as a duplicate of a system that was previously added.</p>	<p>If cloning, make sure that IBM Director Agent, which is installed on the server to be used as the image, has never been started.</p> <p>If you have started your server to confirm installation of IBM Director Agent, perform the appropriate procedure:</p> <p>Linux: Edit the following file: /opt/IBM/director/data/ServiceNodeLocal.properties</p> <p>Remove the value after the equal symbol on the following line: ipc.UID=</p> <p>Also, delete the following file: /etc/TWGAgent/TWGagent.uid</p> <p>Windows: Remove the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName\TWGMachineID</p> <p>Also, delete the following file: \$(Director install path)\data\twgmach.id</p> <p>For example, C:\Program Files\IBM\director\data\twgmach.id</p>
<p>A question mark icon is displayed next to a managed system in IBM Director Console.</p>	<p>Reestablish communication between IBM Director Server and IBM Director Agent on the managed system. To do so, from IBM Director Console, click Tasks → Discover Systems → System Discovery to rediscover the managed system.</p>
<p>Starting</p>	
<p>Errors occur during attempts to log on to the management server using IBM Director Console.</p>	<p>Make sure that:</p> <ul style="list-style-type: none"> • The management server name, user ID, and password are valid. • The management server is running. • 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. <p>(Linux only) A green circle is not displayed in the task bar, but there is a Linux command-line command, called twgstat, that you can use. This reports the status of the management server. You can log on to the management console when twgstat returns a status of Active. The twgstat command returns the following statuses:</p> <ul style="list-style-type: none"> • Active: Server is fully active and ready for work. • Starting: Server is starting but not yet ready for work. • Ending: Server was requested to end, but has not yet ended. • Inactive: Server has ended or was never started. • Error: Server has ended abnormally.
<p>An input/output error connecting-to-server message appears when IBM Director Console is started.</p>	<p>Make sure that IBM Director Server is running before you start IBM Director Console. A green circle icon is displayed in the task bar when IBM Director Server is running.</p> <p>Do not start IBM Director Console if the following icons are displayed in the task bar:</p> <ul style="list-style-type: none"> • Red diamond icon (indicates that IBM Director Server not responding) • Green triangle icon (indicates that IBM Director Server is in the process of starting)

Table 17. IBM Director Console problems (continued)

Symptom	Suggested action
Time zone	
The wrong time zone is displayed.	When the time zone is changed, a managed system does not adjust the time that is shown in the event viewer. Start the managed system again to show the correct time for the new time zone.

IBM Director Agent

Table 18 describes symptoms of problems that are found on managed systems.

Table 18. IBM Director Agent problems

Symptom	Suggested action
(UNIX and Linux only) Shortly after starting IBM Director Agent, 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.
A managed system running an operating system cannot be accessed.	If the password encryption method is set to MD5 (message digest 5) when you install IBM Director Agent, salt values containing only two characters might be generated. IBM Director requires that the salt values be eight characters in length. Issue the passwd command to reset the password for the account that is used to access the managed system.
A problem occurs on a managed system running IBM Director Agent and NetWare 6.0 with Service Pack 2, and is using a Broadcom Gigabit Ethernet network interface card.	Complete the following steps: 1. Open the AUTOEXEC.NCF file. 2. Change CHECKSUM=OFF to the following text: LOAD B57.LAN SLOT=10012 FRAME=ETHERNET_II NAME=B57_1_EII LOAD B57.LAN SLOT=10012 FRAME=ETHERNET_802.2 NAME=B57_1_E82
A managed system returns invalid resource-monitor information for Windows Performance Monitors or Logical Disks after cluster failover, cluster failback, or disk drive unplug operations.	This problem is solved by Microsoft Windows 2000 Service Pack 4, available from Microsoft.
A managed system returns invalid data values for Windows Performance Monitors\LogicalDisk or Windows Performance Monitors\PhysicalDisk.	This problem is solved in an update provided under Microsoft Knowledge Base article ID number 827439. This article and the update can be obtained from the Microsoft Support Web site at http://support.microsoft.com/ .

Managed systems running Windows

Table 19 describes symptoms of problems found on managed systems running Windows.

Table 19. Managed systems running Windows problems

Symptom	Suggested action
IBM Director Server does not start on a system running Windows.	<p>Make sure that the IBM Director Server service account and password are valid. You must use a valid user ID that is part of the administration group. Incorrect user ID and password are most likely to cause a failure. Complete the following steps to change the user account or password for the service:</p> <ol style="list-style-type: none"> 1. Click Start → Settings → Control Panel. 2. Click Administrator Tools. 3. Double-click Services. 4. Right-click IBM Director Server. 5. Select Properties. Click Log On. 6. Select the This account check box, and modify and confirm the password. 7. Click OK, and then restart the IBM Director Server service.
(Windows 2000 only) A problem occurs on servers when the NetBIOS protocol is present and IBM Director is installed. Errors are generated until the event log is full.	Uninstall and then reinstall the network interface card device driver.
(Windows 2000 Server only) After IBM Director Server is installed, an error is displayed in the event log when the server is restarted.	<p>The open procedure for service PerfDisk in the DLL C:\WINNT\System32\perfdisk.dll has taken longer than the established wait time to be completed. One of the following situations might be occurring:</p> <ul style="list-style-type: none"> • The extensible counter might have a problem. • The service from which the counter is collecting data might have a problem. • The system might have been busy when the call was attempted. <p>Use the REGEDIT command and modify the following key entry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance key "Open Timeout"</p> <p>Change the Decimal value to 30000.</p> <p>This gives the system enough time to complete the startup task before starting the PERF counters.</p>
An event ID 2003 warning message appears in the application event log.	<p>If you are using Windows 2000 with Internet Information Services (IIS) installed, the following event ID 2003 warning message might be displayed in the application event log when you start System Monitor and add counters:</p> <p>The configuration information of the performance library "C:\WINNT\system32\w3ctrs.dll" for the "W3SVC" service does not match the trusted performance library information stored in the registry.</p> <p>The functions in this library are not recognized as trusted. Microsoft previously identified that this is a problem in these products.</p>

Table 19. Managed systems running Windows problems (continued)

Symptom	Suggested action
The following report is created indicating that an insufficient amount of space is available on a hard disk: 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 the Windows operating system: <ul style="list-style-type: none"> • Optical • Iomega • Jaz Microsoft identifies this as a Windows Management Instrumentation (WMI) problem.
When Shut Down is selected from the Start menu, a power off message is displayed.	Shutdown might fail on Pre-Advanced Configuration and Power Interface (ACPI) servers (Netfinity 7000) running Windows 2000. This does not turn off the system automatically.

IBM Director tasks

Table 20 describes symptoms of problems that are found when using IBM Director tasks other than Software Distribution.

Table 20. IBM Director task problems

Symptom	Suggested action
Active PCI Manager	
The Active PCI Manager task appears to be available and included after you upgrade to IBM Director 4.1 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 4.1, and be sure to select the Active PCI Manager option from the IBM Director Server Plus Pack.
When you are using the hot-plug feature, the status of the slot is not updated.	To update the status of a hot plug slot, the server must be restarted. This is a limitation of the Common Information Model (CIM) provider.
Configure Alert Standard Format (ASF)	
(xSeries 345 server only) ASF cannot be configured.	Complete the following steps to configure ASF on an xSeries 345 server: <ol style="list-style-type: none"> 1. Disable ASF from either Web-based Access or the management console. 2. Disable the network interface card. You cannot use Configure ASF if the network interface card is disabled.
Common Information Model (CIM) Browser	
When you attempt to enumerate a system, large amounts of CIM data are returned, causing errors in the CIM Browser.	Do not attempt to enumerate the instances of the root/cimv2:CIM_DirectoryContainsFile root/cimv2:Win32_Subdirectory class on Windows. Those CIM classes have instances for every file and directory on every disk in your server. If you attempt to enumerate these classes, your managed system or management server might run out of memory.
Inventory	
IBM Director Server fails Inventory collection on itself, independent of the hardware platform on which it is installed.	To resolve this and other System Health problems, manually start the ticsagent.exe program.

