

IBM Director 4.1



Installation and Configuration Guide

Note: Before using this information and the product it supports, read the general information in Appendix D, “Notices”, on page 195.

First Edition (March 2003)

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

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

Contents

Figures	vii
Tables	xi
Preface	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
Chapter 1. Introducing IBM Director 4.1	1
IBM Director environment	1
IBM Director components	2
IBM Director Server	3
IBM Director Agent	4
IBM Director Console	4
IBM Director Agent features	5
ServeRAID Manager	5
Management Processor Assistant Agent	5
IBM Director Remote Control Agent (Windows only)	5
Web-based Access (Windows only)	5
Web-based Access help files (Windows only)	5
System Health Monitoring (Windows only)	5
SNMP Access and Trap Forwarding	6
Upgrading from previous releases of IBM Director	6
IBM Director extensions	6
IBM Director Server Plus Pack	6
IBM Director Software Distribution (Premium Edition)	8
IBM Remote Deployment Manager 4.10	8
Additional IBM Director extensions	9
Chapter 2. Requirements for installing IBM Director	11
System requirements.	11
Hardware requirements	11
BIOS, device drivers, and firmware	11
Supported operating systems	12
Network requirements	13
Network protocols	13
Ports	13
Web browsers	15
Licensing	15
Database	15
IBM Director security.	16
IBM Director service account (Windows only)	16
IBM Director user accounts	16
IBM Director Console – IBM Director Server security	16
Encryption	17
Web-based Access security	18
Chapter 3. Planning your IBM Director installation	19
General planning considerations	19
Managing service processors	20
Communication between service processors and IBM Director Server.	20

In-band communication and alerts	21
Out-of-band communication and alerts	22
Service processors in IBM Nefinity and xSeries servers	23
Setting up the BladeCenter deployment infrastructure.	25
Database management	26
Microsoft Jet 4.0	26
Microsoft Data Engine 1.0 or SQL Server 2000 Desktop Engine	26
Microsoft SQL Server	26
IBM DB2 Universal Database	27
Oracle Server	29
PostgreSQL	29
Chapter 4. Installing IBM Director Server and IBM Director Console	31
Installing IBM Director Server	31
Installing IBM Director Server on Windows.	31
Installing IBM Director Server on Linux	43
Installing IBM Director Console	45
Installing IBM Director Console on Windows	45
Installing IBM Director Console on Linux	49
Chapter 5. Upgrading IBM Director Server and IBM Director Console	51
Upgrading IBM Director Server	51
Upgrading IBM Director Console	58
Upgrading IBM Director Console using the InstallShield wizard	59
Performing an unattended upgrade of IBM Director Console	62
Chapter 6. Configuring the IBM BladeCenter chassis	65
Starting IBM Director Console	65
Discovering a BladeCenter chassis	66
Automatically discovering the BladeCenter chassis.	67
Manually creating a BladeCenter chassis managed object	68
Manually changing the IP address of the BladeCenter chassis	69
Using the BladeCenter Deployment wizard.	70
Chapter 7. Installing IBM Director Agent	83
Installing IBM Director Agent on Microsoft Windows	83
Installing IBM Director Agent using the InstallShield wizard.	83
Performing an unattended installation of IBM Director Agent	88
Installing IBM Director Agent on Red Hat Linux, SuSE Linux, or VMware ESX	89
Building and installing the IBM Smbus device driver	89
Installing IBM Director Agent	90
Installing IBM Director Agent on NetWare	91
Installing IBM Director Agent on Caldera Open UNIX	94
Chapter 8. Upgrading IBM Director Agent	95
Upgrading IBM Director Agent using standard installation procedures	95
Upgrading IBM Director Agent on Windows	95
Upgrading IBM Director Agent on Red Hat Linux or SuSE Linux	102
Upgrading IBM Director Agent on NetWare	104
Upgrading IBM Director Agent on Caldera Open UNIX	105
Upgrading IBM Director Agent using the Software Distribution task	107
Creating a software package	107
Installing a software package	111
Chapter 9. Configuring IBM Director 4.1	113
Using the Event Action Plan wizard	113

Discovering managed systems, devices, and objects	118
Types of discovery	118
Setting discovery preferences	119
Manually creating a management processor object	120
Authorizing IBM Director users	122
Creating user-account defaults	122
Editing an individual user's access privileges	124
Configuring security settings	127
Enabling SSL	128
Enabling specific cipher suites	128
Configuring a custom access policy for Web-based Access (Windows only)	129
Using software distribution	129
Installing Software Distribution (Premium Edition)	130
Methods of software distribution	131
Setting up file-distribution servers	132
Configuring IBM Director to use a file-distribution server	133
Configuring software-distribution preferences	134
Configuring distribution preferences for managed systems	135
Chapter 10. Installing the IBM Director Server Plus Pack extensions	137
Completing the Rack Manager installation on the management server	137
Completing the Rack Manager installation on Windows	137
Completing the Rack Manager installation on Linux	137
Installing the Server Plus Pack extensions on managed systems	138
Using standard installation procedures	139
Using the IBM Director Software Distribution task (Windows and Linux only)	142
Chapter 11. Modifying and uninstalling IBM Director 4.1	149
Modifying an IBM Director installation	149
Modifying IBM Director running on Windows	149
Modifying IBM Director running on Linux	150
Modifying IBM Director running on NetWare	152
Modifying IBM Director running on Caldera Open UNIX	153
Uninstalling IBM Director	155
Uninstalling IBM Director on Windows	155
Uninstalling IBM Director on Linux	155
Uninstalling IBM Director Agent on NetWare	156
Uninstalling IBM Director on Caldera Open UNIX	156
Chapter 12. IBM Director Agent — IBM Director Server security	157
How authentication works	157
Digital-signature certification	157
Security state of the managed system	157
Where security information is stored	158
How the keys and secin.ini files work together	158
Securing managed systems	159
Automatically securing unsecured systems	159
Manually securing a managed system	159
Changing access or security states	160
Accessing a secure managed system	160
Removing access to a managed system	161
Adding a trusted management server to an existing secure environment	162
Key management	162
Determining the origin of a public or private key	162
Recovering lost public and private key files	162

Chapter 13. Solving IBM Director problems	165
Appendix A. Terminology summary and abbreviation list	175
IBM Director terminology summary	175
Abbreviation and acronym list	175
Appendix B. Creating custom database tables for CIM, DMI, and MIF	
inventory data	179
Creating table property files	179
Creating inventory extension property files	184
Creating translated strings files	186
Initializing custom tables	188
Changing custom tables	189
Generating MIF files for inventory collection	191
Creating the mifgen.ini file	191
Troubleshooting MIF file generation	192
Appendix C. Getting help and technical assistance	193
Before you call	193
Using the documentation	193
Getting help and information from the World Wide Web	193
Software service and support	194
Appendix D. Notices	195
Edition notice	195
Trademarks.	196
Index	197
Glossary	207

Figures

1. Hardware in an IBM Director environment	2
2. Software in an IBM Director environment	3
3. Example of a BladeCenter deployment network	25
4. Installing IBM Director Server on Windows: Server Plus Pack window	32
5. Installing IBM Director Server on Windows: “Feature and installation directory selection” window	32
6. Installing IBM Director Server on Windows: “Features and installation directory selection” window	33
7. Installing IBM Director Server on Windows: Installing the Server Plus Pack	34
8. Installing IBM Director Server on Windows: “IBM Director service account information” window	35
9. Installing IBM Director Server on Windows: “Encryption settings” window	36
10. Installing IBM Director Server on Windows: “Software-distribution settings” window	36
11. Installing IBM Director Server on Windows: “Web-based Access information” window	37
12. Installing IBM Director Server on Windows: “Network driver configuration” window	38
13. Installing IBM Director Server: “IBM Director database configuration” window	39
14. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window	40
15. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window	40
16. Installing IBM Director Server: “IBM Director Microsoft SQL Server database configuration” window	41
17. Installing IBM Director Server: “IBM Director Oracle database configuration” window	41
18. Installing IBM Director Server: “IBM Director Oracle database configuration” window	42
19. Installing IBM Director Console: Server Plus Pack window	46
20. Installing IBM Director Console: “Feature and destination directory selection” window	46
21. Installing IBM Director Console: Installing ServeRAID Manager	47
22. Installing IBM Director Console: Installing the Server Plus Pack	48
23. Upgrading IBM Director Server on Windows: Server Plus Pack window	52
24. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window	52
25. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window	53
26. Upgrading IBM Director Server on Windows: Installing the Server Plus Pack	54
27. Upgrading IBM Director Server on Windows: “IBM Director service account information” window	55
28. Installing IBM Director Server on Windows: “Encryption settings” window	56
29. Upgrading IBM Director Server on Windows: “Software-distribution settings” window	56
30. Upgrading IBM Director Server on Windows: “Web-based Access information” window	57
31. Upgrading IBM Director Server on Windows: “Network driver configuration” window	57
32. Installing IBM Director Console: Server Plus Pack window	60
33. Installing IBM Director Console: “Feature and destination directory selection” window	60
34. Installing IBM Director Console: Installing ServeRAID Manager	61
35. Installing IBM Director Console: Installing the Server Plus Pack	62
36. IBM Director Login window	65
37. IBM Director Console window	66
38. BladeCenter chassis managed object displayed in the Group Contents pane	68
39. Add BladeCenter Chassis window	68
40. Management Module Network Interfaces window	70
41. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window	71
42. BladeCenter Deployment wizard: “Login to the BladeCenter management module” window	72
43. BladeCenter Deployment wizard: “Change the user name and password for the management module” window	73
44. BladeCenter Deployment wizard: “Configure the management module properties” window	74
45. BladeCenter Deployment wizard: “Configure the management module protocols” window	75
46. BladeCenter Deployment wizard: “Configure the IP settings” window	76
47. BladeCenter Deployment wizard: “Change the user name and password for switch modules” window	77
48. BladeCenter Deployment wizard: “Configure the switch module” window	78
49. BladeCenter Deployment wizard: “Deploy operating systems on the blade servers” window	79
50. BladeCenter Deployment wizard: “Configure the deployment policies” window	79

51. BladeCenter Deployment wizard: “Setup summary” window	80
52. IBM Director Console Tasks pane: Deployment Wizard profile	81
53. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window	84
54. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window	85
55. Installing IBM Director Agent on Windows: “Security settings” window	85
56. Installing IBM Director Agent on Windows: “Software Distribution settings” window	86
57. Installing IBM Director Agent on Windows: “Web-based Access information” window	87
58. Installing IBM Director Agent on Windows: “Network driver configuration” window	87
59. Installing IBM Director Agent on NetWare: “Choose destination location” window	92
60. Installing IBM Director Agent on NetWare: Select Components window	92
61. Installing IBM Director Agent on NetWare: “InstallShield Wizard complete” window	93
62. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window	96
63. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window	97
64. Upgrading IBM Director Agent on Windows: “Security settings” window	98
65. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window	99
66. Upgrading IBM Director Agent on Windows: “Web-based Access information” window	99
67. Upgrading IBM Director Agent on Windows: “Network driver configuration” window	100
68. Upgrading IBM Director Agent on NetWare: Select Components window	105
69. Creating a software package: Software Distribution Manager window	107
70. Creating a software package: Software Distribution Manager window (Premium Edition)	108
71. Creating a software package: Director Update Assistant window	108
72. Creating a software package: IBM Update Package/Root Directory Location window	109
73. Creating a software package: IBM Update Package/Root Directory Location window	109
74. Creating a software package: Director Update Assistant window	110
75. Creating software packages: Director Update Assistant window	110
76. All Software Distributions Packages: IBM Director Agent Upgrade	111
77. Scheduling the installation of a software package: New Scheduled Job window	111
78. Event Action Plan wizard: “Welcome to the Event Action Plan wizard” window	113
79. Event Action Plan wizard: “Select the event filters” window	114
80. Event Action Plan wizard: “Select the notification” window	115
81. Event Action Plan wizard: “Apply the event action plan” window	116
82. Event Action Plan wizard: “Discover all systems and devices” window	117
83. Event Action Plan wizard: “Review your selection summary” window	118
84. Discovery Preferences window	120
85. Add Management Processors window	121
86. Management processor object displayed in the Group Contents pane	122
87. User Administration window	123
88. User Defaults Editor window	123
89. User Administration window	124
90. User Editor window: User Properties page	124
91. User Editor window: Privileges page	125
92. User Editor window: Group Access page	126
93. User Editor window: Task Access page	127
94. IBM Director Console: Add Share Name window	133
95. IBM Director Console: Software Distribution Preferences window	134
96. IBM Director Console: Managed System Distribution Preferences window	135
97. IBM Director Console: Add Share Name window	136
98. Installing Capacity Manager on NetWare: Choose Destination Location window	141
99. Installing Capacity Manager on NetWare: Start Copying Files window	141
100. Creating a software package: Software Distribution Manager window (Standard Edition)	142
101. Creating a software package: Software Distribution Manager window (Premium Edition)	143
102. Creating a software package: Director Update Assistant window	143
103. Creating a software package: IBM Update Package/Root Directory Location window	144
104. Creating a software package: IBM Update Package/Root Directory Location window	144
105. Creating a software package: Director Update Assistant window	145
106. Creating software packages: Director Update Assistant window	145

107. Creating software packages: Director Update Assistant window	145
108. All Software Distributions Packages: IBM Director Server Plus Pack	146
109. Scheduling the installation of a software package: New Scheduled Job window	147
110. Program Maintenance window	150
111. Modifying IBM Director Agent on NetWare: "Choose destination location" window	152
112. Modifying IBM Director Agent on NetWare: Select Components window	153
113. Request Access to Systems window	161

Tables

1. Minimum hardware requirements for IBM Director	11
2. Network adapter drivers necessary to run the Fault Tolerant Management Interface	12
3. Supported operating systems for Server Plus Pack extensions installed on managed systems	13
4. Supported network protocols	13
5. Ports used by IBM Director	14
6. In-band communication between service processors and IBM Director Server	21
7. IBM Director Agent features that handle in-band communication and alerts	21
8. Out-of-band communication pathways and alert-forwarding strategies	22
9. Whether service processors connected over LAN to IBM Director Server can communicate with service processors on the ASM interconnect.	23
10. Service processors in IBM Netfinity and xSeries systems	23
11. Supported operating systems for Server Plus Pack extensions installed on managed systems	138
12. Abbreviations and acronyms used in IBM Director	175
13. Table property file properties	181
14. Inventory extension property file properties	185
15. Property mappings.	185
16. Example translated strings files	188
17. Table properties that can be changed.	189

Preface

This book provides information needed to install and configure IBM® Director 4.1. In addition to an overview of IBM Director 4.1 and its requirements, it covers the following topics:

- Planning an IBM Director 4.1 environment
- Installing IBM Director 4.1 and IBM Director extensions
- Upgrading from IBM Director 3.x to IBM Director 4.1
- Configuring IBM Director 4.1

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

Chapter 2, “Requirements for installing IBM Director”, on page 11 contains basic information about IBM Director 4.1. 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 19 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 and IBM Director Console”, on page 31 contains instructions for installing IBM Director Server and IBM Director Console.

Chapter 5, “Upgrading IBM Director Server and IBM Director Console”, on page 51 contains instructions for upgrading from IBM Director 3.x to IBM Director 4.1.

Chapter 6, “Configuring the IBM BladeCenter chassis”, on page 65 contains information about starting IBM Director Console, discovering the BladeCenter chassis, and running the BladeCenter Deployment wizard.

Chapter 7, “Installing IBM Director Agent”, on page 83 contains instructions for installing IBM Director Agent.

Chapter 8, “Upgrading IBM Director Agent”, on page 95 contains instructions for upgrading from IBM Director 3.x to IBM Director 4.1.

Chapter 9, “Configuring IBM Director 4.1”, on page 113 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 10, “Installing the IBM Director Server Plus Pack extensions”, on page 137 contains instructions for installing the IBM Director Server Plus Pack extensions.

Chapter 11, “Modifying and uninstalling IBM Director 4.1”, on page 149 contains information about modifying or uninstalling IBM Director.

Chapter 12, “IBM Director Agent — IBM Director Server security”, on page 157 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.

Chapter 13, “Solving IBM Director problems”, on page 165 lists solutions to problems you might encounter with IBM Director.

Appendix A, “Terminology summary and abbreviation list”, on page 175 contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

Appendix B, “Creating custom database tables for CIM, DMI, and MIF inventory data”, on page 179 contains information about creating custom database tables to accommodate inventory data collected through Common Information Model (CIM), Desktop Management Interface (DMI), and static Management Information Format (MIF) files.

Appendix C, “Getting help and technical assistance”, on page 193 contains information about accessing IBM Director Support Web sites for help and technical assistance.

Appendix D, “Notices”, on page 195 contains product notices and trademarks.

The “Glossary” on page 207 provides definitions for terms used in IBM Director publications.