Table 20. IBM Director task problems (continued)

Symptom	Suggested action
Field-replaceable unit (FRU) information does not appear when inventory is collected.	If a system is not connected to the Internet when IBM Director Agent 4.1 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," in the <i>IBM Director 4.11 Systems Management Guide</i> . Additionally, make sure that the GETFRU command can reach the IBM Support FTP site through your firewall. For the GETFRU command to succeed, the managed system must have firewall access through a standard FTP port.
Logical disk drives	
A PCI adapter with logical disks cannot be stopped using the "Unplug or Eject Hardware" window if the PCI adapter and disks were present when IBM Director was started.	This problem is resolved by Microsoft Windows 2000 Service Pack 4, available from Microsoft.
Management Processor Assistant	
The Communications Configuration subtask is not displaying connection information.	Complete one of the following procedures: <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.
Mass Configuration	
When using Mass Configuration to configure Asset ID, a problem has developed because the system that is being configured is low on data space.	When the size of the configuration is larger than that of the remaining data space, the configuration fails without any indication that this failure occurs. This is a limitation of the data save area. Make sure that, for each byte of data, you have the same amount of space in your data save area.

Software Distribution

Table 21 describes problems that are found when using Software Distribution.

Table 21. 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 before being written to the target system. If disk space is insufficient on the management console, the package creation fails.
Remote Control fails when distributing software packages to managed systems that are behind a firewall.	Remote Control and Software Distribution both use session support to increase data transmission. Session support within TCP/IP causes data to flow through a nonreserved port that is different from the one that IBM Director typically uses for communication. Most firewalls do not allow the data to be transmitted through this other port. You can disable session support by creating an INI file on the managed system. In the <code>IBM\Director\bin</code> directory on the managed system, create a file named <code>tcpip.ini</code> 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 <code>tcpip.ini</code>, <code>tcpip2.ini</code>, <code>tcpip3.ini</code>, and so on. After creating the files, restart the managed system.</p>

Table 21. Software Distribution problems (continued)

Symptom	Suggested action
An error message is displayed when a software package is distributed using a redirector share.	The following error message is displayed: Managed System (system name) has detected that software package (package name) was not found on share (\\server\share). You can delete software packages from the management server. The redirector cache can be maintained only through the File Distribution Server Manager interface. To access it, right-click the Software Distribution task. Errors occur if you manipulate the cache through any means other than IBM Director Console.
Software packages are not using the file-distribution servers.	Make sure that the file-distribution server is a member of the same domain as the management server or has a trust relationship with that domain.
The software package installation failed, and the location of the package must be changed.	Reinstall IBM Director Agent, and specify a different drive and directory.
(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 However, when you press the Yen key, the Share Name field incorrectly displays the backslash (\) symbol.	Complete the following steps: 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 you want to use. Note: If you press the Yen key, do not use the backslashes; the backslashes cause redirected distribution to fail. 3. Exit the “Distribution Preferences” window; then, reenter this window, and retain the Yen symbols in the Share Name field example.
(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 where ₩ represents the Won symbol. However, when you press the Won key, the Share Name field incorrectly displays the backslash (\) symbol.	Complete the following steps: 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 you want to use. Note: If you press the Won key, do not use the backslashes; the backslashes cause redirected distribution to fail. 3. Exit the “Distribution Preferences” window; then, reenter this window, and retain the Won symbols in the Share Name field example.

Web-based Access

Table 22 describes symptoms of problems that are found when using Web-based Access.

Table 22. Web-based Access problems

Symptom	Suggested action
After repeated installations, there are problems logging into the IBM Director Agent Web Server using the Netscape Navigator Web browser.	Save the configuration data when prompted during IBM Director Agent uninstallation. This saves the old Secure Sockets Layer (SSL) certificate and allows the login to the Web Server to proceed after IBM Director Agent is reinstalled.

Table 22. Web-based Access problems (continued)

Symptom	Suggested action
(Windows XP or Windows 2003 only) A system that does not have Java installed displays a message that the Java Virtual Machine (JVM) is needed to view a managed system.	Install a Java Virtual Machine (JVM) from Sun Microsystems.
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 for Web-based Access, 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. Enter the same information that you used for the Microsoft Internet Explorer login.
Web-based Access is unavailable and an error message is displayed indicating that the page cannot be found.	<p>If you install Web-based Access on a managed system that is running Apache Web Server, you must modify the Web-based Access configuration files. Web-based Access and Apache Web Server use the same default connector ports. Complete the following steps:</p> <ol style="list-style-type: none"> 1. Stop the IBM Director Agent Web Server service. 2. Open the server.xml file. If you installed IBM Director in the default location, this file is located at e:\Program Files\IBM\Director\webserv\conf, where e is the hard disk drive where IBM Director is installed. 3. Change the server port to a port that is not already in use by another application: Server port="8005" 4. Change the connector port to a port that is not already in use by another application: port="8009" 5. Save the modified server.xml file. 6. Open the workers.properties file. If you installed IBM Director in the default location, this file is at e:\Program Files\IBM\Director\webserv\conf, where e is the hard disk drive where IBM Director is installed. 7. Change the connector port: port="8009" <p>You must specify a port that is not already in use by another application.</p> <ol style="list-style-type: none"> 8. Save the modified worker.properties file. 9. Open the tomcat.conf file. If you installed IBM Director in the default location, this file is at e:\Program Files\IBM\Director\webserv\conf, where e is the hard disk drive where IBM Director is installed. 10. Change the connector port to a port that is not already in use by another application: port="8009" 11. Save the modified tomcat.conf file. 12. Restart the IBM Director Agent Web Server service.
(Traditional and Simplified Chinese) When opening Web-based Access in a Netscape Web browser, all Chinese characters sometimes display as boxes.	<p>To ensure Chinese characters display properly, complete the following steps:</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 be sure that they are set correctly for Chinese language display.

Table 22. Web-based Access problems (continued)

Symptom	Suggested action
Load all Events does not function.	When the security log gets very large (approximately 4000 records), clicking Load All Events produces the Loading data...please wait message. After approximately 5 minutes, the message stops, and only the 30 most recent events are displayed. The Load All Events button is not enabled.

Chapter 15. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM® products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation® system, and whom to call for service, if it is necessary.

Before you call

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

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

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

Using the documentation

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

Getting help and information from the World Wide Web

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

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

Software service and support

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

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

Part 6. Appendixes

Appendix A. IBM Director Agent — IBM Director Server security

This chapter contains information about IBM Director Agent — IBM Director Server security. It includes an overview of authentication, procedures for securing managed systems, and information about key management.

How authentication works

Integrated into IBM Director is a security mechanism by which a managed system can authenticate any management server attempting to access it. Authentication enables IBM Director Agent to accept commands only from an IBM Director Server that is trusted (that is, authorized to manage it). Authentication protects managed systems from access by unauthorized management servers or rogue managed-system applications.

The IBM Director authentication process is based on two interlocking concepts:

- Digital-signature certification
- Security state of the managed system

Digital-signature certification

IBM Director authentication is based on the Digital Signature Algorithm (DSA). DSA is the public-key algorithm specified by the Digital Signature Standard of the National Institute of Standards and Technology. It enables the holder of a public key to verify the signature for a digital document that has been signed by a holder of the corresponding private key. In an IBM Director environment, it works in the following way:

1. IBM Director Server attempts to access IBM Director Agent. IBM Director Server bids the public keys that correspond to the private keys it holds.
2. IBM Director Agent checks these keys. If it considers the keys to be trusted, IBM Director Agent replies with a challenge that consists of one of the trusted public keys and a random data block.
3. IBM Director Server generates a digital signature of the random data block using the private key that corresponds to the public key included in the challenge. IBM Director Server sends the signature back to IBM Director Agent.
4. IBM Director Agent uses the public key to verify that the signature is a valid signature for the random data block. If the signature is valid, IBM Director Agent grants access to IBM Director Server.

This digital signature scheme has the following benefits:

- The public keys stored on the managed systems can be used only for verifying access.
- Using a random data block for signing makes replay attacks unusable.
- Generating a private key corresponding to a given public key is cryptographically improbable, requiring 2^{128} or more operations to accomplish.

Security state of the managed system

A managed system is in either an unsecured or secured state. A managed system is *unsecured* when any management server can access it and perform functions on it. A managed system is *secured* when only an authorized (trusted) management server can access it.

For all operating systems except NetWare, you can secure managed systems when you install IBM Director Agent. (Managed systems running Linux or UNIX are secured by default.) Managed systems also can be secured manually or during discovery.

Note: The IBM Director Agent running on a management server is secured automatically. It has a trust relationship only with the IBM Director Server installed on the same system.

On managed systems running Windows, the security state is determined by the `secin.ini` file. If the `secin.ini` file is initialized as unsecured, any management server can access the managed system and establish a trust relationship with IBM Director Agent. IBM Director Server establishes a trust relationship by giving IBM Director Agent a copy of its public key.

When the managed system has been secured by a management server, only that management server (and other management servers that had previously established a trust relationship) are able to access the managed system.

Where security information is stored

The information needed for authentication is stored in files on both the management server and the managed systems.

The public keys are stored in `dsaxxxx.pub` files, where `xxxxx` is a unique identifier. The private keys held by IBM Director Server are stored in `dsaxxxx.pvt` files. For example, the `dsa23ef4.pub` file contains the public key corresponding to the private key stored in the `dsa23ef4.pvt` file.

On systems running Windows, the secured/unsecured state data is stored in the `secin.ini` file, which is generated when you first start IBM Director Server or IBM Director Agent. On management servers, this file is initialized as secured; on managed systems, it is initialized as either secured or unsecured, depending on which options were selected during the installation of IBM Director Agent.

By default, the files are located in the following directories.

Operating system	Directory
Windows NT 4.0, Windows 2000, Windows XP, and Windows 2003	<code>d:\Program Files\IBM\Director\Data</code>
Red Hat Linux, SuSE Linux, VMware ESX	<code>/opt/IBM/director/data</code>
Caldera Open UNIX and SCO UnixWare	<code>/opt/IBM/director/data</code>
NetWare	<code>d:\IBM\Director</code>

where *d* is the hard disk on which IBM Director is installed and IBM Director is installed in the default location.

How the keys and `secin.ini` files work together

When you first start IBM Director Server, it randomly generates a matching set of public and private key files (`dsa*.pub` and `dsa*.pvt` files). The `secin.ini` file is generated and initialized as secure.

The initial security state of a managed system depends on the following factors:

- Which operating system it is running
- Which features were selected during the installation of IBM Director Agent

Managed systems running NetWare are set to the unsecured state automatically. For all other managed systems, the initial security state depends on which features are selected when IBM Director Agent is installed. If either encryption or agent/server security is selected, the managed system is set automatically to the secured state.

While a managed system is in the unsecured state, it accepts a public key from every management server that attempts to access it. Through this process, the managed system establishes trust relationships with those management servers.

If a management server secures that unsecured managed system, it gives that managed system a copy of its public key *and* its secin.ini file, which is initialized as secure. After this has occurred, the managed system no longer accepts any new public keys from management servers. However, the managed system continues to grant access to any management server whose public key is stored on the managed system.

Securing managed systems

There are several ways IBM Director Server can secure managed systems: during discovery, during the installation of IBM Director, and by manually copying the key files to managed systems.

Automatically securing unsecured systems

To configure IBM Director Server to secure unsecured managed systems automatically, in IBM Director Console click **Options** → **Discovery Preferences**; then, select the **Automatically secure unsecured systems** check box.

Manually securing a managed system

Note: Use this procedure in the following situations:

- You suspect that a rogue management server was introduced into an IBM Director environment before all managed systems were secured, and you want to resolve any possible security risks.
- You want to establish trust relationships between a managed system and multiple management servers.

Complete the following steps to manually secure a managed system running Windows or NetWare. You can use this procedure to secure either an unsecured or secured system:

1. If you have not done so already, install and start IBM Director Server. IBM Director Server creates a dsa*.pub and dsa*.pvt file, as well as a secin.ini file set to secure.
2. Copy the dsa*.pub and secin.ini files to a file server or other accessible location.

Note: If you want to authorize more than one IBM Director Server to manage a system, copy the dsa*.pub files from each. Only one copy of secin.ini is necessary.

3. If IBM Director Agent installed on the managed system has not been started yet, continue to step 5. Otherwise, stop IBM Director Agent. From a command prompt, type the following command and press Enter:

For Windows NT 4.0, Windows 2000, Windows XP, and Windows 2003	<code>net stop twgipc</code>
For NetWare	<code>unload twgipc</code>

4. Delete all existing `dsa*.pub` files from the managed system.
5. Place the `dsa*.pub` and `secin.ini` files (that you copied in step 2 on page 205) into one of the following directories:

For Windows NT 4.0, Windows 2000, Windows XP, and Windows 2003	<code>d:\Program Files\IBM\director\data</code>
For NetWare	<code>d:\IBM\Director</code>

where *d* is the hard disk where IBM Director Agent is installed, and IBM Director Agent is installed in the default directory.

6. To restart IBM Director Agent, type one of the following commands and press Enter:

For Windows NT 4.0, Windows 2000, Windows XP, and Windows 2003	<code>net start twgipc</code>
For NetWare	<code>load twgipc</code>

After IBM Director Agent starts, the managed system is secure; it permits *only* authorized IBM Director Servers (that is, the ones whose `dsa*.pub` file you copied to the managed system) to manage it.

You can automate this procedure by using logon scripts or other automated execution mechanisms.

Changing access or security states

This section provides information about gaining access to a secure managed system, removing access to a managed system, and adding another management server to an existing secure environment.

Accessing a secure managed system

If a managed system is secure but the management server to which you are connected does not have authorization to access it, the managed system is displayed in the Group Contents pane of IBM Director Console with a padlock icon beside it.

Complete the following steps to access a secure managed system from an unauthorized management server:

1. In IBM Director Console, right-click the managed system to which you do not have access.
2. Click **Request Access**. The "Request Access to Systems" window opens.



Figure 113. "Request Access to Systems" window

3. To access the system, type an authorized user ID and password; then, click **OK**.

Notes:

- a. The user ID must have administrator privileges on the managed system.
- b. The dsa*.pub files in the director\data directory on the managed system are the public key files used for authentication. They are largely unreadable binary files. However, the first string of characters in the file is the name of the management server that is trusted by the managed system.

You also can copy the dsa*.pub file from the management server to the managed system. After the managed system is restarted, it trusts the new management server.

Removing access to a managed system

To revoke the ability of a management server to access a managed system, delete the dsa*.pub file from the director\data directory on the managed system. Complete the following steps:

1. Change to the Director\Data directory on the managed system.
2. Using an ASCII text editor, view each dsa*.pub file. The first characters in a dsa*.pub file are of the form DSAxxxx, where xxxx is the name of the management server.
3. Locate the dsa*.pub file for the management server that you want to unauthorize, and delete it.
4. To stop IBM Director Agent, from a command prompt, type one of the following commands and press Enter:

For Windows NT 4.0, Windows 2000, Windows XP, and Windows 2003	net stop twgipc
---	-----------------

For Red Hat Linux, SuSE Linux, VMware ESX, Caldera Open UNIX, and SCO UnixWare	/opt/IBM/director/twgstop
---	---------------------------

For NetWare	unload twgipc
--------------------	---------------

5. To restart IBM Director Agent, type one of the following commands and press Enter:

For Windows NT 4.0, Windows 2000, Windows XP, and Windows 2003	net start twgipc
---	------------------

For Red Hat Linux, SuSE Linux, VMware ESX, Caldera Open UNIX, and SCO UnixWare	/opt/IBM/director/twgstart
---	----------------------------

For NetWare	load twgipc
--------------------	-------------

After IBM Director Agent starts, the management server whose dsa*.pub file you removed is no longer able to access the managed system.