Notices that are used in this book

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

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

IBM Director publications

The following publications are available in Portable Document Format (PDF) on the *IBM Director* CD in the docs directory:

- *IBM Director 4.1 Installation and Configuration Guide* (dir41_install.pdf)
- *IBM Director 4.1 Systems Management Guide* (dir41_sysmgt.pdf)

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

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

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

- *Remote Supervisor Adapter, User's Guide*
- *Remote Supervisor Adapter, Installation Guide*
- *Remote Supervisor Adapter II, User's Guide*
- *Remote Supervisor Adapter II, Installation Guide*

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

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

- *Implementing Systems Management Solutions using IBM Director* (SG24-6188-01)
- *IBM @server BladeCenter Systems Management* (REDP3582)
- *The Cutting Edge: IBM @server BladeCenter* (REDP3581)
- *IBM @server BladeCenter Type 8677 Planning and Installation Guide* (SG24-6196-00)
- *IBM @server xSeries 440 Planning and Installation Guide* (SG24-6196-00)
- *Server Consolidation with the IBM @server xSeries 440 and VMware ESX Server* (SG24-6852-00)
- *Managing IBM TotalStorage NAS with IBM Director* (SG24-6830-00)
- *IBM Director Security* (REDPO417)
- *Integrating IBM Director with Enterprise Management Solutions* (SG24-5388-01)
- *Using Active PCI Manager* (REDP0446)
- *Implementing Asset ID* (SG 24-6165-00)

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

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

IBM Director resources on the World Wide Web

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

IBM Online Assistant and e-Mail

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

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

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

IBM Universal Manageability Discussion Forum

<http://www7.pc.ibm.com/~ums/>

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

IBM Systems Management Software: Download/Electronic Support page

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

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.

Systems Management - Quick Reference Guide

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

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

IBM Universal Manageability page

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

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

IBM ServerProven® page

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

This Web page provides information about IBM hardware compatibility with IBM Director 4.1, as well as operating system support.

IBM Support page

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

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

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

Chapter 1. Introducing IBM Director 4.1

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

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

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

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

IBM Director environment

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

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

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

Figure 1 shows the hardware in an IBM Director environment.

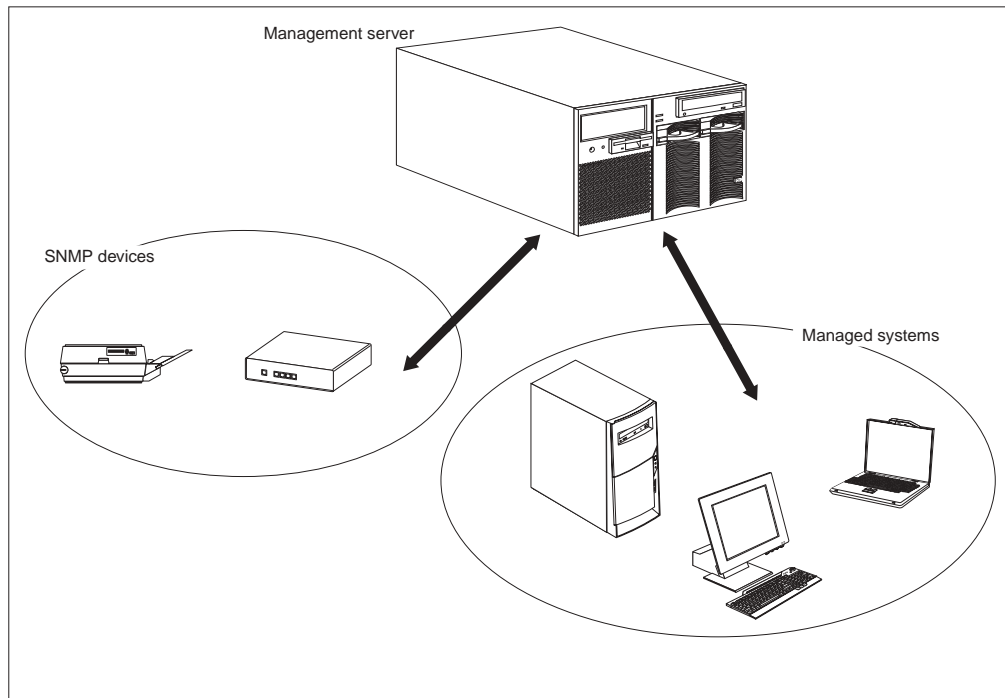


Figure 1. Hardware in an IBM Director environment

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

IBM Director components

The IBM Director software has three components:

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

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

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

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

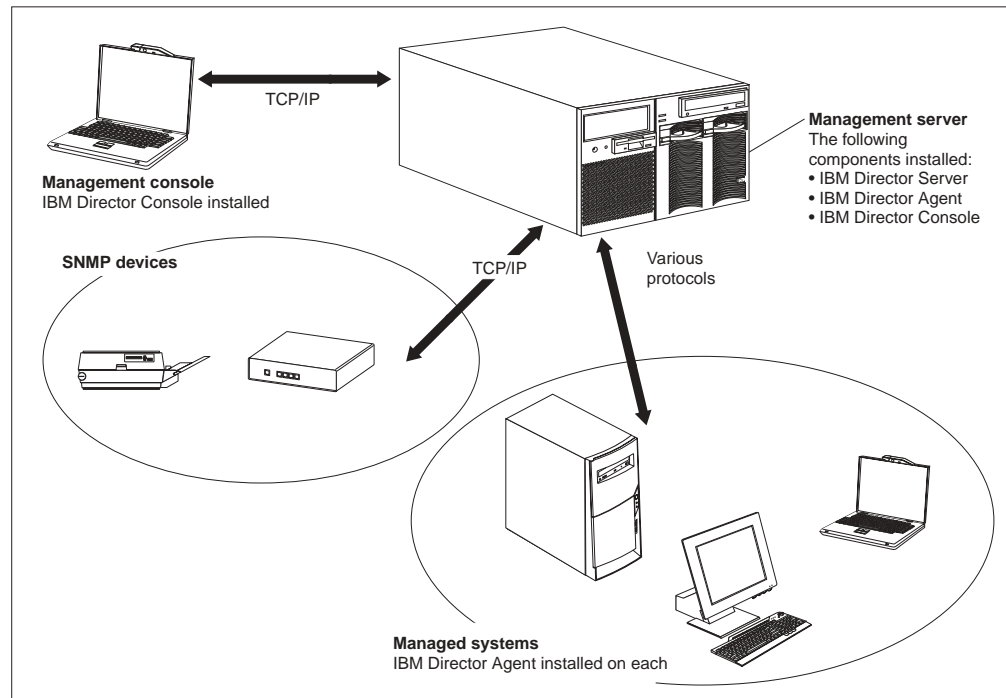


Figure 2. Software in an IBM Director environment

IBM Director Server

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

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

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

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

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

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

IBM Director Agent

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

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

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

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

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

IBM Director Console

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

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

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

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

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

IBM Director Agent features

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

ServeRAID Manager

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

Management Processor Assistant Agent

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

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

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

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

IBM Director Remote Control Agent (Windows only)

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

Web-based Access (Windows only)

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

Web-based Access help files (Windows only)

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

System Health Monitoring (Windows only)

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

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

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

SNMP Access and Trap Forwarding

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

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

Upgrading from previous releases of IBM Director

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

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

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

IBM Director extensions

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

IBM Director Server Plus Pack

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

- Active[™] PCI Manager
- Capacity Manager
- Rack Manager

- Software Rejuvenation
- System Availability

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

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

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

The *IBM Director Server Plus Pack* CD is offered 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, and 440 servers, as well as the RXE-100 Remote Expansion Enclosure.

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

Notes:

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

Capacity Manager

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

Rack Manager

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

Software Rejuvenation

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

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

System Availability

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

IBM Director Software Distribution (Premium Edition)

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

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

IBM Remote Deployment Manager 4.10

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

- Update system firmware
- Modify configuration settings
- Install operating systems

- Back up and recover primary partitions
- Securely erase data from disks

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

Additional IBM Director extensions

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

Real Time Diagnostics

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

Cluster Systems Management

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

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

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

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

APC PowerChute Extension for IBM Director

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

Electronic Service Agent

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

Application Workload Management (Aurema)

Manages how multiple applications use server resources.

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

Chapter 2. 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 security features in IBM Director 4.1.

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, device drivers, and firmware to the latest version 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 appropriate driver installed. The following table lists the minimum version of supported drivers for each network adapter.

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

Manufacturer	Version
Intel	8.0
3Com	2.3
Broadcom	6.6.7

Ensure that the managed system has the supported version or later of the driver installed.

Supported operating systems

The IBM Director software components and extensions have different levels of operating-system support.

Note: For the most recent list of supported operating systems, see *Compatibility Documents for IBM Director 4.1*. You can download this PDF file from http://www.ibm.com/pc/ww/eserver/xseries/systems_management/nfdir/agent.html. It is updated every 6 to 8 weeks.

IBM Director Server

IBM Director Server is supported on the following operating systems:

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

IBM Director Agent

IBM Director Agent is supported on the following operating systems:

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

IBM Director Console

IBM Director Console is supported on the following operating systems:

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

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 are supported. (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 2000 Server, Advanced Server, and Datacenter Server	<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 Linux Advanced Server, version 2.1 SuSE Linux, versions 7.2, 7.3, and 8.0	<ul style="list-style-type: none"> • Capacity Manager • Software Rejuvenation • System Availability
NetWare 6.0	Capacity Manager
VMware ESX Server 1.5.2	<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 what IBM Director services are installed (such as Web-based Access or IBM Director Remote Control Agent), IBM Director needs certain ports free 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	
	Telnet to service processor	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 Microsoft Internet Explorer on Windows XP, you must install Service Pack 1 for Windows XP.

Licensing

IBM Director 4.1 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 *Compatibility Documents for IBM Director 4.1*. You can download this PDF file from 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 10 (Windows only)
- IBM DB2 Universal Database 7.2, Fix Pack 8
- Oracle Server versions 8.1.7 or 9.0.x
- PostgreSQL, version 7.2 (Linux only)

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

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.

IBM Director security

IBM Director offers several security features, including user-administration options that enable system administrators to carefully tailor 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 diradmin and dirsuper groups are not automatically populated. A user with root privileges must assign users to the appropriate groups.

IBM Director Console – IBM Director Server security

SSL can be used 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 4.1 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 allows 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, while OpenSSL provides ciphers for Windows 2000 and Windows XP.

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 above matrix 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 login to an operating-system account on the local system. Once logged in, user privileges are based on operating-system privileges. Users with Administrator authority can use Web-based Access to modify system settings, while members with User authority can view system settings only.

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.
 - a. Determine the physical location and network address of all servers, computers, and other devices in your network. Identify subnets and whether there are any remote subnets. Identify the communication method you are using; this determines the type of discovery to deploy.
 - b. 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.
 - c. Ensure that all servers, computers, and devices are properly installed and cabled to ensure discovery.
 - d. 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.

You must 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. You must install IBM Director Agent on each managed system so that it can be discovered.
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 across UDP port 14247. This is important to consider when 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 119 for more information.

Managing service processors

To effectively use IBM Director 4.1 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, since 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.

In-band communication and alerts

To enable in-band communication between IBM Director Server and a managed system that contains a server 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 systems 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	Yes	Yes	Yes	Yes
Integrated systems 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 (AMSP)	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	System Health Monitoring	MPA Agent	MPA Agent	MPA Agent

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

Type of service processor	Operating system on managed system			
	Windows	Linux	NetWare	Caldera Open UNIX
Integrated systems 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 what 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)	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	<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
Integrated systems management processor (ISMP)	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 on 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 publications” on page xiv 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				
	ASM processor	ISMP	ASM PCI adapter	Remote Supervisor Adapter	Remote Supervisor Adapter II
ASM PCI adapter	Yes	No	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 use 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	ASM processor	ISMP	ASM PCI Adapter	Remote Supervisor Adapter
Netfinity 1000	No	No	No	No
Netfinity 3000	No	No	No	No
Netfinity 3500 family (3500 /M10/M20)	No	No	No	No
Netfinity 4000R	No	No	No	No
Netfinity 4500R	Standard	No	Optional	No
Netfinity 5000	Standard	No	Optional	No
Netfinity 5100	Standard	No	Optional	No
Netfinity 5500 family (5500, M10, M20)	Standard	No	Optional	No
Netfinity 5600	Standard	No	Optional	No
Netfinity 6000R	Standard	No	Optional	No
Netfinity 7000	No	No	No	No
Netfinity 7000 M10	No	No	Standard	No
Netfinity 7100	Standard	No	Optional	No
Netfinity 7600	Standard	No	Optional	No
Netfinity 8500R	No	No	Standard	No

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

Server	ASM processor	ISMP	ASM PCI Adapter	Remote Supervisor Adapter
xSeries 130 Value Line (8672)	No	No	No	No
xSeries 130 Performance Line (8654)	Standard	No	No	No
xSeries 135 Value Line	No	No	No	No
xSeries 135 Performance Line	Standard	No	No	No
xSeries 150	Standard	No	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	Standard	No	Optional	No
xSeries 232	No	Standard	No	Optional
xSeries 235	No	Standard	No	Optional
xSeries 240	Standard	No	Optional	No
xSeries 250	Standard	No	Optional	No
xSeries 255	No	Standard	No	Optional
xSeries 300	No	No	No	No
xSeries 305	No	No	No	Optional
xSeries 330 (8654)	Standard	No	Optional	Optional
xSeries 330 (8674)	No	Standard	No	Optional
xSeries 330 (8675)	No	Standard	No	Optional
xSeries 335 (8676)	No	Standard	No	Optional
xSeries 340	Standard	No	Optional	No
xSeries 342	No	Standard	No	Optional
xSeries 343	No	No	No	No
xSeries 345	No	Standard	No	Optional
xSeries 350	Standard	No	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	No

Setting up the BladeCenter deployment infrastructure

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.

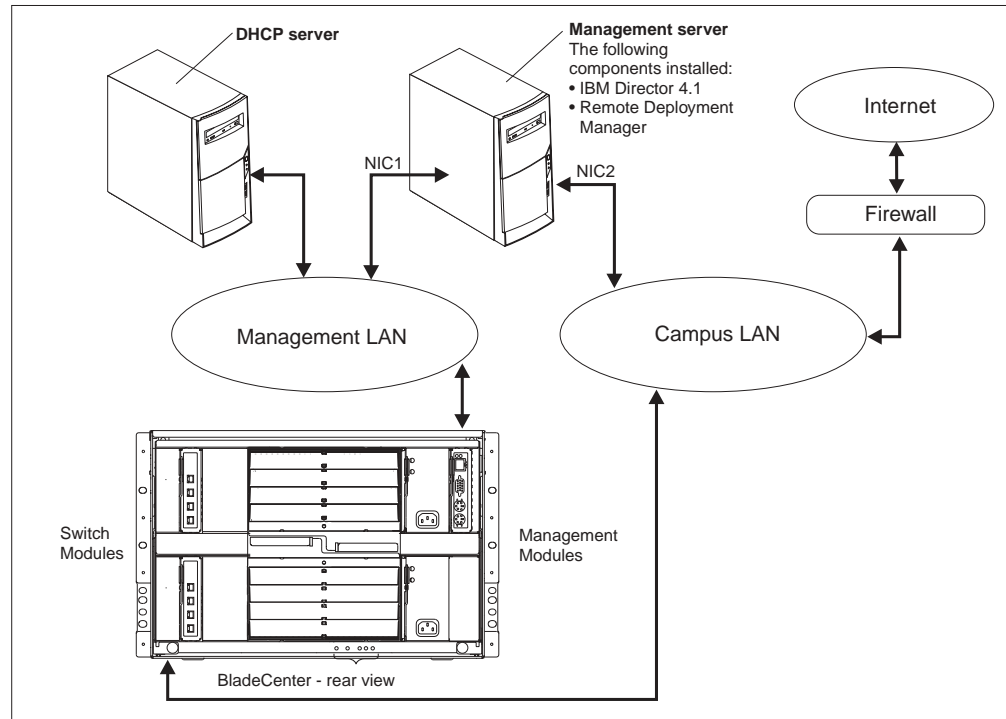


Figure 3. Example of a BladeCenter deployment network

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 LAN 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.

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 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 10 (Windows only)
- IBM DB2 Universal Database 7.2, Fix Pack 8
- Oracle Server versions 8.1.7 or 9.0.x
- PostgreSQL, version 7.2 (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, 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 onto SQL Server.
4. Do one of the following:
 - 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:
 - 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 system administrator who will install IBM Director Server with the host name of the database server and the name of the database.