Adding a trusted management server to an existing secure environment

To add another trusted management server to an existing secure environment, you can perform one of the following procedures:

- Set up the new server, install IBM Director Server, and copy the new server dsa*.pvt file to a trusted management server. Stop and restart IBM Director Server on the trusted management server. As IBM Director Server initializes, it delivers the dsa*.pub file corresponding to the new dsa*.pvt file to all of its trusting managed systems. This causes the managed systems to trust the new management server.
- Set up the new server, install IBM Director Server, and copy the dsa*.pvt file from an existing trusted management server. This enables the new management server to authenticate itself immediately to the managed systems that trusted the existing management server. The new management server also is trusted by the older management server.

Key management

This section provides information about determining the origin of a key and recovering lost keys.

Determining the origin of a public or private key

The public and private key files are binary files, but they contain textual data that indicates their origin. If a dsa*.pub or dsa*.pvt file is printed using the type command at a command prompt, the following data is displayed in the first line:

```
xxxxDSAKeytypeString
```

where:

- *xxxx* is a four-character header.
- *Keytype* indicates the type of the key. “P” denotes public, and “p” denotes private.
- *String* is the name of the management server that generated the key file.

For example, DSAPdirector4_1 indicates a public key file generated by a management server named director4_1, and DSApdirector4_1 indicates the private key file generated by the same management server.

Recovering lost public and private key files

It is *very important* to back up and protect the dsa*.pvt files. If they are lost, you cannot regenerate these files.

If a private key file is lost, you must repeat one of the previously described procedures for initializing security or adding a new trusted management server, either using another existing trusted dsa*.pvt key or the new key generated by the management server when it restarts without its private key file. See “Adding a trusted management server to an existing secure environment”.

If a public key file is lost, you can regenerate it by having the management server that holds the corresponding private key discover, add, or access any unsecured managed system. The public key file is generated on the managed system. The

management server does not require the dsa*.pub file that corresponds to its dsa*.pvt file; the private key file includes all the information from the public key files.

Appendix B. 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.

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

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

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

Abbreviations

The following table lists abbreviations that are used in the IBM Director 4.1 publications.

Table 23. Abbreviations used in IBM Director

Abbreviation	Definition
ACPI	Advanced Configuration and Power Interface
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI adapter
BIOS	basic input/output system
CIM	Common Information Model
CIMOM	CIM Object Manager
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management

Table 23. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
CSV	comma-separated value
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
EEPROM	electrically erasable programmable read-only memory
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	file transfer protocol
GB	gigabyte
Gb	gigabit
GMT	Greenwich mean time
GUI	graphical user interface
GUID	globally unique identifier
HTML	hypertext markup language
IETF	Internet Engineering Task Force
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPX	internetwork packet exchange
ISDN	integrated services digital network
ISMP	integrated system management processor
JVM	Java [®] Virtual Machine
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JFC	Java Foundation Classes
JRE	Java Runtime Environment
KB	kilobyte
KBps	kilobytes per second
Kb	kilobits
Kbps	kilobits per second
KVM	keyboard/video/mouse
LAN	local area network
LED	light-emitting diode
MAC	media access control

Table 23. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
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
MSCS	Microsoft Cluster Server
MSDE	Microsoft Data Engine
MST	Microsoft software transformation
MTU	maximum transmission unit
NAS	network attached storage
NIC	network interface card
NNTP	Network News Transfer Protocol
NVRAM	nonvolatile random access memory
ODBC	Open DataBase Connectivity
OID	object ID
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PFA	Predictive Failure Analysis
PIN	personal identification number
POST	power-on self-test
PPMO	physical platform managed object
RAM	random access memory
RDM	Remote Deployment Manager
RPM	(1) Red Hat Package Manager (2) revolutions per minute
SID	(1) security identifier (2) Oracle system identifier
SLP	Service Location Protocol
SMBIOS	System Management BIOS
SMI	System Management Information
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology

Table 23. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
SNMP	Simple Network Management Protocol
SNA	Systems Network Architecture
SPB	software package block
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSM	Scalable Systems Manager
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
UDP	User Datagram Protocol
UID	unique ID
UIM	upward integration module
UNC	universal naming convention
USB	Universal Serial Bus
UUID	universal unique identifier
VPD	vital product data
VRM	voltage regulator module
WAN	wide area network
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
XML	Extensible Markup Language

Appendix C. 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 2003. 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	Predictive Failure Analysis
Asset ID	Redbooks
BladeCenter	ServeRAID
DB2	ServerProven
DB2 Universal Database	SurePOS
e-business logo	ThinkPad
@server	Tivoli
IBM	Tivoli Enterprise
IntelliStation	TotalStorage
Netfinity	Wake on LAN
NetVista	Update <i>Xpress</i>
OS/2	xSeries
OS/2 WARP	

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.

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

Glossary

A

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

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

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

alert standard format (ASF). A specification created by the Distributed Management Task Force (DMTF) that defines remote-control and alerting interfaces that can best serve a client 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.

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 and standard Category 5 cables. When servers containing ISMPs and ASM processors are connected to such a network, IBM Director can manage them out-of-band.

Advanced System Management (ASM) PCI adapter. An IBM service processor 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 an ASM gateway, the ASM PCI adapter can communicate with other ASM PCI adapters and ASM processors only.

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

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

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

B

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

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

BladeCenter chassis. A BladeCenter component that acts as an enclosure. This 7-U modular chassis can contain up to 14 blade servers. It enables the individual

blade servers to share resources such as the management, switch, power, and blower modules.

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

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

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 includes 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 system-management application using the CIM layer.

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

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, including microprocessor type, installation date, attached printers and other peripheral devices, power sources, and maintenance history. DMI is not related to any specific hardware, operating system, or management protocols. It is mappable to existing management protocols such as Simple Network Management Protocol (SNMP).

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

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

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

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

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

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

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

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

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

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

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

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

DMI. See Desktop Management Interface.

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

dynamic group. See group, dynamic.

E

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

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

event action plan. A user-defined plan that determines how IBM Director will manage certain events. An event action plan 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 simple event action plans.

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

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

extension. See IBM Director extension.

F

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

field-replaceable unit (FRU). A component of an IBM system that can be replaced in the field by a service

technician. Each FRU is identified by a unique seven-digit alphanumeric code.

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

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

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

FRU. See field-replaceable unit.

FTMI. See Fault Tolerant Management Interface.

G

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

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

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

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

GUID. See Universal Unique Identifier.

H

Hardware Status task. An IBM Director task that can be used to view managed-system and -device hardware status from the management console. The Hardware Status task notifies you whenever a managed system or device has a hardware status change by displaying an icon in the lower-right corner of 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).

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

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

integrated 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 or Caldera Open UNIX. For IBM Director Server to connect out-of-band to an ISMP,

the server containing the ISMP must be installed on an ASM interconnect network with a Remote Supervisor Adapter serving as the ASM gateway.

interprocess communication (IPC). A 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 installed software that does not correspond to a predefined software profile included with IBM Director, you can edit the software-dictionary file to update your software inventory.

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

IPC. See interprocess communication.

ISMP. See integrated 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 device. An SMNP device managed by IBM Director.

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

managed object. An item managed by IBM Director. Managed objects include managed systems, Windows NT clusters, BladeCenter chassis, management processors, SNMP devices, multi-node servers (scalable systems), scalable partitions, physical platforms, scalable nodes, and remote I/O enclosures. In IBM Director Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or 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 BladeCenter modules, multiplexes the keyboard/video/mouse (KVM), and monitors critical information about the chassis and blade servers.

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

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

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

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

address (preceded by “MM”) as the default name for a BladeCenter management module.

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

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

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

MMC. See Microsoft Management Console.

MPA. See Management Processor Assistant.

multicast discovery. See discovery, multicast.

N

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 both the operating system and interprocess communication (IPC).

P

partition. See scalable partition.

partition descriptor.

A small data structure located in NVRAM that defines a scalable system and the number of scalable nodes in it and defines any scalable partitions created from the scalable nodes. For multi-chassis servers, the partition descriptor defines one server as the primary server and the other as secondary.

The partition descriptor is read by BIOS code to start the scalable partition created from the scalable nodes. For some servers, the Configuration/Setup Utility program (in BIOS) provides a default partition descriptor. However, it is recommended that you use Scalable Systems Manager to create and modify partition descriptors.

PCI. See peripheral component interconnect.

PCI-X. See peripheral component interconnect-extended.