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 10 	<ul style="list-style-type: none"> • Communications protocols • Applications development interface • Base DB2 client support • System bind files • Fix Pack 8

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
```

Issuing 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 an "Access is denied. The process cannot access the file because it is being used by another process" message 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 onto DB2. See the *DB2 Administration Guide* for additional information about DB2 security.
12. Do one of the following:
 - 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 system administrator who will install IBM Director Server with the host name of the database server and the name of the database.

Configuring a management server running Linux to use DB2

Notes:

1. Verify that you have installed Fix Pack 8. IBM Director 4.1 and DB2 will not run without it.
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. 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. Give root the appropriate DB2 authority.

During the installation of IBM Director Server, you configure settings that enable IBM Director Server to use DB2 as the IBM Director database application.

Oracle Server

Note: IBM Director 4.1 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 c:\oracle\lib\classes12.zip, where c is 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 system administrator who will install IBM Director Server with the following information:
 - 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, a role (TWG_ROLE), and 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.

During the installation of IBM Director Server, you configure settings that enable IBM Director Server to use PostgreSQL as the IBM Director database application.

Chapter 4. Installing IBM Director Server and IBM Director Console

This chapter contains procedures for installing IBM Director Server and IBM Director Console. If you are upgrading from IBM Director 3.x, go to Chapter 5, “Upgrading IBM Director Server and IBM Director Console”, on page 51.

Installing IBM Director Server

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

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

Before you install IBM Director Server, verify that you have performed any necessary preinstallation steps. See “Database management” on page 26 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: Before you install IBM Director Server 4.1, ensure that you have uninstalled any Active PCI Manager components. Earlier versions of Active PCI Manager, such as versions 1.0, 1.1, and 3.1.1, are not compatible with IBM Director 4.1.

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 16.
2. Insert the *IBM Director 4.1* 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.

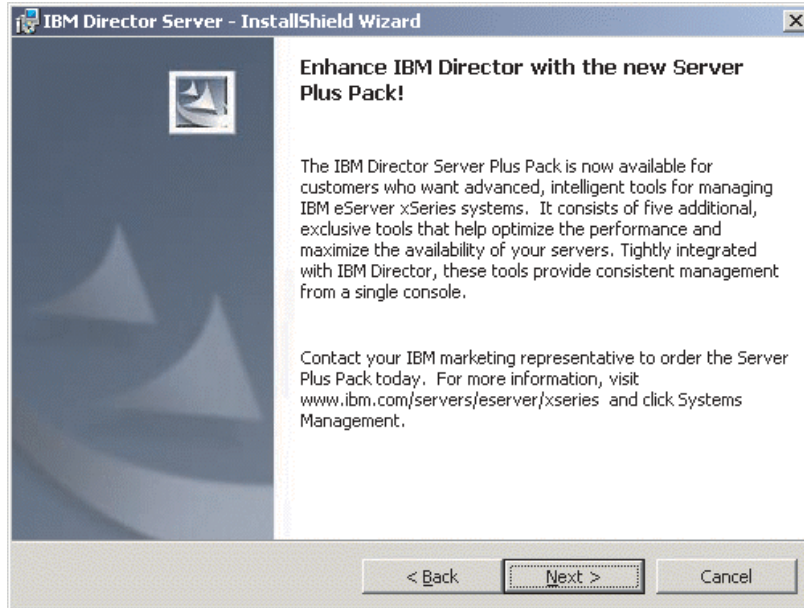


Figure 4. Installing IBM Director Server on Windows: Server Plus Pack window

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

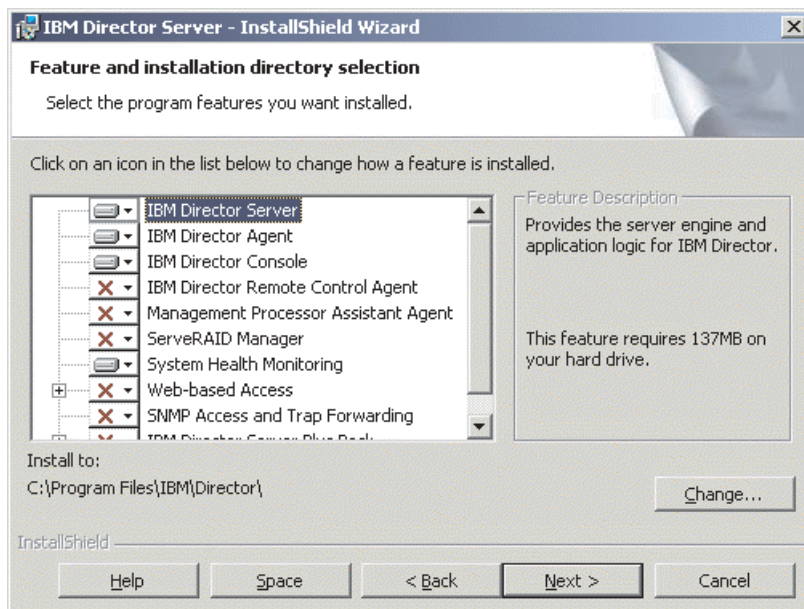




Figure 5. Installing IBM Director Server on Windows: “Feature and installation directory selection” window

10. IBM Director Server, IBM Director Agent, and IBM Director Console are selected automatically for installation; a hard disk 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

Permits 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

Permits 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.

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

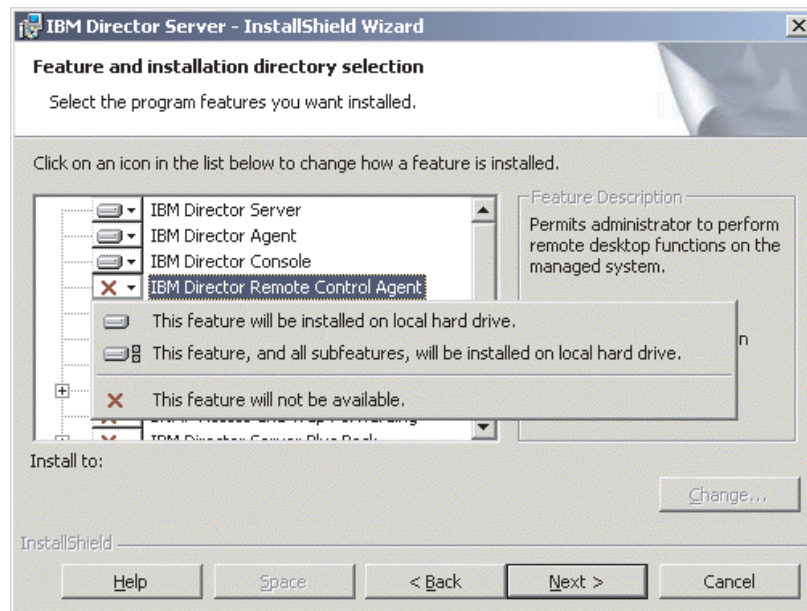


Figure 6. Installing IBM Director Server on Windows: “Features and installation directory selection” window

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. You can install the following Server Plus Pack 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.

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.

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

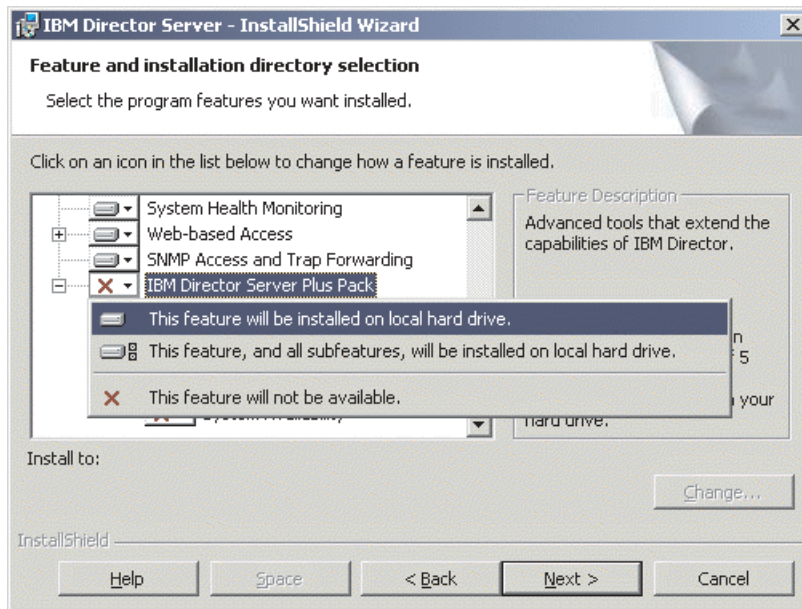
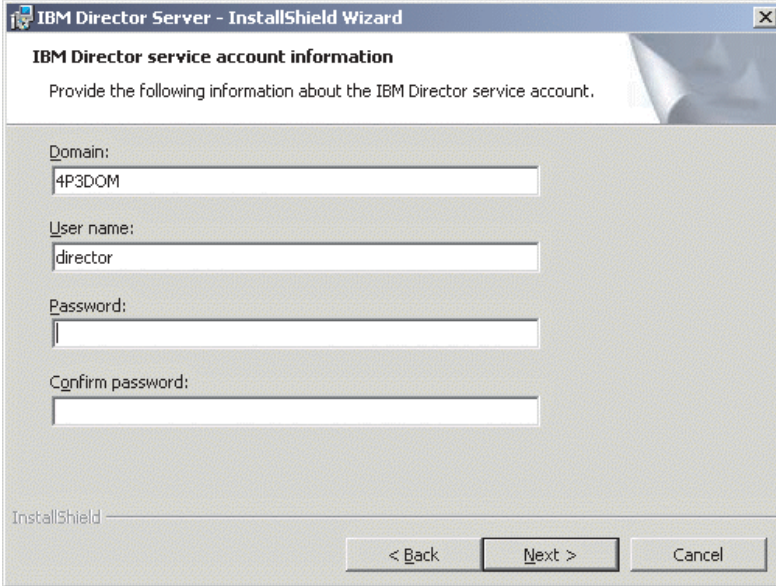


Figure 7. Installing IBM Director Server on Windows: Installing the Server Plus Pack

Otherwise, select the Server Plus Pack extensions individually.

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 16.)



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 are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

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.

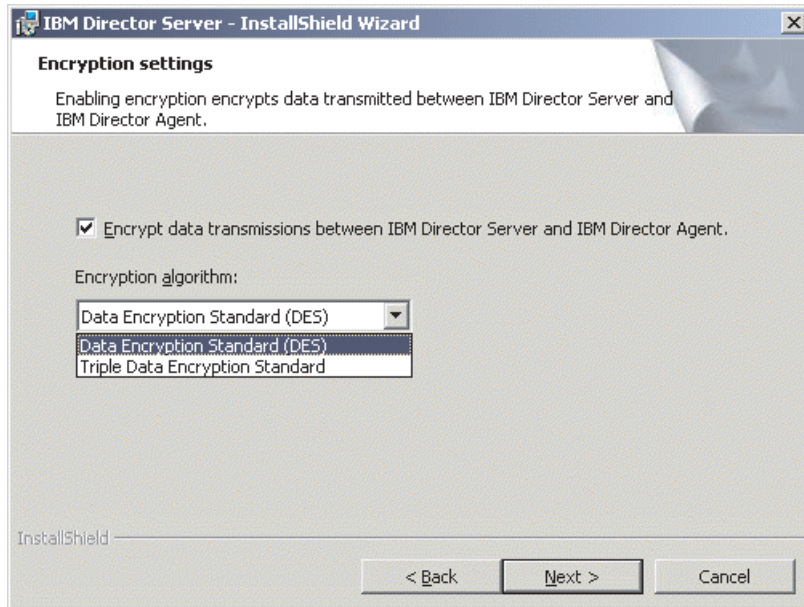


Figure 9. Installing IBM Director Server on Windows: “Encryption settings” window

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.

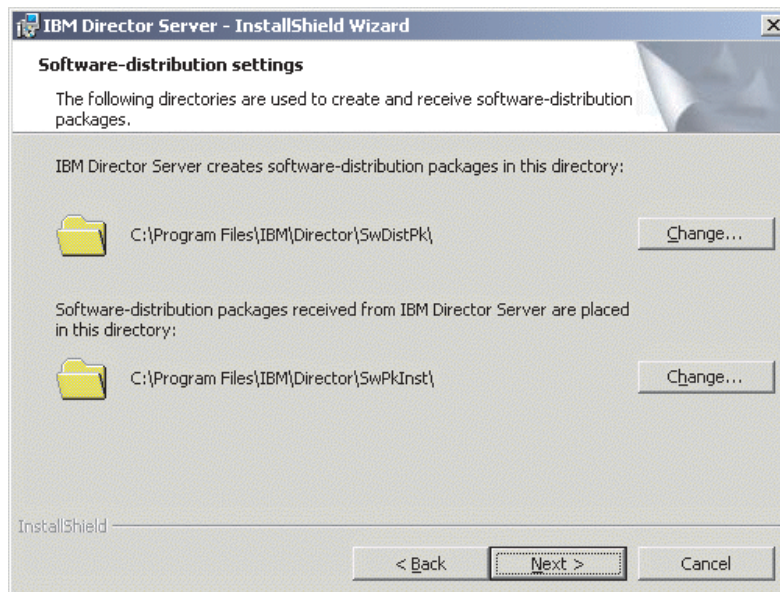


Figure 10. Installing IBM Director Server on Windows: “Software-distribution settings” window

17. To select an alternate location for where IBM Director Server creates software-distribution packages, click **Change** and select another directory. To select an alternate 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 choose 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.

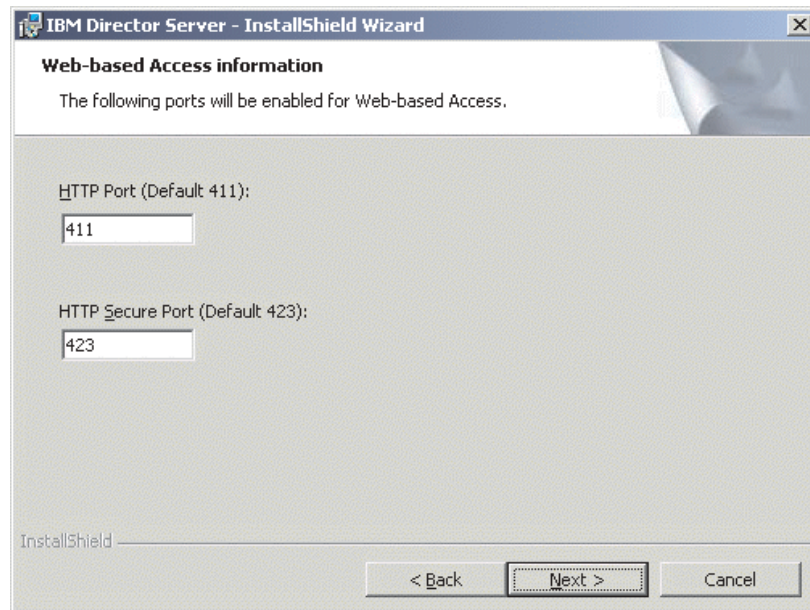


Figure 11. Installing IBM Director Server on Windows: “Web-based Access information” window

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.

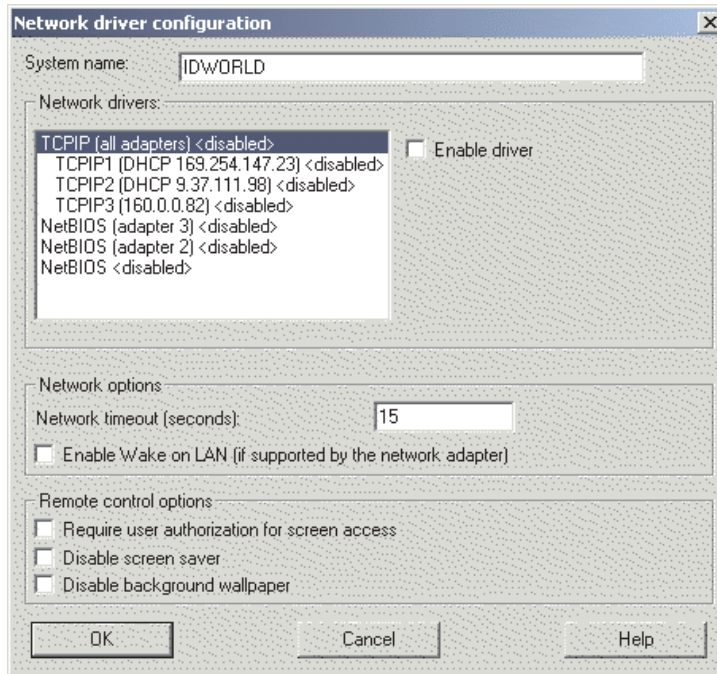


Figure 12. Installing IBM Director Server on Windows: “Network driver configuration” window

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.

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 driver on a system with multiple network adapters, IBM Director Server will receive data packets addressed to the individual adapter *only*.

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.

Select **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.

23. If you chose 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.

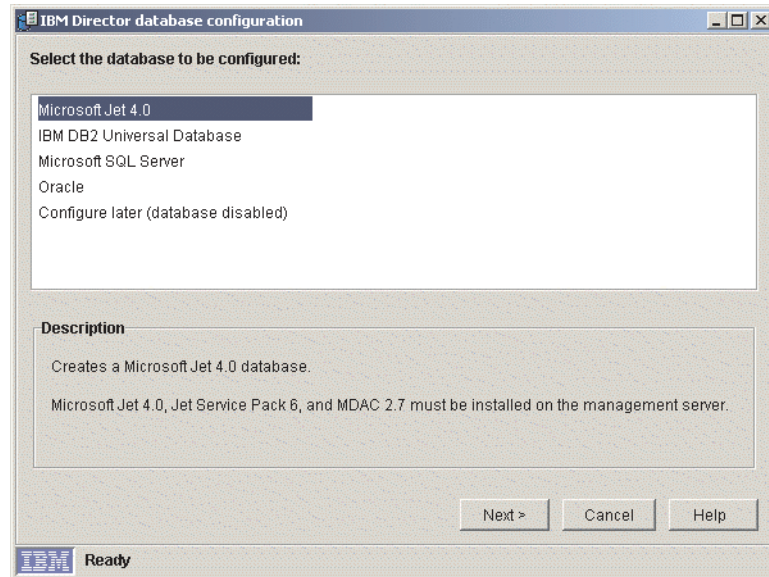


Figure 13. Installing IBM Director Server: “IBM Director database configuration” window

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**. Do one of the following:

If you selected	Go to
Microsoft Jet 4.0	Step 33 on page 43
IBM DB2 Universal Database	Step 27
Microsoft SQL Server	Step 29
Oracle	Step 30 on page 41
Configure later (database disabled)	Step 33 on page 43

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

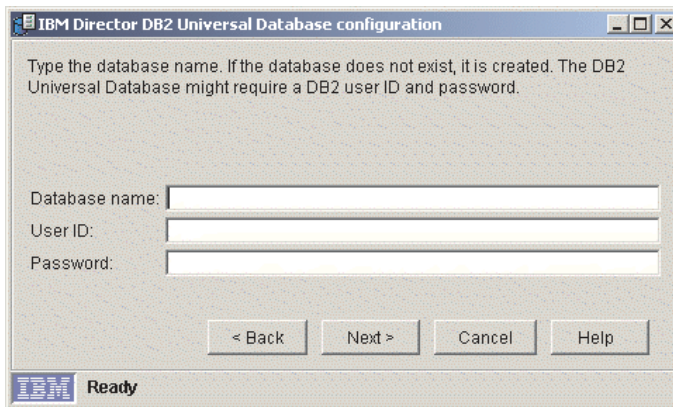


Figure 14. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window

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

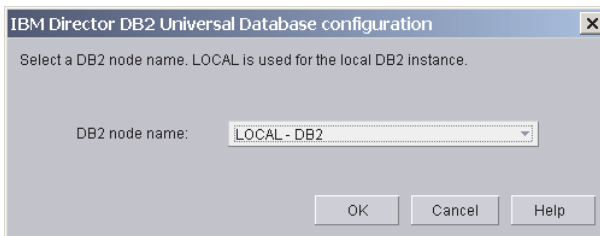


Figure 15. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window

In the **DB2 node name** field, select the location of the DB2 database. Then click **OK** and go to step 33 on page 43.

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

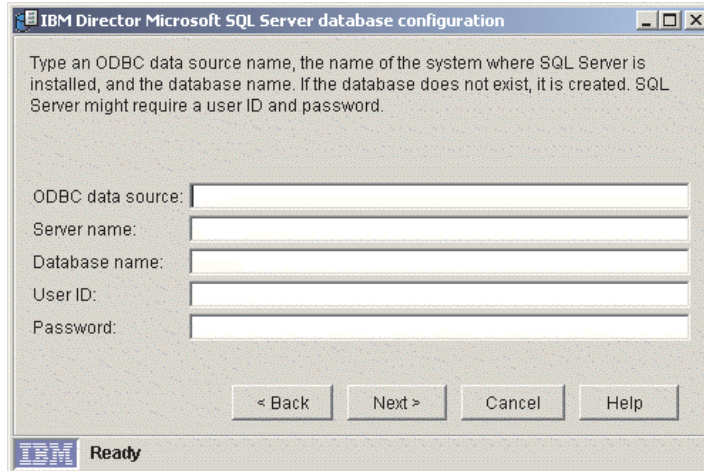


Figure 16. Installing IBM Director Server: “IBM Director Microsoft SQL Server database configuration” window

- 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 33 on page 43.

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

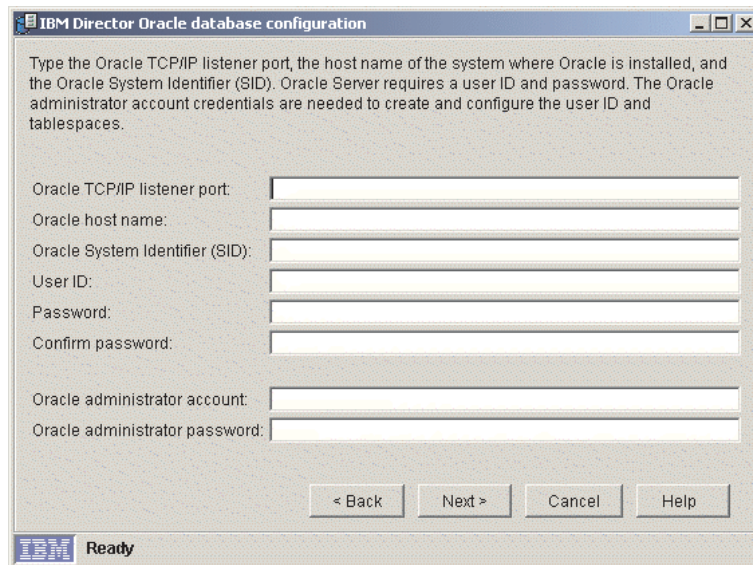


Figure 17. Installing IBM Director Server: “IBM Director Oracle database configuration” window

- 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.

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

32. Type information in the following entry fields:

Tablespace information

- 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.

Temporary tablespace information

- a. In the **Temporary tablespace name** field, type a name for the temporary tablespace.
 - b. 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.
 - c. In the **Temporary tablespace size (MB)** field, type the size of the temporary tablespace in MB.
33. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the InstallShield Wizard Completed window opens.
 34. Click **Finish**. A window opens, asking you if you want to restart the server.
 35. Remove the *IBM Director 4.1* CD from the CD-ROM drive.
 36. Click **Yes** to restart the server.

Installing IBM Director Server on Linux

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

1. Insert the *IBM Director 4.1* 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 44.

6. To customize the installation, 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.

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 choose log file options.

8. Save the modified installation script.

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

where *destinationdirectory* 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

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

```
. /home/db2inst1/sqllib/db2profile
. /home/db2inst1/sqllib/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.
13. (Oracle only) Create a `/etc/TWGserver/setup_env` file. Add the following statement to the file:

```
export CLASSPATH=filename
```

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.
15. (PostgreSQL only) Create a `/etc/TWGserver/setup_env` file. Add the following statement to the file:

```
export CLASSPATH=filename
```

where *filename* is the fully-qualified name of the PostgreSQL JDBC driver, for example, `/opt/postgres/lib/postgresql.jar`.

16. Set the `setup_env` file attributes to read-execute.
17. Using an ASCII text editor, open the `TWGDatabase.TWGExt` file. This file is located in the `opt/IBM/director/classes/extensions` directory. If necessary, edit the `CLASSPATH` statement to read as follows:

```
classpath.append.3=classpath:filename.jar
```

where *filename* is the name of the PostgreSQL JDBC driver file. By default, the `CLASSPATH` statement points to `postgresql.jar`; however, some Linux distributions, such as SuSE 7.3, have changed the name of the PostgreSQL JDBC driver.

18. To configure the database for use with IBM Director, type the following command and press Enter:
`/opt/IBM/director/bin/cfgdb`

Follow the onscreen instructions.

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 4.1* CD from the CD-ROM drive.

Installing IBM Director Console

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

- Windows XP Professional (Service Pack 1 recommended)
- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Professional (Service Pack 3 required)
- Red Hat Linux, version 7.3
- SuSE Linux, 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: Before you install IBM Director Console 4.1, ensure that you have uninstalled any Active PCI Manager components. Earlier versions of Active PCI Manager, such as versions 1.0, 1.1, and 3.1.1, are not compatible with IBM Director 4.1.

Installing IBM Director Console using the InstallShield wizard

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

1. Insert the *IBM Director 4.1* 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.

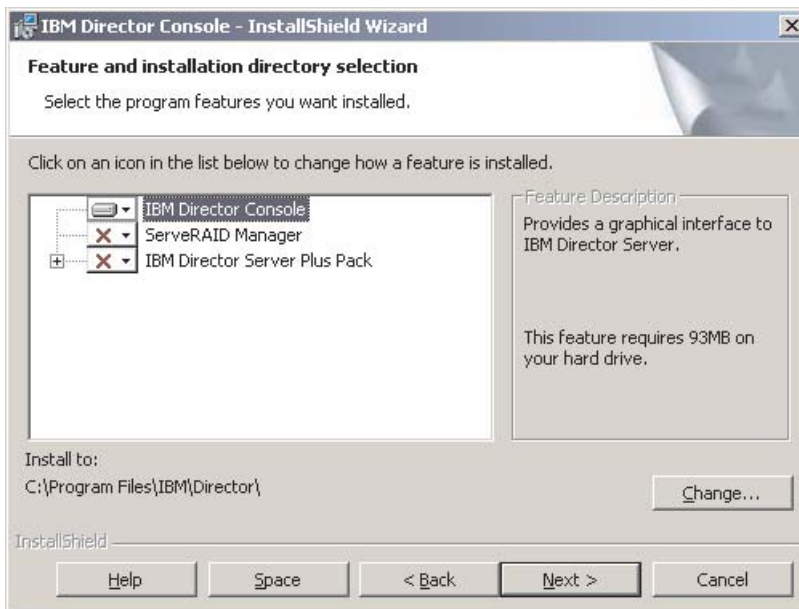





Figure 20. Installing IBM Director Console: "Feature and destination directory selection" window

9. IBM Director Console is selected automatically for installation; a hard disk icon  is displayed to its left.  is displayed to the left of the optional features: ServeRAID Manager and the IBM Director Server Plus Pack. Be sure to install these applications if you want to run them against managed systems.
10. To select ServeRAID Manager, a feature that manages and monitors IBM ServeRAID adapters, click  to the left of the feature name. A menu opens.

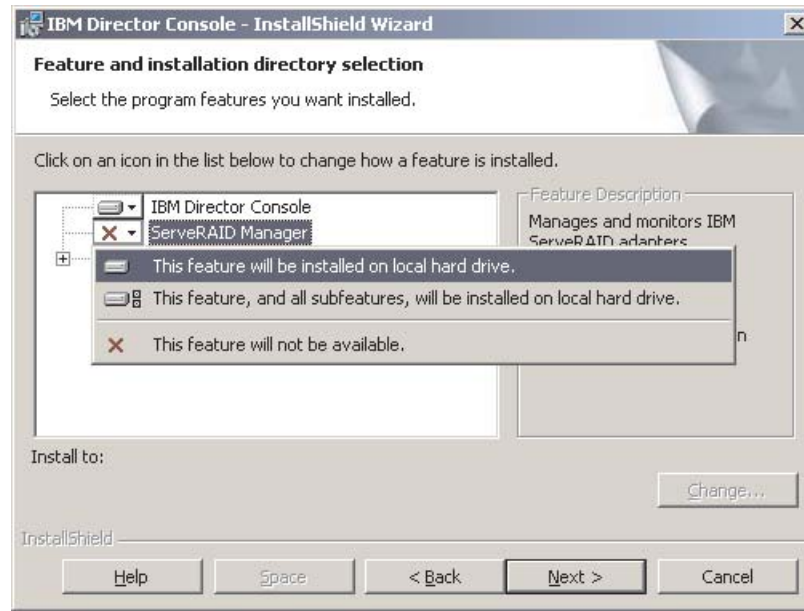


Figure 21. Installing IBM Director Console: Installing ServeRAID Manager

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

11. You can install the following Server Plus Pack 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.

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.

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.**

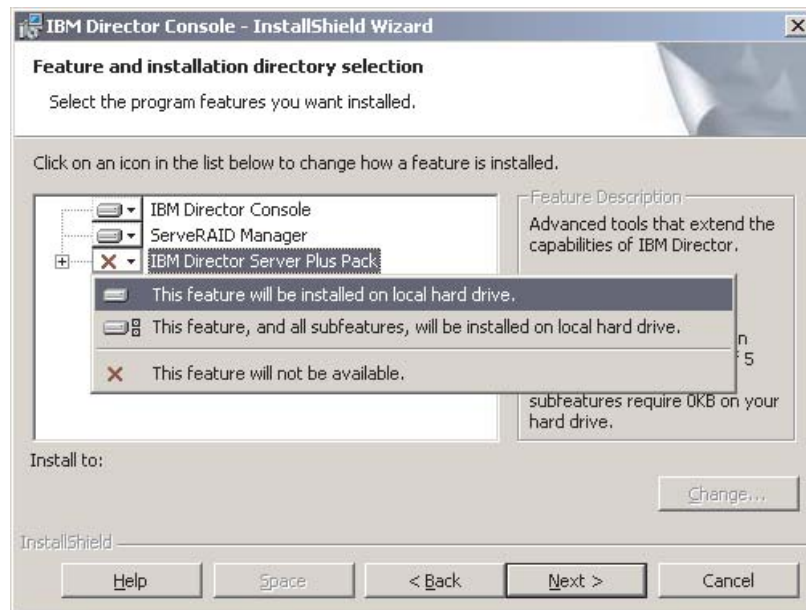


Figure 22. Installing IBM Director Console: Installing the Server Plus Pack

Otherwise, select the Server Plus Pack extensions individually.

12. Click **Next**. The Ready to Install the Program window opens.
13. 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.
14. Click **Finish**.
15. Remove the *IBM Director 4.1* 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. A system administrator 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 4.1* 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 4.1* 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** checkbox 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 4.1* 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 48.
8. When the installation is completed, remove the *IBM Director 4.1* 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 4.1* 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 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 50.

6. To customize the installation, 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.

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 choose log file options.

8. Save the modified installation script.

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

```
/destinationdirectory/dirinstall
```

where *destinationdirectory* 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 4.1* CD from the CD-ROM drive.

Chapter 5. Upgrading IBM Director Server and IBM Director Console

This chapter contains procedures for upgrading IBM Director Server and IBM Director Console from version 3.x to version 4.1.

Upgrading IBM Director Server

You can upgrade from IBM Director Server 3.x to IBM Director Server 4.1 on the following operating systems:

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

When you upgrade IBM Director Server, the InstallShield wizard also automatically upgrades IBM Director Console and IBM Director Agent.

Notes:

1. IBM Director 4.1 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. Before you upgrade to IBM Director Server 4.1, ensure that you have uninstalled any Active PCI Manager components. Earlier versions of Active PCI Manager, such as versions 1.0, 1.1, and 3.1.1, are not compatible with IBM Director 4.1.

Complete the following steps to upgrade to IBM Director Server 4.1 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 29 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 4.1* CD into the CD-ROM drive.
5. If the installation program starts automatically and the InstallShield wizard starts, go to 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.

After a few moments, 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.

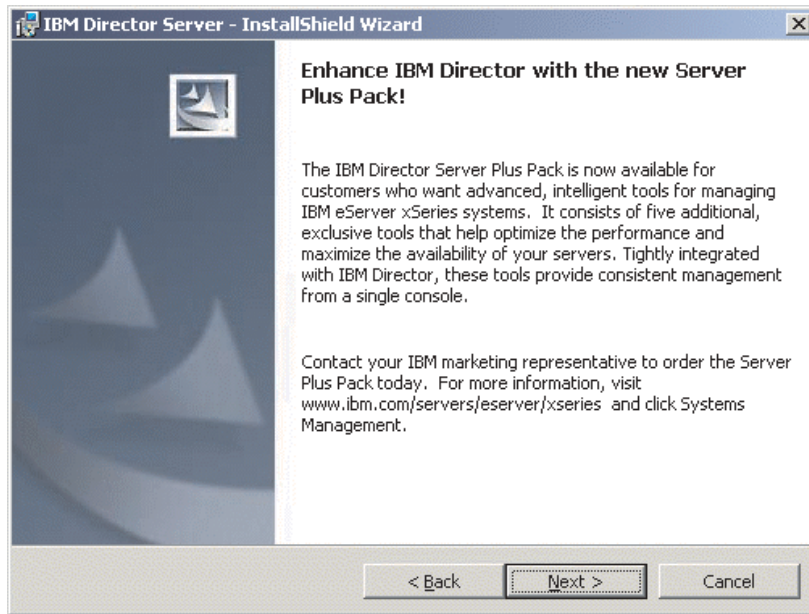


Figure 23. Upgrading IBM Director Server on Windows: Server Plus Pack window

11. Click **Next**. The "Feature and installation directory selection" window opens.

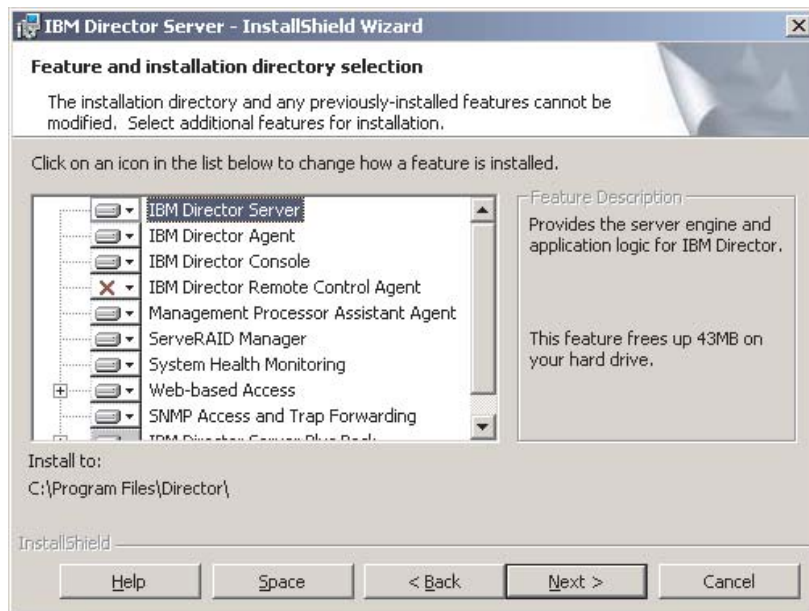




Figure 24. Upgrading IBM Director Server on Windows: "Feature and installation directory selection" window

12. IBM Director Server, IBM Director Agent, IBM Director Console, and any previously-installed features are selected automatically for installation; a hard disk 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

Permits 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

Permits 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.

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

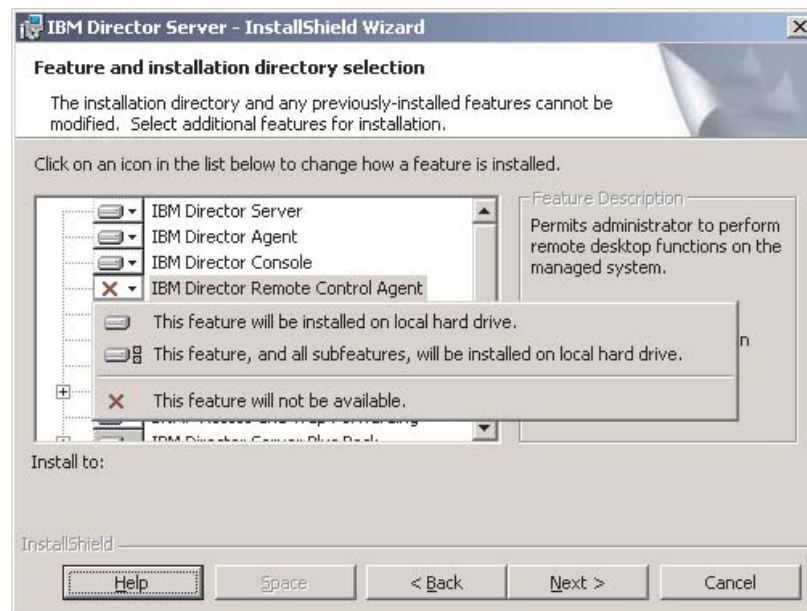


Figure 25. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window

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. 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.