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

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

PFA. See Predictive Failure Analysis.

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

plug-in. See IBM Director extension.

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

private key. A central component of the digital-signature algorithm. Each management server holds a private key and uses it to generate digital signatures that managed systems use to authenticate 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. It is available for use on servers running Windows 2000 or Windows 2000 Advanced Server only.

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

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

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

remote I/O enclosure. An IBM Director managed object representing 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 an ASM gateway, the Remote Supervisor Adapter can communicate with all service processors on the ASM interconnect.

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

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

RXE Expansion Port. The dedicated high-speed port used to connect a remote I/O expansion unit, for example, the RXE-100 Remote Expansion Enclosure, to a server such as the xSeries 445 server.

S

scalable node. A physical platform that has at least one SMP Expansion Module. At the time of publication, the xSeries 440 and xSeries 445 are the only server models whose chassis can be scalable nodes. 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: it can be powered-on and powered-off 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. At the time of publication, only the xSeries 445 servers can be used to create scalable partitions in IBM Director.

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 scalable nodes, the servers that they represent must be interconnected through their SMP Expansion Modules to make a 16-way configuration, for example, a 16-way xSeries 445 server. Scalable nodes that represent xSeries 445 servers in supported configurations are used in manageable scalable systems. Scalable nodes that represent xSeries 440 servers in a 16-way configuration are used in view-only scalable systems.

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

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

Server Plus Pack. See IBM Director Server Plus Pack.

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

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

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, when installed on a managed system, enables SNMP-based managers to poll the managed system and receive its alerts. If System Health Monitoring is installed on the managed system also, hardware alerts can be forwarded as SNMP traps.

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

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

SNMP discovery. See discovery, SNMP.

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

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

SSL. See secure sockets layer.

static group. See group, static.

static partition. A view-only scalable partition comprised of xSeries 440 servers.

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

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

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

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

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

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

T

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

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

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

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

TTL. See time to live.

U

unicast discovery. See discovery, unicast.

universal unique identifier (UUID). A 128-bit character string guaranteed to be globally unique and

used to identify components under management. The UUID enables inventory-level functionality and event tracking of nodes, partitions, complexes, and remote I/O enclosures.

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

upward integration. The methods, processes and procedures that 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 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 211
- Active PCI Manager
 - hardware, supported 9
 - managed systems, installing on 121
 - management console, installing on 57
 - management server, installing on 42
 - operating systems, supported 9, 15
 - overview 9
 - prerequisites 9, 13
 - subtasks 9
 - troubleshooting 131, 193
- Add BladeCenter Chassis window 83
- Add Management Processors window 105
- Advanced Systems Management PCI adapter
 - See ASM PCI adapter
- Advanced Systems Management processor
 - See ASM processor
- Agent
 - function 6
 - hardware requirements 13
 - license 6, 18
 - Linux, installing on
 - dirinstall script 70
 - encryption, enabling 71
 - prerequisites 69, 159
 - SMBus device driver 69
 - Wake on LAN, enabling 71
 - modifying an installation
 - Linux 174
 - NetWare 176
 - Open UNIX 178
 - Windows 173
 - NetWare, installing on
 - features, selecting 73
 - network driver, configuring 74
 - network protocols 16
 - Open UNIX, installing on
 - dirinstall script 74
 - encryption, enabling 75
 - Wake on LAN, enabling 75
 - operating systems, supported 6, 14
 - troubleshooting 183, 191
 - uninstalling
 - Linux 180
 - NetWare 181
 - Open UNIX 181
 - Windows 179
 - upgrading
 - Linux 158
 - NetWare 162
 - Open UNIX 163
 - Software Distribution task, using 165
 - upgrading on Windows
 - diragent.rsp file 158
 - encryption, enabling 154
 - features, selecting 153

- Agent (*continued*)
 - upgrading on Windows (*continued*)
 - InstallShield wizard, using 152
 - network driver, configuring 157
 - securing managed system 155
 - security state, setting 154
 - software-distribution settings 155
 - unattended installation, using 157
 - Wake on LAN, enabling 157
 - Web site xvi
 - Windows, installing on
 - diragent.rsp file 68
 - encryption, enabling 64
 - features, selecting 63
 - InstallShield wizard, using 62
 - network driver, configuring 67
 - securing managed system 65
 - security state, setting 64
 - software-distribution settings 65
 - unattended installation, using 67
 - Wake on LAN, enabling 67
- Agent features
 - Management Processor Assistant Agent 7
 - Remote Control Agent 7
 - ServeRAID Manager 7
 - SNMP Access and Trap Forwarding 8
 - System Health Monitoring 8
 - Web-based Access 7
 - Web-based Access help files 8
- alert-forwarding strategy
 - ASM PCI adapter 24, 25
 - ASM processor 24, 25
 - ISMP 24, 25
 - Remote Supervisor Adapter 24, 25
- alerts
 - in-band 7
 - ISMP and limitations 24
 - Management Processor Assistant Agent, role of 24
 - out-of-band 24
 - System Health Monitoring, role of 24
- APC PowerChute Extension for IBM Director 11
- Application Workload Management (Aurema) 11
- ASF, troubleshooting 193
- ASM interconnect gateway
 - definition 23
 - ISMPs, enabling out-of-band communication with 23
 - supported service processors 23
- ASM interconnect network
 - ASM interconnect gateway, role of 23
 - ASM PCI adapter 25
 - ASM processor 25
 - configuring 22
 - definition 23
 - ISMP 25
 - Remote Supervisor Adapter 25
- ASM PCI adapter
 - alert-forwarding strategies 24, 25

- ASM PCI adapter *(continued)*
 - ASM interconnect network 25
 - configuring 105
 - Management Processor Assistant Agent 7
 - management processor object, creating 105
 - Netfinity servers 25
 - out-of-band communication, pathways for 24, 25
 - use as an ASM interconnect gateway 23
 - xSeries servers 25
- ASM processor
 - alert-forwarding strategies 24, 25
 - ASM interconnect network 25
 - Management Processor Assistant Agent 7
 - Netfinity servers 25
 - out-of-band communication, pathways for 24, 25
 - out-of-band management 105
 - xSeries servers 25
- Asset ID, troubleshooting 194
- attention notice xiv

B

- BIOS, updating 13
- blade servers
 - boot sequence 85
 - deployment policies 85
 - installing operating systems 79, 94
 - Remote Deployment Manager, using 79
- BladeCenter
 - chassis
 - assigning IP addresses 81
 - automatically discovering 81
 - configuring 84
 - DHCP server, using 81
 - discovering 81
 - IP address conflicts 81
 - managed object 81, 82
 - manually assigning IP addresses 81, 83
 - manually discovering 82
 - deployment infrastructure
 - changing Director database 79
 - DHCP server, using 28, 81
 - illustration 28
 - IP address conflicts 28, 81
 - security 28
 - management module
 - assigning temporary IP addresses 28
 - default IP address 28
 - default user name and password 83
 - troubleshooting 186, 188
- BladeCenter Deployment wizard
 - chassis detect-and-deploy profile
 - creating 84, 95
 - overwriting 95
 - configuring the chassis 84
 - deployment policies 85
 - IP settings, configuring 91
 - management module
 - logging in to 87
 - network protocols, configuring 90
 - properties, configuring 89

- BladeCenter Deployment wizard *(continued)*
 - operating systems, deploying 94
 - profiles
 - changing name of 95
 - displayed in Console (illustration) 96
 - overview 85
 - switch modules
 - external ports, configuring 93
 - network protocols, configuring 93
 - user name and password, changing 92
- books xiv
- broadcast discovery 102
- broadcast relay 103