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.

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**.

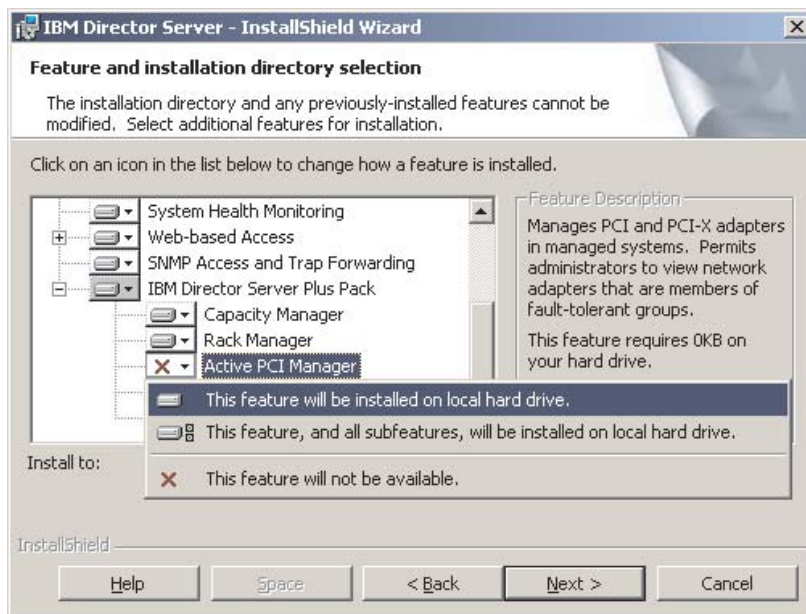
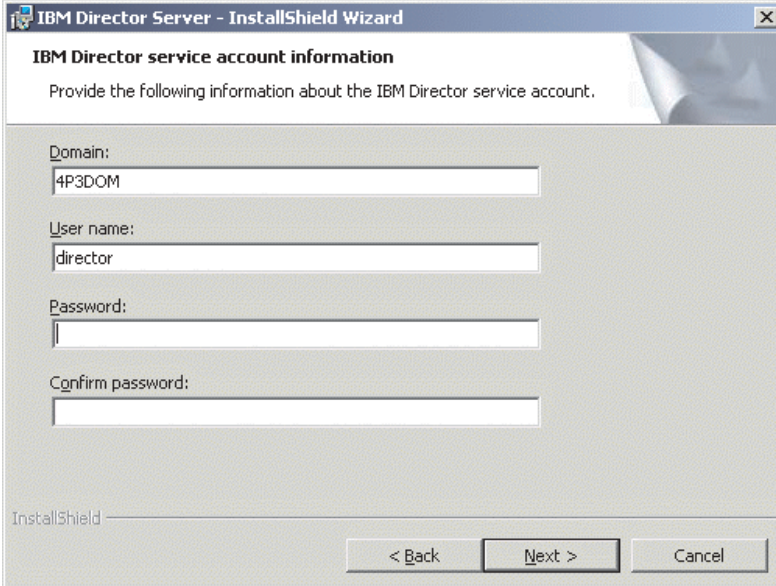


Figure 26. Upgrading IBM Director Server on Windows: Installing the Server Plus Pack

Otherwise, select the Server Plus Pack extensions individually.

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 16.)



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 >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

Figure 27. Upgrading IBM Director Server on Windows: “IBM Director service account information” window

15. 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 be for the IBM Director service account used to install IBM Director 3.x. Otherwise, the installation will fail.

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

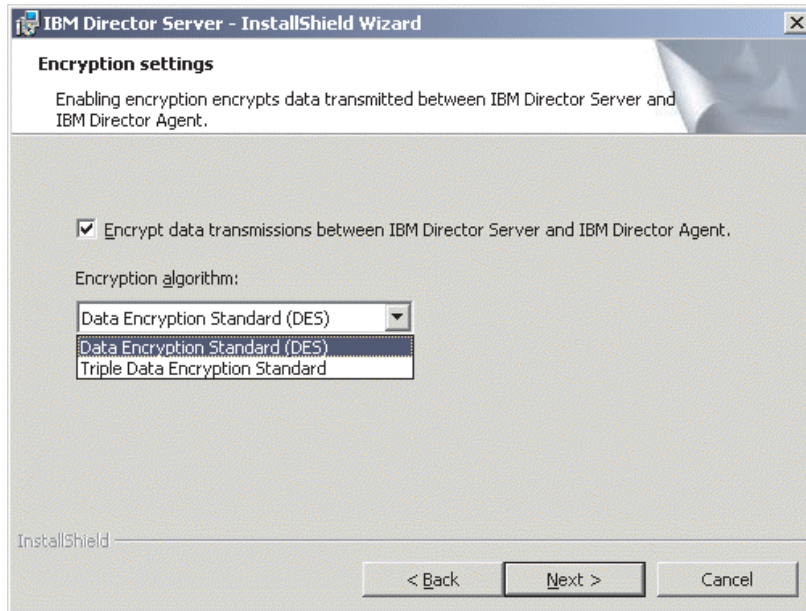


Figure 28. Installing IBM Director Server on Windows: “Encryption settings” window

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.

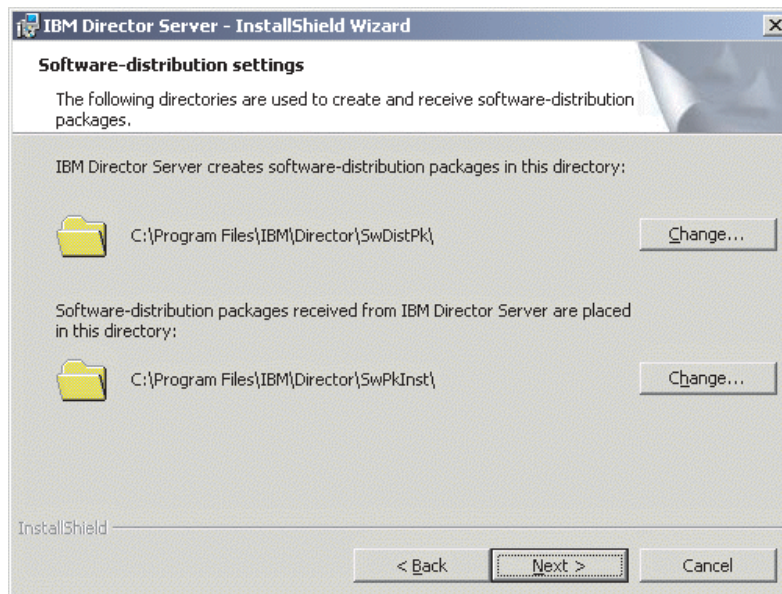


Figure 29. Upgrading IBM Director Server on Windows: “Software-distribution settings” window

19. Click **Next**. If you did not choose to install the Web-based Access feature, the Ready to Install the Program window opens; go to step 21 on page 57. Otherwise, the “Web-based Access information” window opens.

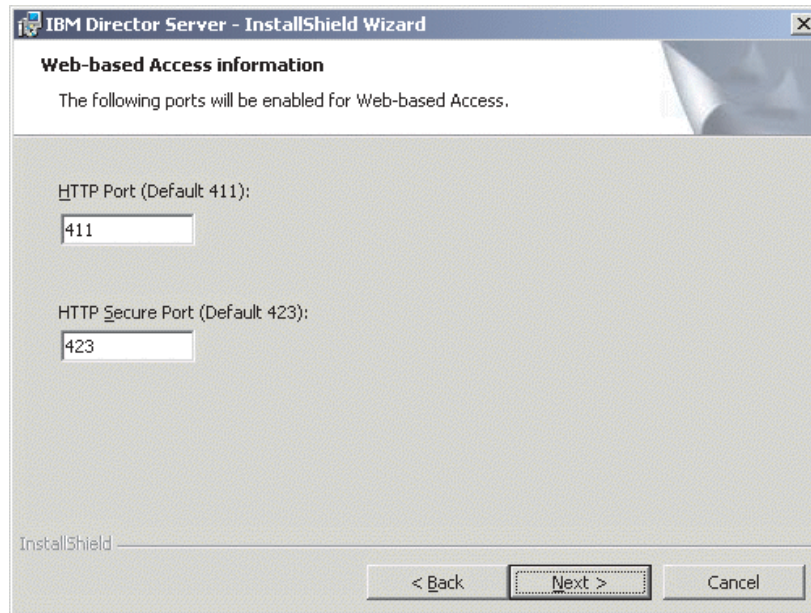


Figure 30. Upgrading IBM Director Server on Windows: “Web-based Access information” window

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.

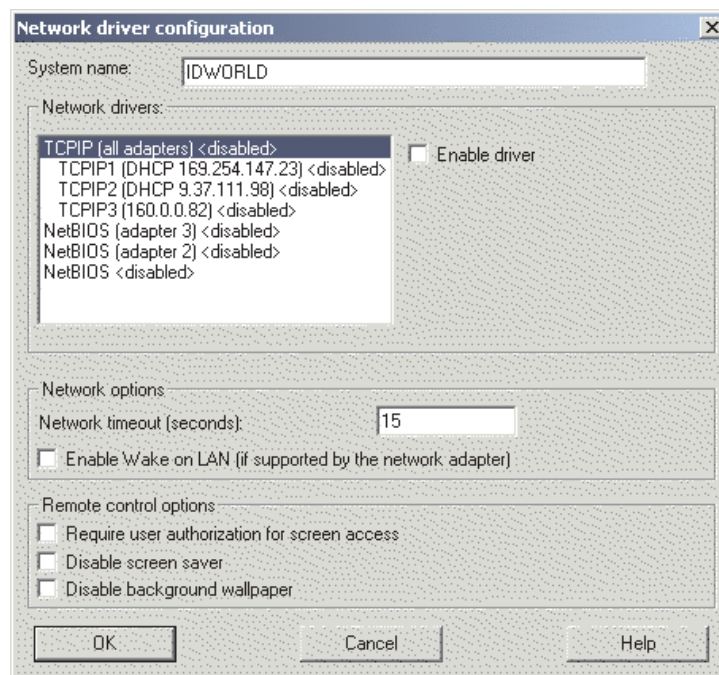


Figure 31. Upgrading IBM Director Server on Windows: “Network driver configuration” window

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.
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 driver on a system with multiple network adapters, IBM Director Server will receive data packets addressed to the individual adapter *only*.

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.

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.

24. If you chose 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 4.1* CD from the CD-ROM drive.
28. Click **Yes** to restart the server.

Upgrading IBM Director Console

You can upgrade from IBM Director Console 3.x to IBM Director Console 4.1 on the following operating systems:

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

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. Before you upgrade to IBM Director Console 4.1, ensure that you have uninstalled any Active PCI Manager components. Earlier versions of Active PCI Manager, such as versions 1.0, 1.1, and 3.1.1, are not compatible with IBM Director 4.1.
2. If you have both IBM Director Console 3.x and IBM Director Agent 3.x 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 95.

Upgrading IBM Director Console using the InstallShield wizard

Complete the following steps to upgrade to IBM Director Console 4.1 on Windows:

1. If IBM Director Agent 3.x 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 4.1* 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.

After a few moments, 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**; then, click **Next**. The Server Plus Pack window opens.



Figure 32. Installing IBM Director Console: Server Plus Pack window

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

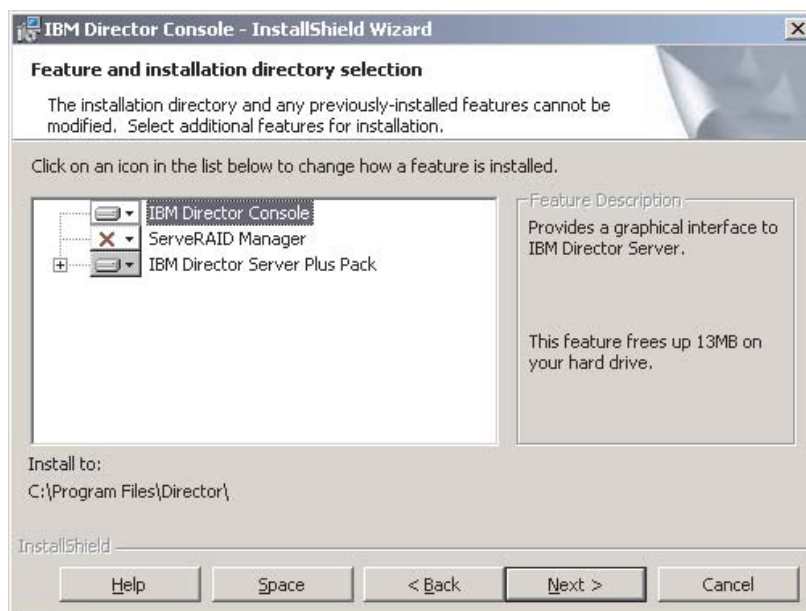




Figure 33. Installing IBM Director Console: “Feature and destination directory selection” window

11. IBM Director Console and any previously-installed features are selected automatically for installation; a hard disk 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.

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

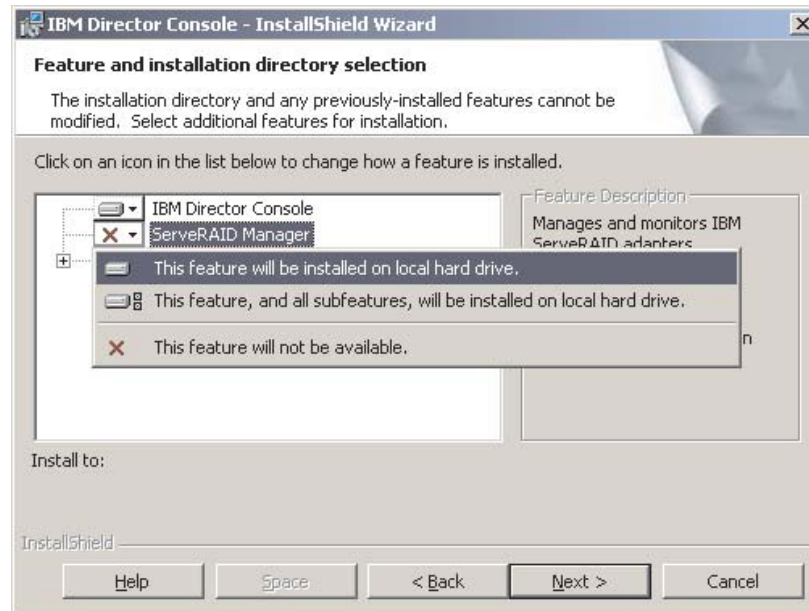


Figure 34. Installing IBM Director Console: Installing ServeRAID Manager

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

12. You can install the following Server Plus Pack 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.

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.

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.**

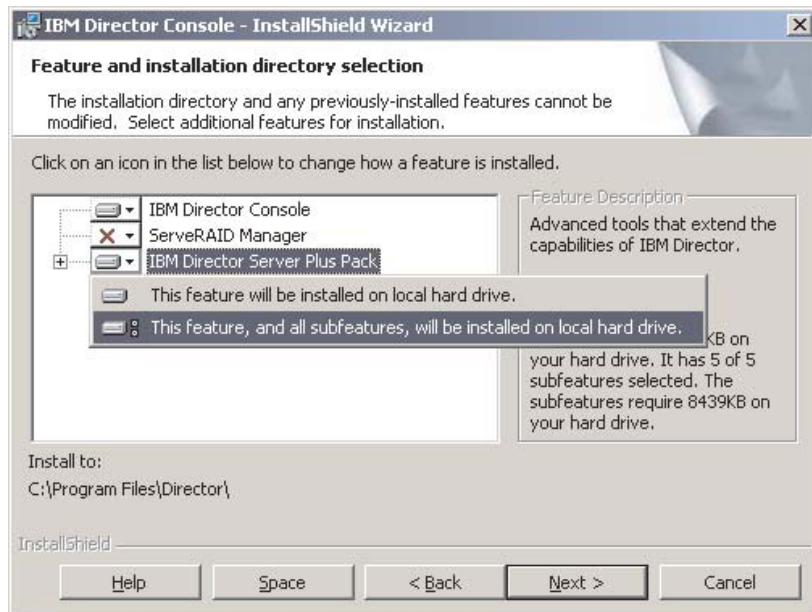


Figure 35. Installing IBM Director Console: Installing the Server Plus Pack

Otherwise, select the Server Plus Pack extensions individually.

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 4.1* 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 to IBM Director Console 4.1 on Windows:

1. If IBM Director Agent 3.x 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 4.1* 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 4.1* 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 3.x installation. However, you can choose to 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 4.1* 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 4.1* CD from the CD-ROM drive.

Chapter 6. Configuring the IBM BladeCenter chassis

This chapter contains information about discovering and configuring the BladeCenter chassis.

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	Check to see if 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 36. 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 opens.

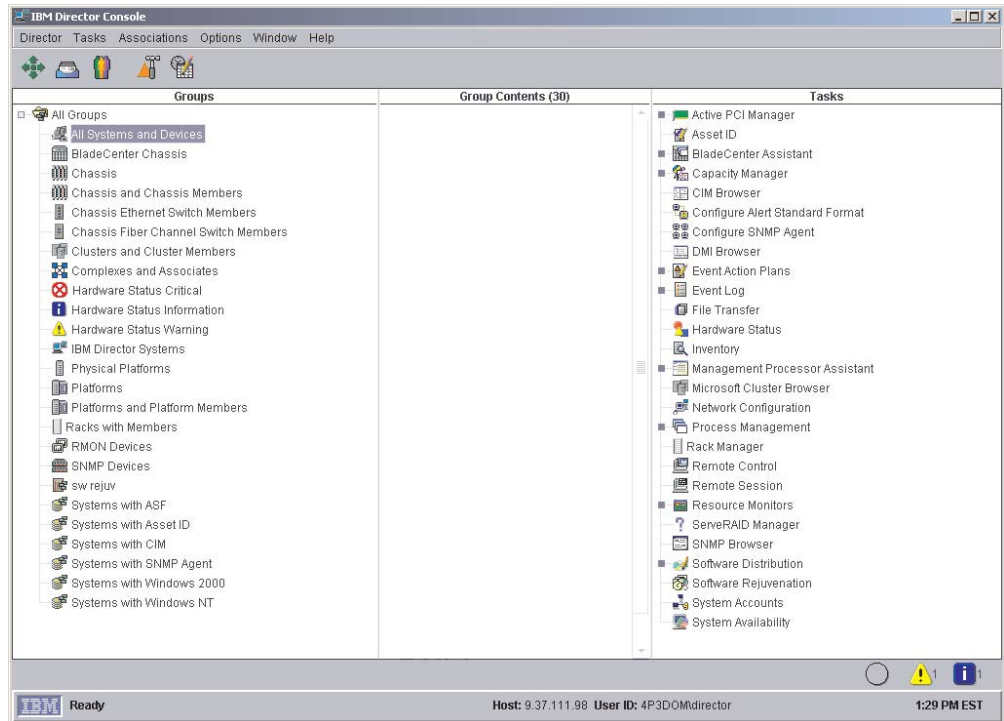


Figure 37. IBM Director Console window

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 either must 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” on page 67.

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 68.

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 4.1 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, non-routable 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**.
3. The BladeCenter chassis managed object is displayed in the Group Contents pane.

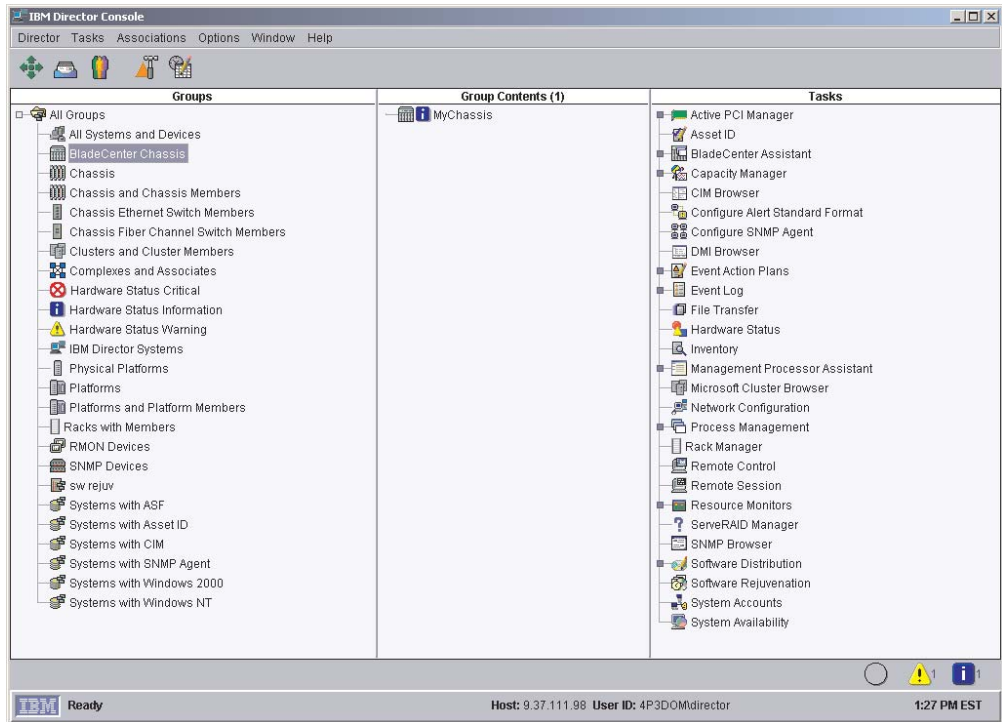


Figure 38. BladeCenter chassis managed object displayed in the Group Contents pane

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 non-routable IP address. For instructions, see “Manually changing the IP address of the BladeCenter chassis” on page 69.
2. From IBM Director Console, right-click in the Group Contents pane; then click **New → BladeCenter Chassis**. The Add BladeCenter Chassis window opens.

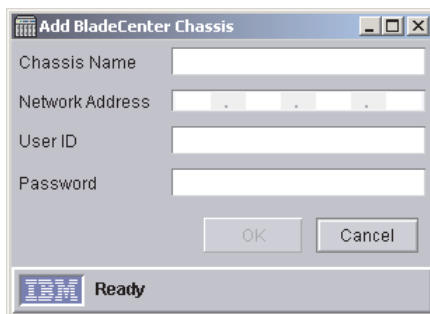


Figure 39. Add BladeCenter Chassis window

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 appropriate fields, type the default user name (USERID) and password (PASSWORD) for the BladeCenter management module.

Note: Use uppercase letters and substitute a zero for the “O” in “PASSWORD.”

6. Click **OK**. The BladeCenter Management Module window opens.
7. Click **Continue**. The System Status Summary window opens.
8. In the left pane, under MM Control, click **Network Interfaces**. The Management Module Network Interfaces window opens.

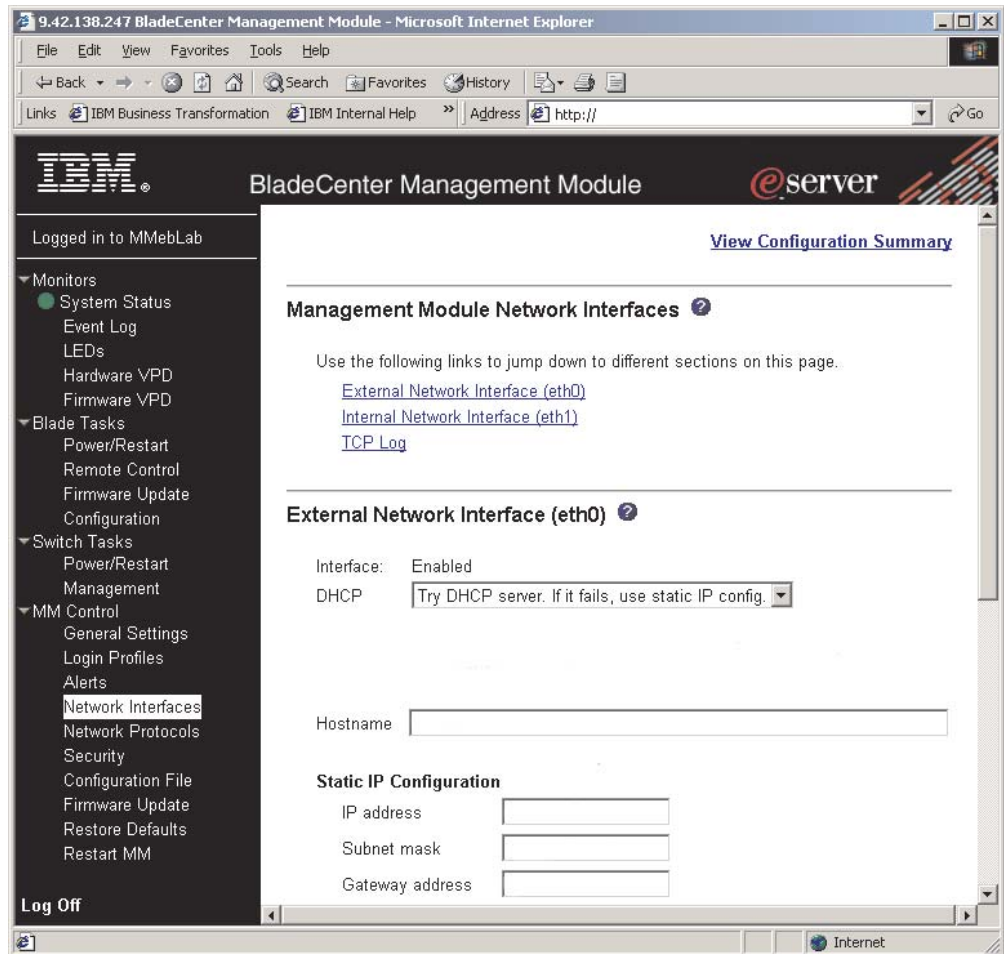


Figure 40. Management Module Network Interfaces window

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, under MM Control, click **Restart MM**.

Using the BladeCenter Deployment wizard

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

- Configuring 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.
- Creating a reusable profile that can be used to configure new BladeCenter chassis automatically when they are added to the IBM Director environment.

Notes:

1. In order to use the BladeCenter Deployment wizard, IBM Director 4.1 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.

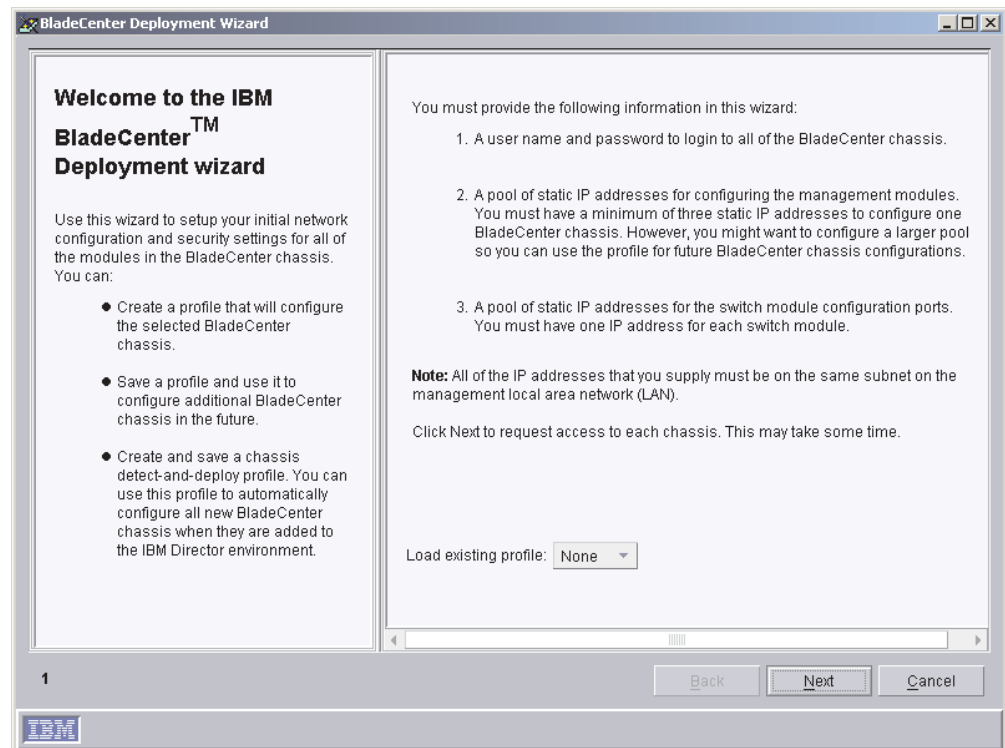


Figure 41. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window

3. Click **Next**. If you are already logged into the management module or if you are using the factory-default user name and password for the management module, the “Change the user name and password for the management module” window opens. Go to step 6 on page 73.
4. If the user name and password for the management module have been changed, the “Login to the BladeCenter management module” window opens.

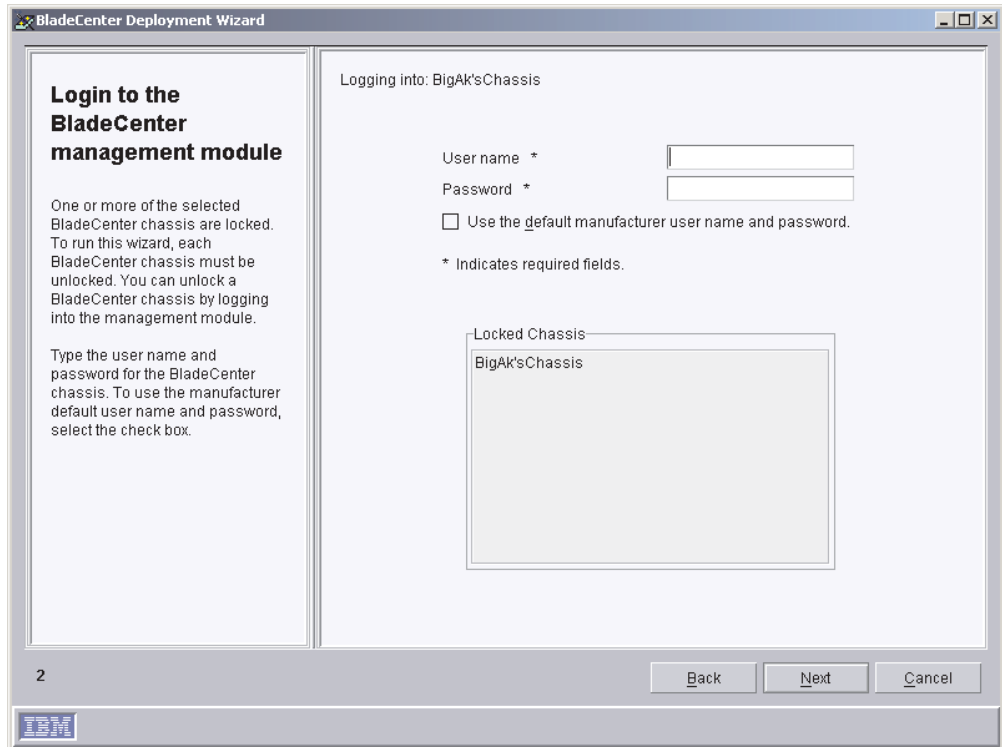


Figure 42. BladeCenter Deployment wizard: "Login to the BladeCenter management module" window

5. In the appropriate fields, type the current user name and password; then, press **Next**. The "Change the user name and password for the management module" window opens.

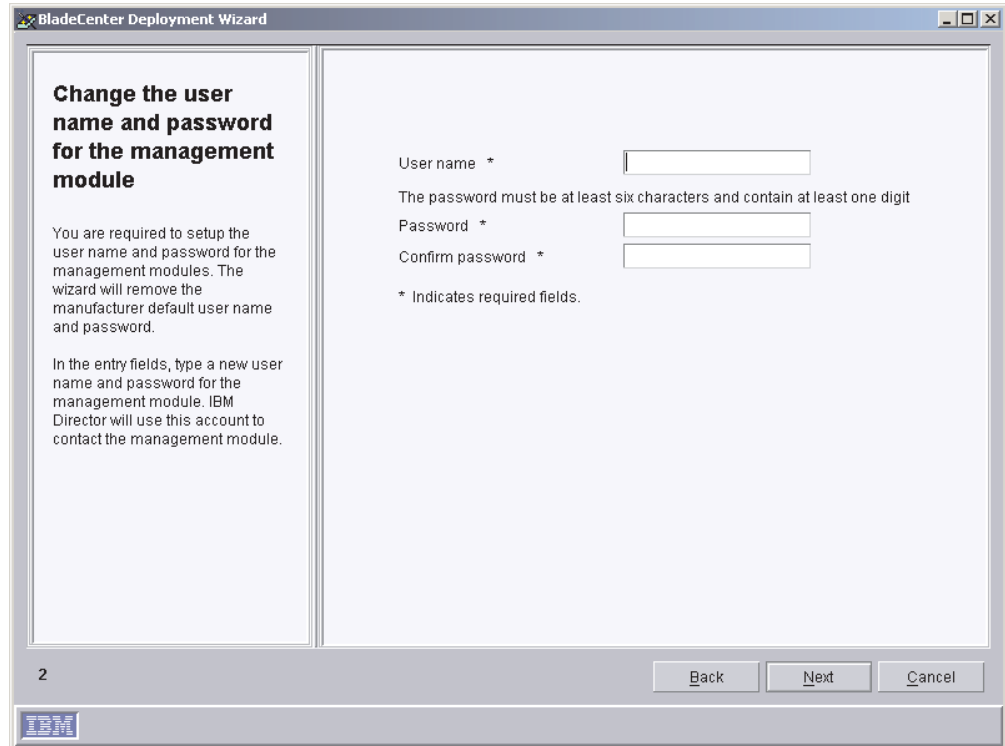


Figure 43. BladeCenter Deployment wizard: “Change the user name and password for the management module” window

6. If you logged into the management module using the factory-default user name and password, change them now. In the **User name** field, type a new user name. 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 into 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.
7. Click **Next**. The “Configure the management module properties” window opens.