C

- Capacity Manager
 - managed systems, installing on 121
 - management console, installing on 57
 - management server, installing on 42
 - overview 9
 - supported operating systems 15
- chassis (BladeCenter)
 - assigning IP addresses 81
 - automatically discovering 81
 - configuring 84
 - DHCP server, using 81
 - discovering 81
 - IP address conflicts 81
 - managed object 81, 82
 - manually assigning IP addresses 81, 83
 - manually discovering 82
- chassis detect-and-deploy profile
 - creating 84
 - definition 85
 - overwriting 95
- chassis managed objects
 - creating 82
 - displayed in Console (illustration) 82
 - troubleshooting 85
- CIM Browser, troubleshooting 193
- Cluster Systems Management 11
- Compatibility Documents for IBM Director 4.1 14, 18
- Console
 - features, selecting 56
 - function 6
 - hardware requirements 13
 - installing on Linux 59
 - installing on Windows
 - dircon.rsp file 58
 - InstallShield wizard, using 55
 - Server Plus Pack 57
 - unattended mode, using 58
 - license 7, 18
 - modifying an installation
 - Linux 174
 - Windows 173
 - network protocols 16
 - screenshot 80
 - starting 79
 - supported operating systems 7, 15

- Console (*continued*)
 - troubleshooting
 - BladeCenter 188
 - dialog boxes 188
 - event action plans 189
 - installing 183
 - JRE exceptions 189
 - management server log on failure 190
 - not displaying discovered systems 188
 - starting 190
 - time zone error 191
 - uninstalling
 - Linux 180
 - Windows 179
 - upgrading on Linux 149
 - upgrading on Windows
 - dircon.rsp file 148
 - features, selecting 147
 - InstallShield wizard, using 145
 - unattended mode, using 148
- customer support xv

D

- Data Encryption Standard
 - See DES
- database
 - DB2 Universal Database
 - Linux Director installation 32
 - Windows Director installation 30
 - installing after Director Server is installed 173
 - Microsoft Data Engine 1.0 30
 - Microsoft Jet 4.0
 - overview 29
 - size limitations 29
 - Microsoft SQL Server 30
 - Oracle Server
 - JDBC driver 32
 - overview 32
 - PostgreSQL 33
 - SQL Server 2000 Desktop Engine 30
 - troubleshooting 185, 186
- database server, definition 29
- DB2 Universal Database
 - Linux Director installation 32
 - Windows Director installation 30
- deployment infrastructure (BladeCenter)
 - changing Director database 79
 - DHCP server, using 28, 81
 - illustration 28
 - IP address conflicts 28, 81
 - security 28
- deployment policies 85
- DES 34
- detect-and-deploy profile
 - creating 84
 - overwriting 95
- device driver, SMBus
 - binary RPM file 69, 159
 - building and installing 69, 159
 - downloading 69, 159

- device driver, SMBus (*continued*)
 - source RPM file 69, 159
- device drivers, updating 13
- DHCP server 81
- Diffie-Hellman key exchange 34
- Digital Signature Algorithm 203
- DirAdmin 33, 106
- diragent.rsp file
 - customizing 68, 158
 - location 68, 158
 - upgrading Agent using Software Distribution 165
- dircon.rsp file
 - customizing 58, 149
 - location 58, 148
- Director
 - compatibility documents xvi
 - database applications, supported 18, 29
 - database, function of 5
 - downloading xv
 - environment (illustration) 4
 - extensions 11
 - hardware requirements 13
 - hardware, supported 4
 - managing systems running Agent 3.x 12
 - network protocols, supported 6
 - operating systems, supported 14
 - publications xiv
 - Redbooks xv
 - security 203
 - software components (illustration) 5
 - terminology 211
 - upgrading from earlier versions 11
 - Web site xv
- Director Agent
 - See Agent
- Director Console
 - See Console
- Director Server
 - See Server
- dirinstall script
 - Agent 70, 160
 - Console 59, 150
 - Server 51, 143
 - upgrading Agent using Software Distribution 165
- DirSuper 33, 106
- diruns utility 180
- discovery
 - BladeCenter chassis 81
 - broadcast 102
 - broadcast relay 103
 - multicast 103
 - overview 102
 - Remote Supervisor Adapter 27
 - service processors 104
 - setting preferences 103
 - troubleshooting 186, 187
 - unicast 103
- discovery preferences, setting 103
- documentation xiv
- downloading
 - compatibility documents xvi

downloading (*continued*)
hardware compatibility information xvi
IBM Director code xv
IBM Director publications xv
management module firmware 29
Remote Supervisor Adapter firmware 27
SMBus device driver 69, 159
systems-management software xv

E

eFixes
See interim fixes
Electronic Service Agent 11
encryption
algorithms 34
enabling 34
performance penalty 34
troubleshooting 186
Event Action Plan wizard
access to, restricting 108, 111
event action plan, applying 100
event action plan, naming 102
event filters, selecting 98
event substitution variables, using 100
notification method, selecting 99
systems and devices, discovering 101
event actions, troubleshooting 186
extensions
APC PowerChute Extension for IBM Director 11
Application Workload Management (Aurema) 11
Cluster Systems Management 11
Electronic Service Agent 11
Real Time Diagnostics 11
Remote Deployment Manager 10
Scalable Systems Manager 11
Server Plus Pack 8
Software Distribution (Premium Edition) 10
extensions, definition 8

F

Fault Tolerant Management Interface
overview 9
prerequisites 13
file-distribution servers
configuring Director to use 116
considerations 115
setting up 115
firmware
Remote Supervisor Adapter 27
updating 13
FRU information, troubleshooting 194

G

glossary 217

H

hardware compatibility xvi
help files, Web-based Access 8
help, Director resources xv

I

IBM Active PCI Software for Microsoft Windows 9
IBM Director
See Director
IBM Director Agent
See Agent
IBM Director Console
See Console
IBM Director Remote Control Agent
See Remote Control Agent
IBM Director Server
See Server
IBM systems-management software
downloading xv
overview xv
IBM Web sites
Publication Ordering System 199
Redbooks xv
ServerProven xvi, 4
Support xvi
Support Line 200
Systems Management Software xv
xSeries Systems Management xv
illustrations
BladeCenter deployment infrastructure 28
Director environment 4
Director software components 5
important notice xiv
in-band alerts
managed systems running Linux, NetWare, or Open UNIX 7
managed systems running Windows 8
Management Processor Assistant Agent, role of 7
SNMP traps 8
System Health Monitoring, role of 8
in-band communication
definition 22
enabling 23
ISMPs in servers running NetWare or Open UNIX 23
Management Processor Assistant Agent, role of 23
InstallShield wizard
IBM Director Agent 62
IBM Director Console 55
IBM Director Server 39
insufficient disk space, troubleshooting 193
integrated systems management processor
See ISMP
interim fixes xv
interprocess communication, definition 22
inventory errors, troubleshooting 79
inventory, troubleshooting 193, 194
IP address conflicts, troubleshooting 81

ISMP
alert-forwarding strategies 24, 25
ASM interconnect network 25
limitations on in-band communication 23
MPA Agent 7
Netfinity servers 25
out-of-band communication, pathways for 24, 25
xSeries servers 25

J

JDBC driver
DB2 31
Oracle Server 32
PostgreSQL 33

K

keys
files, location of 204
origin of, determining 208
recovering lost keys 208

L

license
IBM Director Agent 6, 18
IBM Director Console 7, 18
IBM Director Server 6, 18
Linux installation
Agent 69, 159
Console 59, 149
modifying
adding a feature 175
installing the Director database 175
overview 174
removing a feature 175
Wake on LAN, enabling 175
Rack Manager installation, completing 121
Server 51, 143
Server Plus Pack extensions 124
uninstalling 180
logical disk drives, troubleshooting 194

M

managed objects, creating
BladeCenter chassis 81
management processor 22, 105
managed systems
definition 3
distribution preferences, configuring 118
hardware requirements 13
installing the Server Plus Pack
manually 123
using Software Distribution task 126
securing
Agent installation, during 65
Agent upgrade, during 155
automatically 205

managed systems (*continued*)
securing (*continued*)
manually 205
methods 205
security 206
troubleshooting
access failure 191
encryption 186
NetWare 6.0 191
performance-monitor information 191
resource-monitor information 191
time zone error 191
management console
definition 4
hardware requirements 13
management module
assigning temporary IP addresses 28
default IP address 28
default user name and password 83
logging in to 87
network protocols, configuring 90
properties, configuring 89
Management Module Network Interfaces window 84
Management Processor Assistant Agent
managed system, installing on 63
management server, installing on 41
overview 7
Management Processor Assistant task
overview 7
troubleshooting 184, 194
management processor object
creating 22, 105
displayed in Console (illustration) 106
naming 105
management server
DB2 database
Linux installation 32
Windows installation 30
definition 3
hardware requirements 13
Rack Manager installation, completing 121
Mass Configuration, troubleshooting 194
MIB file attribute values, troubleshooting 186, 187
Microsoft Data Engine 1.0 30
Microsoft Internet Explorer, troubleshooting 196
Microsoft Jet 4.0
overview 29
size limitations 29
Microsoft Management Console 7, 18
Microsoft SQL Server 30
modifying a Director installation
Linux installation
adding a feature 175
installing the IBM Director database 175
removing a feature 175
Wake on LAN, enabling 175
NetWare installation
adding a feature 176
limitations 176
Open UNIX installation
adding a feature 178

- modifying a Director installation (*continued*)
 - Open UNIX installation (*continued*)
 - removing a feature 179
 - Wake on LAN, enabling 178
 - Windows installation
 - adding a feature 173
 - installing the IBM Director database 173
 - Program Maintenance window 174
 - removing a feature 173
- MPA
 - See Management Processor Assistant
- multicast discovery 103

N

- Netscape Navigator, troubleshooting 195, 196
- NetWare installation
 - Agent 71
 - limitations on in-band communication 23
 - modifying
 - adding a feature 176
 - limitations 176
 - Server Plus Pack extensions 125
 - uninstalling 181
- network protocols 16
- New Scheduled Job window 131, 169
- notices
 - attention xiv
 - important xiv
 - notes xiv

O

- Open UNIX installation
 - Agent installation 74
 - limitations on in-band communication 23
 - modifying
 - adding a feature 178
 - removing a feature 179
 - Wake on LAN, enabling 178
 - uninstalling 181
- operating system compatibility xvi
- optional service processors, configuring 22
- Oracle Server
 - JDBC driver 32
 - overview 32
- out-of-band communication
 - ASM interconnect, role of 24
 - ASM PCI adapter 24, 25
 - ASM processor 24, 25
 - definition 22
 - ISMP 24, 25
 - Remote Supervisor Adapter 24, 25
 - SSM 23

P

- PCI adapter, troubleshooting 194
- performance-monitor data, troubleshooting 191
- planning considerations 21
- policies, deployment 85

- ports 16
- PostgreSQL
 - JDBC driver 33
 - overview 33
- problem solving 183
- profiles (BladeCenter Deployment wizard)
 - changing name of 95
 - displayed in Console (illustration) 96
 - overview 85
- publications xiv

R

- Rack Manager
 - completing installation on management server
 - Linux 121
 - Windows 121
 - management console, installing on 57
 - management server, installing on 42
 - overview 9
 - supported operating systems 15
- RAID arrays, monitoring and managing 7
- Real Time Diagnostics 11
- Redbooks xv
- Remote Control Agent
 - managed system, installing on 63
 - management server, installing on 41
 - overview 7
- Remote Control, troubleshooting 194
- Remote Deployment Manager
 - BladeCenter deployment infrastructure 29
 - installing operating systems on blade servers 79
 - overview 10
- Remote Supervisor Adapter
 - alert-forwarding strategies 24, 25
 - ASM interconnect network 25
 - configuring 105
 - discovery 27
 - firmware levels 24, 25
 - Management Processor Assistant 7
 - management processor object, creating 105
 - Netfinity servers 25
 - out-of-band communication, pathways for 24, 25
 - updating firmware 27
 - use as an ASM interconnect gateway 23
 - xSeries servers 25
- resource-monitor information, troubleshooting 191
- response files
 - See diragent.rsp file, dircon.rsp file, and dirinstall script
- RS-485 ports 23
- RXE-100 Remote Expansion Enclosures
 - configuring using SSM 11
 - use with xSeries 360 or 440 servers 23

S

- Scalable Systems Manager
 - See SSM
- secure socket layers
 - cipher suites 33

- secure socket layers *(continued)*
 - enabling 112
 - overview 33
 - restricting sessions 112
- security
 - Agent-Server authentication 203
 - BladeCenter deployment infrastructure 28
 - Digital Signature Algorithm 203
 - encryption
 - algorithms 34
 - enabling 34
 - overview 34
 - performance penalty 35
 - key management
 - location of files 204
 - origin of a key, determining 208
 - overview 208
 - public and private keys 204
 - recovering lost keys 208
 - managed system
 - accessing a secured system 206
 - removing access to 207
 - securing automatically 205
 - securing manually 205
 - management server, adding another 208
 - overview 33
 - secure socket layers
 - cipher suites 33
 - enabling 112
 - overview 33
 - restricting sessions 112
 - user administration
 - default profile, creating 107
 - editing user privileges 108
 - Event Action Plan wizard, restricting access to 108, 111
 - group access, restricting 110
 - task access, restricting 111
 - user login 106
 - Web-based Access
 - custom access policy, configuring 113
 - overview 35
- Server
 - function 5
 - hardware requirements 13
 - Inventory, troubleshooting 193
 - license 6, 18
 - Linux, installing on
 - database, configuring 52, 53
 - encryption, enabling 53, 144
 - modifying an installation
 - Linux 174
 - Windows 173
 - network protocols 16
 - supported operating systems 5, 14
 - troubleshooting
 - BladeCenter unit 186
 - event log error 192
 - installing 183
 - Microsoft Jet 185
 - Oracle Server 185
- Server *(continued)*
 - troubleshooting *(continued)*
 - starting 187, 192
 - Telnet 185
 - unexpected shut down 187
 - uninstalling
 - Linux 180
 - Windows 179
 - upgrading
 - encryption settings 140
 - features, selecting 137
 - network driver, configuring 142
 - Oracle JDBC driver 135
 - Server Plus Pack 138
 - software-distribution settings 140
 - Wake on LAN, enabling 142
 - upgrading on Linux 142
 - Windows, installing on
 - database configuration 47
 - encryption settings 44
 - features, selecting 41
 - network driver, configuring 46
 - Server Plus Pack 42
 - service account 39
 - Software Distribution settings 44
 - Wake on LAN, enabling 46
 - Server Plus Pack
 - installation 8
 - managed systems, installing on manually 123
 - using Software Distribution task 126
 - operating systems, supported 15
 - overview 8
 - purchasing 9
 - ServeRAID Manager 7
 - managed system, installing on 63
 - management console, installing on 56
 - management server, installing on 41
 - overview 7
 - ServerProven Web site 4
 - service account
 - creating 33
 - definition 33
 - Service Location Protocol 81
 - Service Pack 1 for Windows XP 18
 - service packs xv
 - service processors
 - See also* ASM processor, ASM PCI Adapter, ISMP, and Remote Supervisor Adapter
 - alert-forwarding strategies 24
 - ASM interconnect 25
 - communicating with Director Server
 - in-band 7
 - interprocess communication 22
 - out-of-band 24
 - over the ASM interconnect 22
 - over the LAN 22
 - configuring 22
 - discovery of 104
 - identifying 22
 - in-band alerts 7

- service processors (*continued*)
 - in-band communication
 - Management Processor Assistant Agent, role of 23
 - operating system 23
 - service processor type 23
 - management processor object, creating 105
 - managing 7
 - Netfinity servers 25
 - xSeries servers 25
- silent installations
 - See unattended installations
- silent parameter 59, 68
- Slot Manager
 - overview 9
 - troubleshooting 131
- SMBIOS 13
- SMBus device driver
 - binary RPM file 69, 159
 - building and installing 69, 159
 - downloading 69, 159
 - source RPM file 69, 159
- SNMP Access and Trap Forwarding
 - managed system, installing on 63
 - management server, installing on 41
 - overview 8
- SNMP device
 - definition 3
 - troubleshooting 186, 187
- SNMP traps, troubleshooting 187
- software distribution
 - methods
 - redirected distribution 114
 - streaming from management server 114
 - overview 113
 - preferences, configuring 117
 - Server Plus Pack, installing
 - creating a software package 127
 - installing a software package 130
 - overview 126
 - XML files, location of 126
 - troubleshooting
 - file-distribution server 195
 - package creation 194
 - package installation 195
 - redirected share 195
 - Remote Control 194
 - upgrading Agent
 - overview 165
 - software package, installing 169
- Software Distribution (Premium Edition)
 - installing on the management server
 - Linux 123
 - Windows 122
 - overview 10, 114
- software packages
 - creating 165
 - displayed in Console (illustration) 130, 169
- Software Rejuvenation
 - managed systems, installing on 121
 - management console, installing on 57