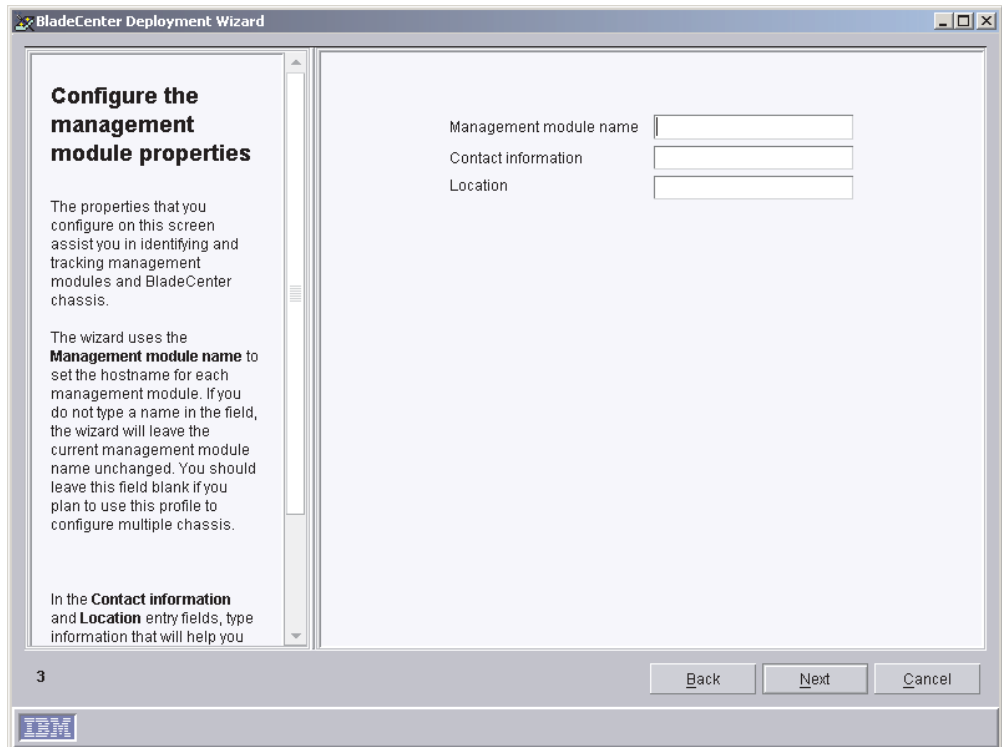


Figure 44. BladeCenter Deployment wizard: “Configure the management module properties” window

8. Complete the following entry fields:

Management module name

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 MMxxxxxxxxxxxx, where xxxxxxxxxxxx is the burned-in media access control (MAC) address of the management module.

Contact information

Type the name of the asset owner.

Location

Type information about where the BladeCenter is located.

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

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

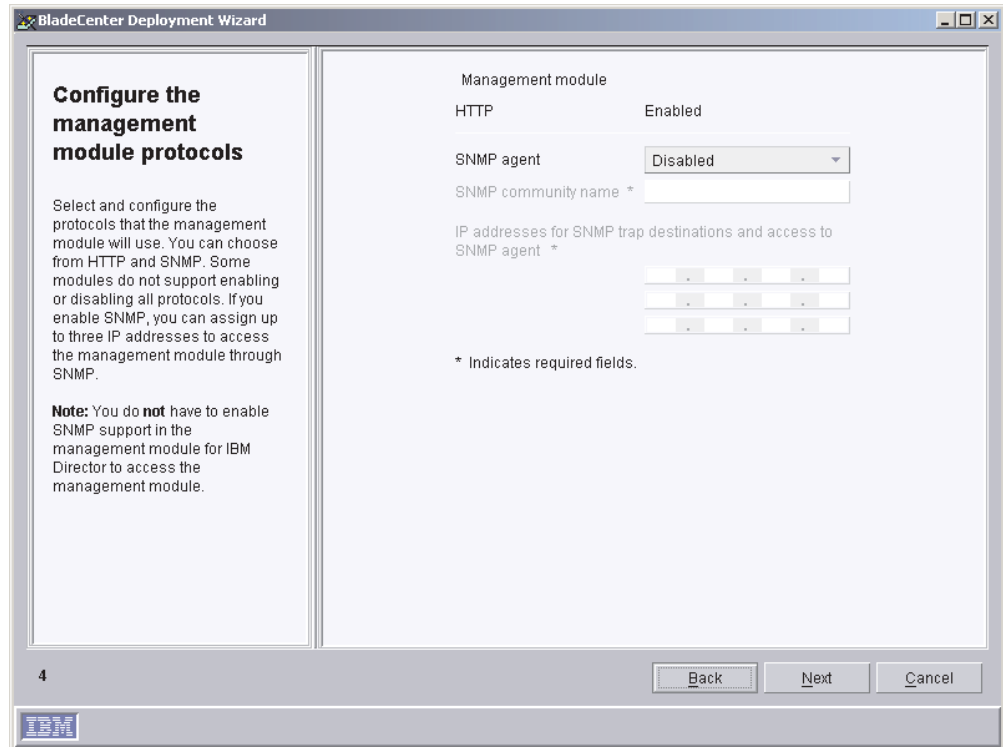


Figure 45. BladeCenter Deployment wizard: “Configure the management module protocols” window

10. 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 on the previous window. To do so, click **Back** to return to the “Configure the management module properties” window.

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

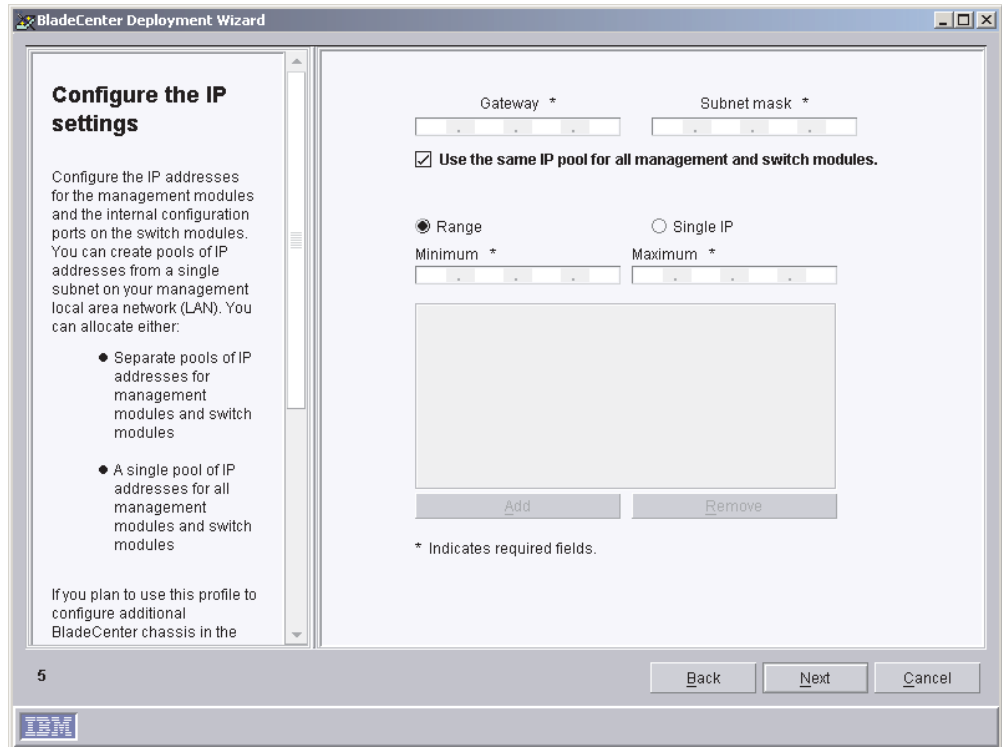


Figure 46. BladeCenter Deployment wizard: “Configure the IP settings” window

12. 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.
13. To configure separate pools of IP addresses for the management modules and switch modules, go to step 16. Otherwise, select the **Use the same IP pool for all management and switch modules** check box.
14. Create a pool of IP addresses. You can add IP addresses to the pool in the following ways:

Individual

Click **Single IP**. In the **IP address** field, type the IP address; then, click **Add**.

Range

Click **Range**. In the **Minimum** and **Maximum** fields, type the IP addresses that specify the range. Click **Add**.

15. When you have finished creating the pool of IP addresses for the management modules and switch modules, go to step 17.
16. 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 14.
 - b. To create the pool of IP addresses for the switch modules, click **Network Switch Module** and follow the instructions outlined in step 14.
17. Click **Next**. The “Change the user name and password for switch modules” window opens.

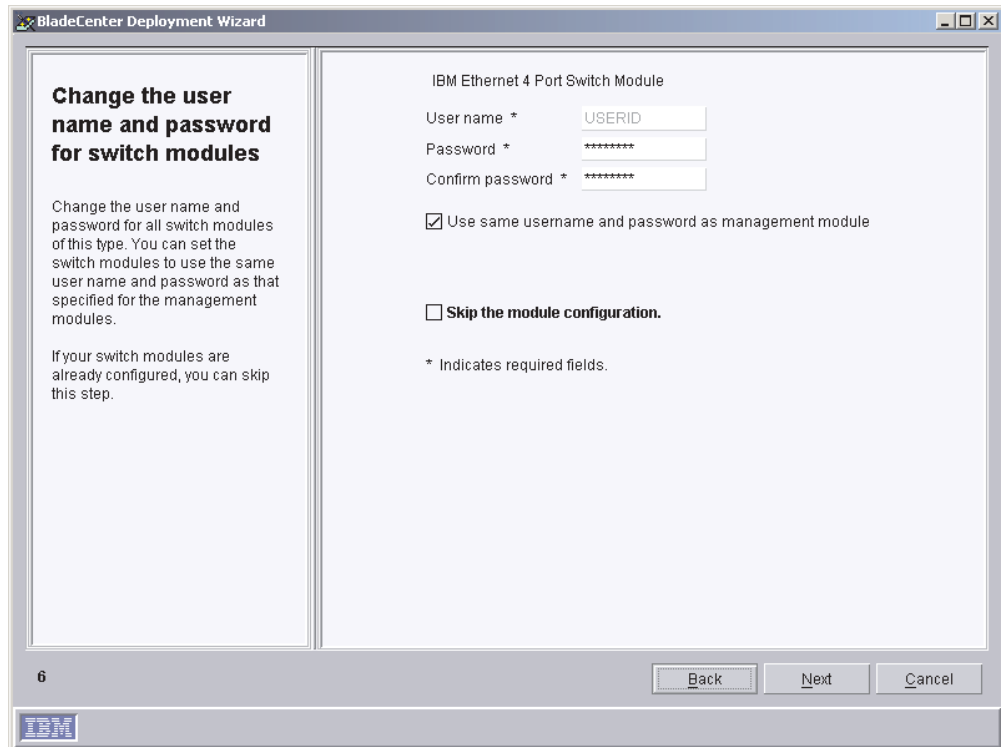


Figure 47. BladeCenter Deployment wizard: “Change the user name and password for switch modules” window

18. 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 19.
 If the switch modules are configured already, select the **Skip the module configuration** check box. Go to step 23 on page 78.
 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.
19. Click **Next**. The “Configure the switch module” window opens.

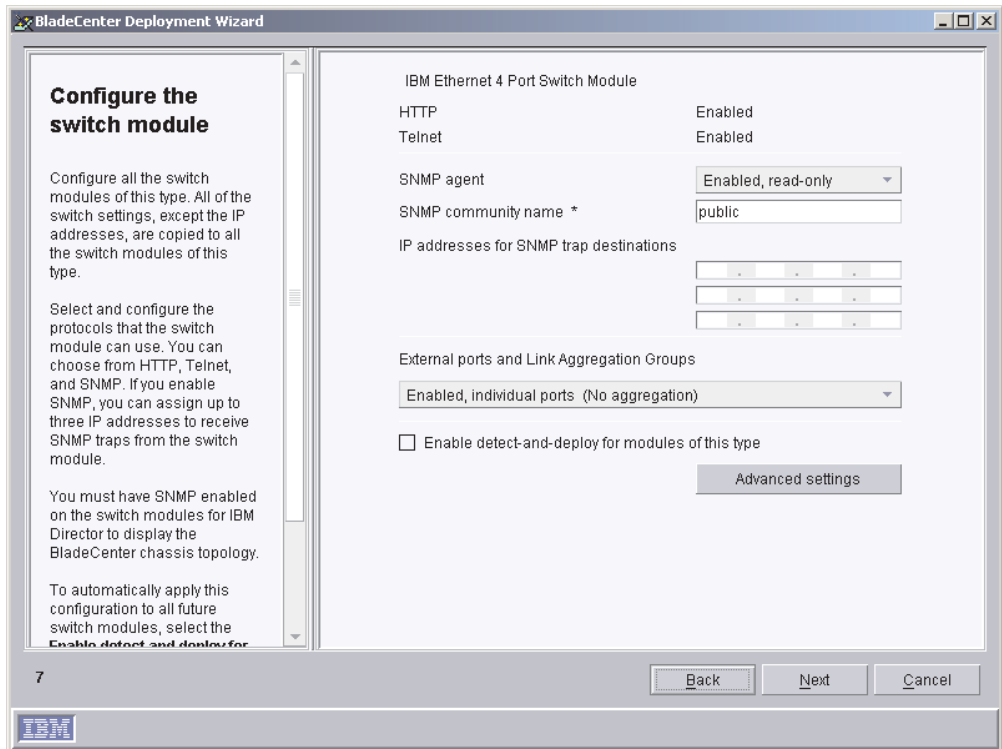


Figure 48. BladeCenter Deployment wizard: “Configure the switch module” window

20. 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.

21. 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 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.

22. 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.
23. Click **Next**. The “Deploy the operating systems on the blade servers” window opens.

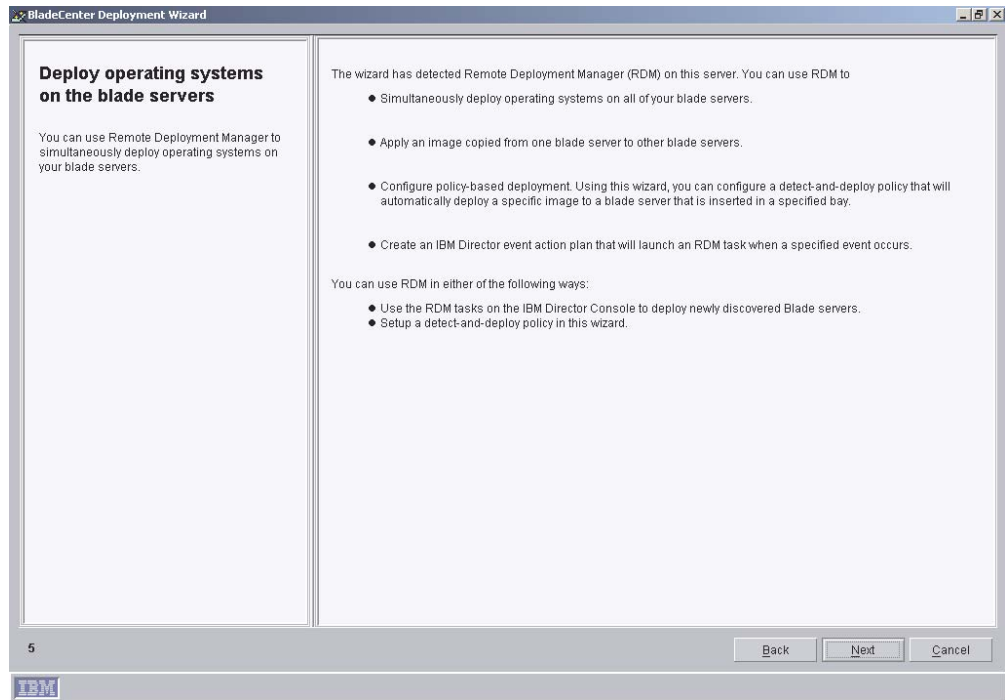


Figure 49. BladeCenter Deployment wizard: “Deploy operating systems on the blade servers” window

24. If you have IBM Remote Deployment Manager installed on your management server, go to step 25. Otherwise, go to step 28 on page 80.
25. Click **Next**. The “Configure the deployment policies” window opens.