- Software Rejuvenation (*continued*)
 - management server, installing on 42
 - overview 10
 - supported operating systems 15
- solving problems 183
- SQL Server 2000 Desktop Engine 30
- SSM
 - IP addresses 23
 - out-of-band communication 23
 - overview 11
- support telephone numbers 200
- switch modules
 - external ports, configuring 93
 - network protocols, configuring 93
 - user name and password, changing 92
- System Availability
 - managed systems, installing on 121
 - management console, installing on 57
 - management server, installing on 42
 - overview 10
 - supported operating systems 15
- System Health Monitoring
 - managed system, installing on 63
 - overview 8
 - uninstalling 173

T

- telephone numbers, IBM support 200
- temperature thresholds, loss of 135
- terminology
 - ASM interconnect network 23
 - database server 29
 - Director 211
 - extensions 8
 - in-band communication 22
 - interprocess communication 22
 - managed system 3
 - management console 4
 - management server 3
 - out-of-band communication 22
 - service account 33
 - SNMP device 3
- trademarks 216
- Triple DES 34
- troubleshooting
 - ACPI servers 193
 - Active PCI Manager 193
 - Agent
 - installing 183
 - starting 191
 - ASF, configuring 193
 - Asset ID 194
 - BladeCenter
 - database 186
 - discovery 186
 - cfgdb utility 185
 - CIM Browser 193
 - Console
 - BladeCenter object not displayed 188
 - dialog boxes 188

troubleshooting (*continued*)

- Console (*continued*)
 - discovered systems not displayed 188
 - event action plans 189
 - installing 183
 - JRE exceptions 189
 - managed system access request denied 189
 - managed system duplicated 190
 - managed system with question mark 190
 - managed systems not displayed 189
 - management server log on failure 190
 - starting 190
- database 185, 186
- dialog boxes 188
- discovery 186, 187
- encryption 186
- event actions 186
- event ID 2003 192
- event log error after restarting 192
- event log full 192
- FRU information 194
- IIS 192
- insufficient disk space 193
- Inventory 193, 194
- logical disk drive 194
- managed systems
 - encryption 186
 - performance-monitor information 191
 - resource-monitor information 191
 - running NetWare 6.0 191
 - unable to access 191
- Management Processor Assistant 184, 194
- Mass Configuration 194
- MIB file attribute value 186, 187
- Microsoft Jet 185
- Oracle Server 185
- performance-monitor data 191
- power off message 193
- Remote Control 194
- resource-monitor information 191
- Server
 - installing 183
 - starting 187, 192
 - unexpected shut down 187
 - uninstalling 185
- SNMP device 186, 187
- SNMP device discovery 187
- SNMP traps 187
- Software Distribution
 - file-distribution server 195
 - package creation 194
 - package installation 195
 - redirected share 195
 - Remote Control 194
- Telnet 185
- temperature thresholds, loss of 135
- time zone error 191
- uninstalling 185
- upgrading 184
- Web-based Access
 - Java security warning 196

troubleshooting (*continued*)

- Web-based Access (*continued*)
 - JVM 196
 - Load All Events 197
 - Netscape Navigator 195, 196
 - starting 196
 - Win32_DiskDrive.Size 193
- TWGshare 115

U

- unattended installations
 - Agent 67, 157
 - Console 58, 148
- unattended parameter 59, 68
- unicast discovery 103
- uninstalling Director
 - Linux 180
 - NetWare 181
 - Open UNIX 181
 - troubleshooting 185
 - Windows 179
- updating
 - BIOS 13
 - device drivers 13
 - firmware 13
 - Remote Supervisor Adapter firmware 27
- upgrading
 - Agent
 - Linux 158
 - NetWare 162
 - Open UNIX 163
 - Windows 151
 - Console
 - Linux 149
 - Windows 145
 - Server
 - Linux 142
 - Windows 135
 - Software Distribution task, using 165
 - temperature thresholds, loss of 135
 - troubleshooting
 - error message 1306 184
 - error message 1921 184
 - error message 1922 184
- upward integration 3
- user accounts
 - DirAdmin and DirSuper 33
 - management server running Linux 33
 - management server running Windows 33
 - service account 33
- user administration 106
 - default profile, creating 107
 - DirAdmin group 106
 - DirSuper group 106
 - editing user privileges 108, 109
 - Event Action Plan wizard, restricting access to 108, 111
 - group access, restricting 110
 - task access, restricting 111
 - User Administration window 107

User Defaults Editor 107

W

Wake on LAN

- enabling on Linux 175
- enabling on Open UNIX 178
- enabling on Windows
 - Agent, installing 67
 - Agent, upgrading 157
 - Server, installing 46
 - Server, upgrading 142

Web browsers 18

Web sites

- Director resources xv
- IBM Redbooks xv
- IBM ServerProven xvi, 4
- IBM Support xvi
- IBM Support Line 200
- IBM Systems Management Software xv
- IBM xSeries Systems Management xv
- Oracle Technology Network 32
- PostgreSQL JDBC drivers 33
- Source for Java Technology 113

Web-based Access

- custom access policy, configuring 113
- help files 8
- managed system, installing on 63
- management server, installing on 41
- overview 7
- security 35
- Service Pack 1 for Windows XP 18
- troubleshooting
 - Java security warning 196
 - JVM 196
 - Load All Events 197
 - Netscape Navigator 195, 196
 - starting 196

Web browsers, supported 18

windows

Agent installation (NetWare)

- Choose destination location 72
- InstallShield Wizard complete 73
- Select Components 73, 162

Agent installation (Windows)

- Feature and destination directory selection 63, 153
- Network driver configuration 66, 156
- Security settings 64, 154
- Software Distribution settings 65, 155
- Web-based Access information 66, 156

Capacity Manager installation (NetWare)

- Choose Destination Location 125
- Start Copying Files 126

Console

- Add BladeCenter Chassis 83
- Add Management Processors 105
- Add Share Name 116, 119
- Director Update Assistant 127, 166
- Discovery Preferences 104
- IBM Director Login 80

windows (continued)

Console (continued)

- IBM Update Package/Root Directory 128, 167
- Managed System Distribution Preferences 118
- New Scheduled Job 131, 169
- Server Preferences 116
- Software Distribution Manager (Premium Edition) 127, 166
- Software Distribution Manager (Standard Edition) 127, 165
- Software Distribution Preferences 117
- User Administration 107
- User Defaults Editor 107

Console installation

- Feature and destination directory selection 56, 146
- Server Plus Pack 56, 146
- Management Module Network Interfaces 84
- Program Maintenance 174

Server installation

- DB2 Universal Database configuration 48
- Director service account information 43
- Encryption settings 44, 140
- Feature and installation directory selection 40, 136
- IBM Director database configuration 47
- IBM Director service account information 139
- Microsoft SQL database configuration 49
- Network driver configuration 46, 141
- Oracle database configuration 49
- Server Plus Pack 40, 136
- Software-distribution settings 44, 140
- Web-based Access information 45, 141

Windows installation

- Agent 61
- Console 55
- modifying
 - adding a feature 173
 - installing the IBM Director database 173
 - overview 173
 - removing a feature 173
- Rack Manager installation, completing 121
- Server 39
- Server Plus Pack extensions 124
- troubleshooting
 - event ID 2003 192
 - event log error 192
 - event log full 192
 - power off message 193
 - Win32_DiskDrive.Size 193
- uninstalling 179

Wired for Management (WfM) specifications 13

wizards

- BladeCenter Deployment 84
- Event Action Plan 97
- InstallShield
 - IBM Director Agent 62
 - IBM Director Console 55
 - IBM Director Server 39



Part Number: 90P2905

Printed in U.S.A.

SC09-P290-50



(1P) P/N: 90P2905