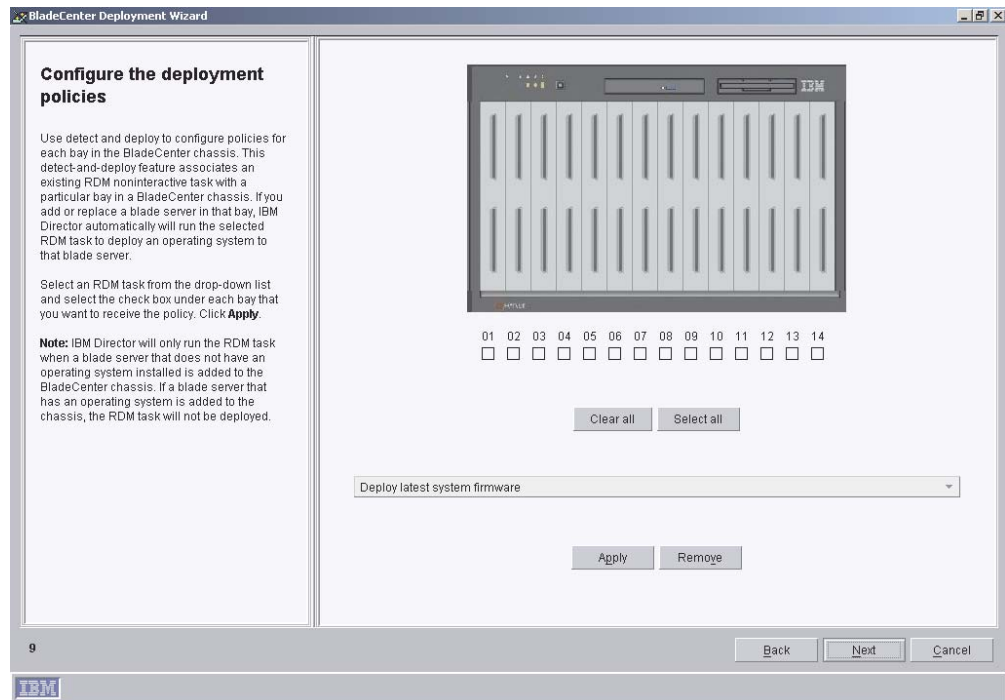


Figure 50. BladeCenter Deployment wizard: “Configure the deployment policies” window

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

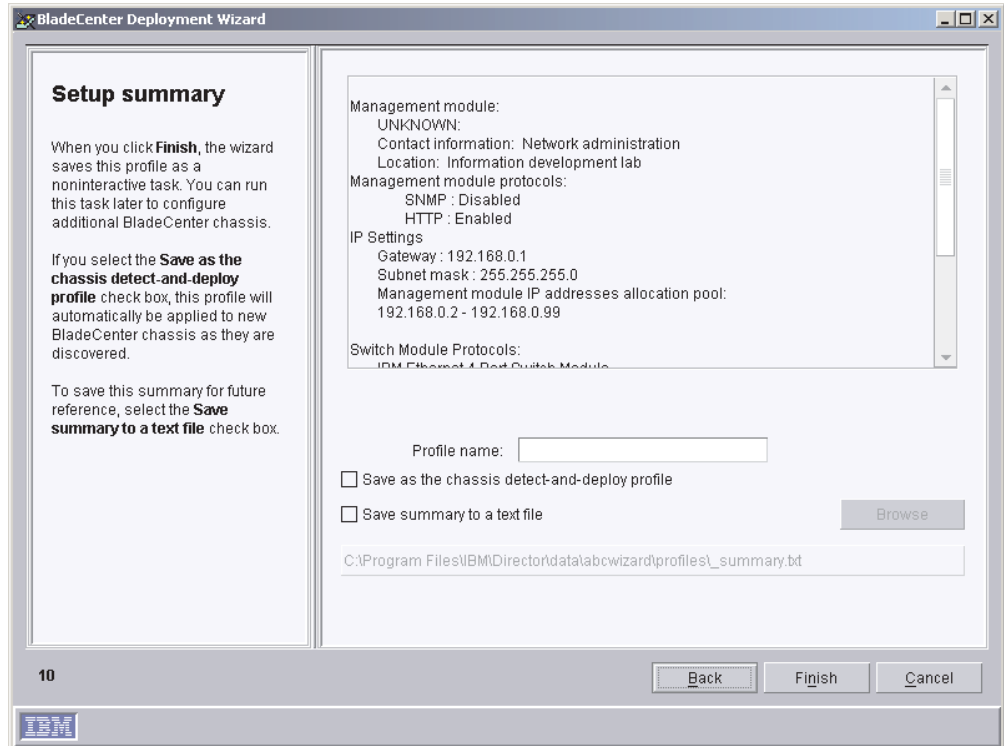


Figure 51. BladeCenter Deployment wizard: “Setup summary” window

29. A summary of the configuration options selected is displayed in the right pane. By default, the profile is given the name you assigned to the management module. To change it, select the text in the **Profile name** field and type a new name for the profile.

To apply this profile automatically to all new BladeCenter chassis when they are discovered by IBM Director 4.1, select the **Save as the chassis detect-and-deploy profile** check box.

Note: 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.

To save the setup summary for future reference, select the **Save summary to a text file** check box.

30. Click **Finish**. The profile is created. It appears as a subtask under Deployment Wizard in the Tasks pane of IBM Director Console.

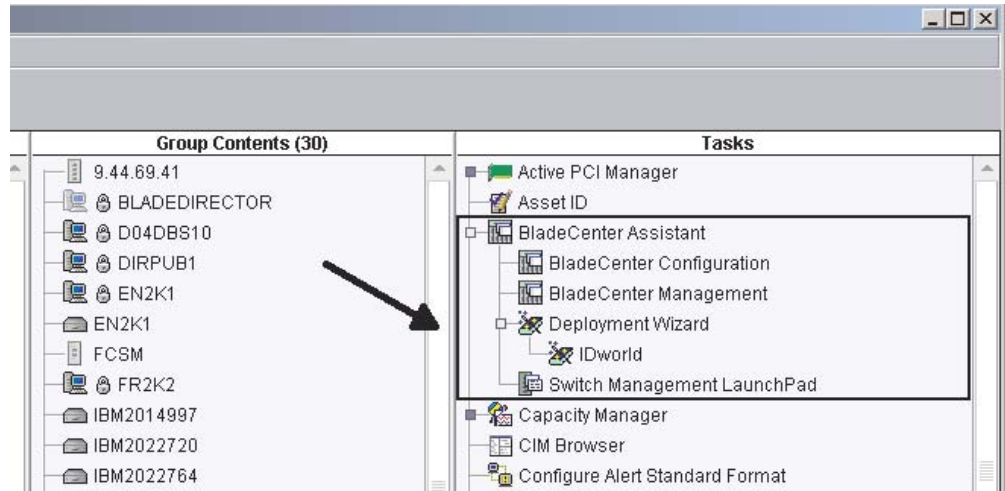


Figure 52. IBM Director Console Tasks pane: Deployment Wizard profile

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

Chapter 7. Installing IBM Director Agent

This chapter contains procedures for installing IBM Director Agent. If you are upgrading from IBM Director 3.x, go to Chapter 8, “Upgrading IBM Director Agent”, on page 95.

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

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

Installing IBM Director Agent on Microsoft Windows

This section provides 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.

Note: Before you install IBM Director Agent 4.1, ensure that you have uninstalled any Active PCI Manager components. Earlier versions of Active PCI Manager, such as versions 1.0, 1.1, and 3.1.1, are not compatible with IBM Director 4.1.

Installing IBM Director Agent using the InstallShield wizard

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

1. Insert the *IBM Director 4.1* 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.

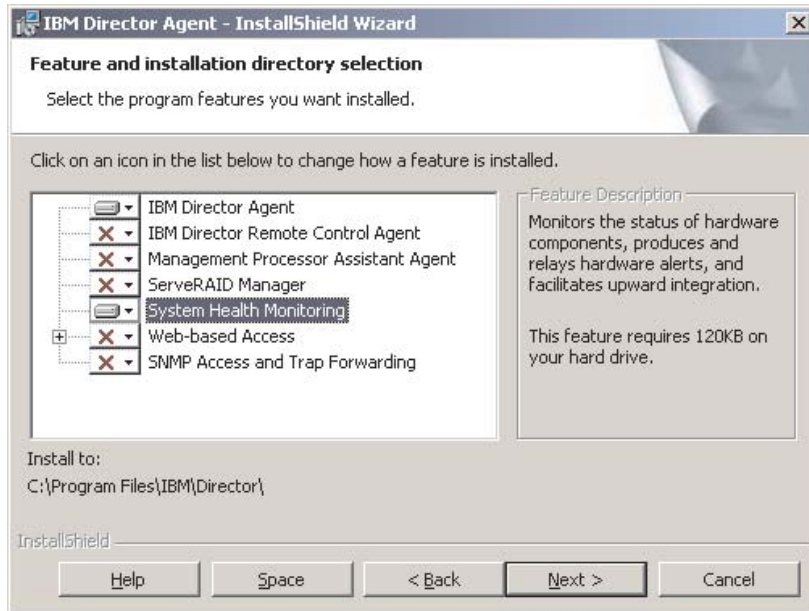




Figure 53. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

- IBM Director Agent is selected automatically for installation; a hard disk 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

Permits 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

Permits 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.

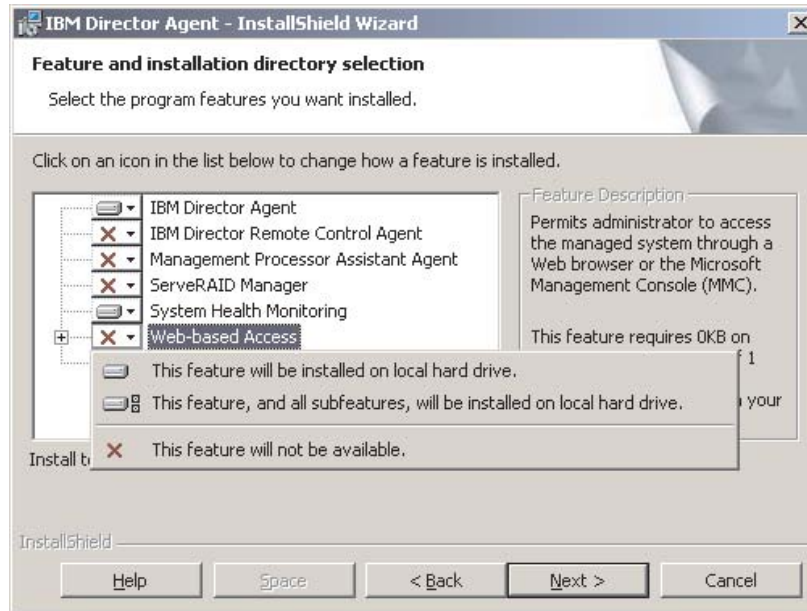


Figure 54. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

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 55. 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 on page 86. 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:

- a. The managed system is automatically secured, and the **Secure – IBM Director Server must request access to manage this system** check box is unavailable.
 - b. 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.

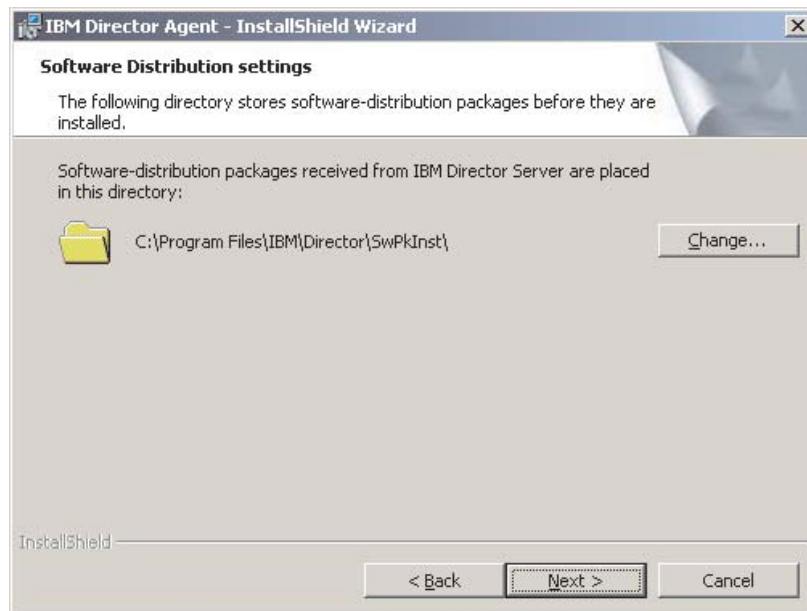


Figure 56. Installing IBM Director Agent on Windows: “Software Distribution settings” window

To select an alternate 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 choose to install the Web-based Access feature, go to step 15 on page 87. Otherwise, the “Web-based Access information” window opens.



Figure 57. 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.

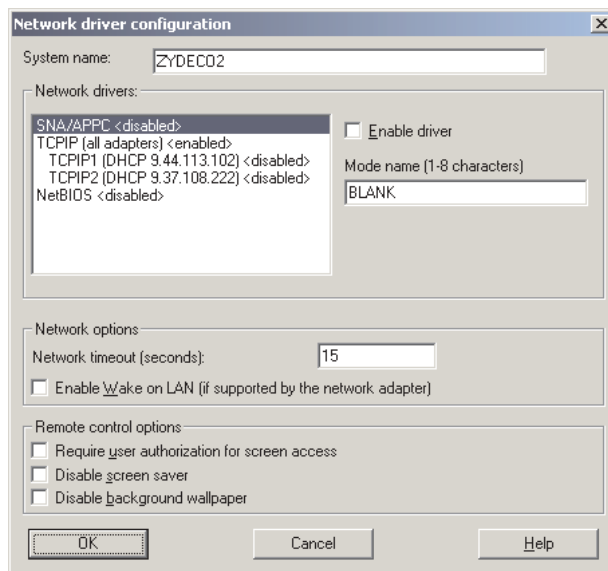


Figure 58. Installing IBM Director Agent on Windows: “Network driver configuration” window

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.

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 driver on a system with multiple network adapters, IBM Director Agent will receive data packets addressed to the individual adapter *only*.

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.

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 chose 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 4.1* CD from the CD-ROM drive.
22. Click **Yes** to restart your system.

Performing an unattended installation of IBM Director Agent

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. A system administrator 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. Insert the *IBM Director 4.1* CD into the CD-ROM drive.
2. Copy the `diragent.rsp` file to a local directory. This file is located in the `director\agent\windows\i386` directory on the *IBM Director 4.1* CD.
3. 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**.
4. Open the copy of the `diragent.rsp` file in an ASCII text editor.

5. Modify and save the `diragent.rsp` file. This file follows the Windows INI file format and is fully commented.
6. 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 4.1* CD.
7. 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 5.
 - `waitforme` is an optional parameter that ensures that `ibmsetup.exe` process will not end until the installation of IBM Director Agent is completed.
8. If you issued the UNATTENDED command in step 7, restart the operating system when prompted to do so.
9. Remove the *IBM Director 4.1* CD from the CD-ROM drive.

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

Before you install IBM Director Agent on systems running Linux, you must install the IBM SMBus device driver for Linux. This driver ensures that the Asset ID™ and Management Processor Assistant tasks function properly.

Building and installing the IBM SMBus device driver

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 driver, shared library, and all configuration files to their appropriate locations
- Loads the device driver

Installing IBM Director Agent

Notes:

1. Before installing IBM Director Agent, verify that the operating-system password-encryption method is set to message digest 5 (MD5) or DES.
2. (SuSE Linux 7.x only) Before installing IBM Director Agent, 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)
3. If you want to use the Remote Session task on this 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.

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

1. Verify that you have installed the IBM SMBus device driver for Linux, version 4.1. See “Building and installing the IBM SMBus device driver” on page 89.
2. Insert the *IBM Director 4.1* 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. If you want to customize the installation, go to step 7 on page 91. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 11 on page 91.

7. To customize the installation, 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.

8. 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 choose log file options.

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

```
/destinationdirectory/dirinstall
```

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

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

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

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

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

13. 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.

14. Remove the *IBM Director 4.1* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable Wake on LAN. See “Enabling Wake on LAN” on page 153.

Installing IBM Director Agent on NetWare

Notes:

1. 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.
2. 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, 330, 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.

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

1. Insert the *IBM Director 4.1* 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.

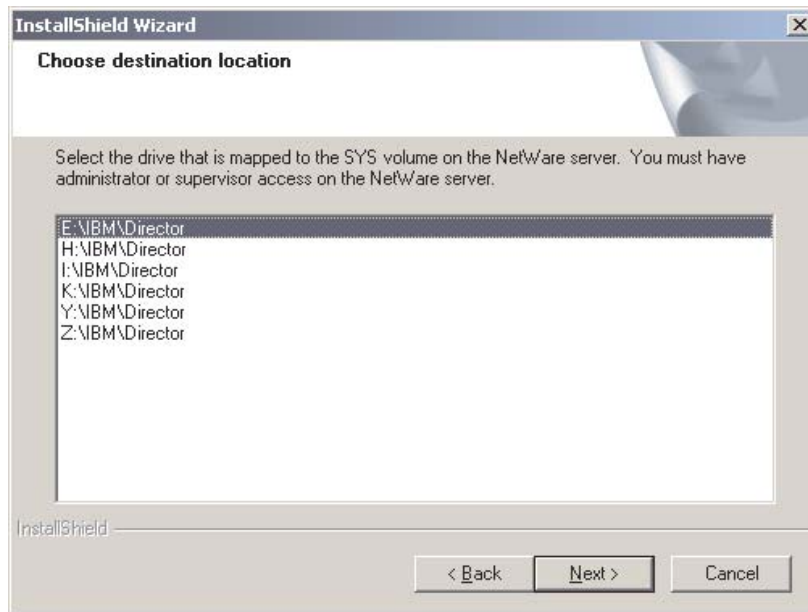


Figure 59. Installing IBM Director Agent on NetWare: “Choose destination location” window

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

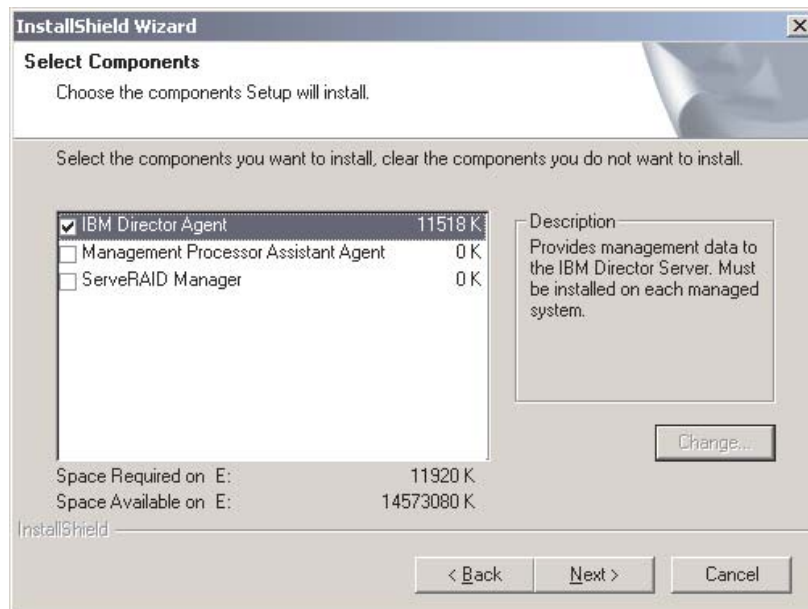


Figure 60. Installing IBM Director Agent on NetWare: Select Components window

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.

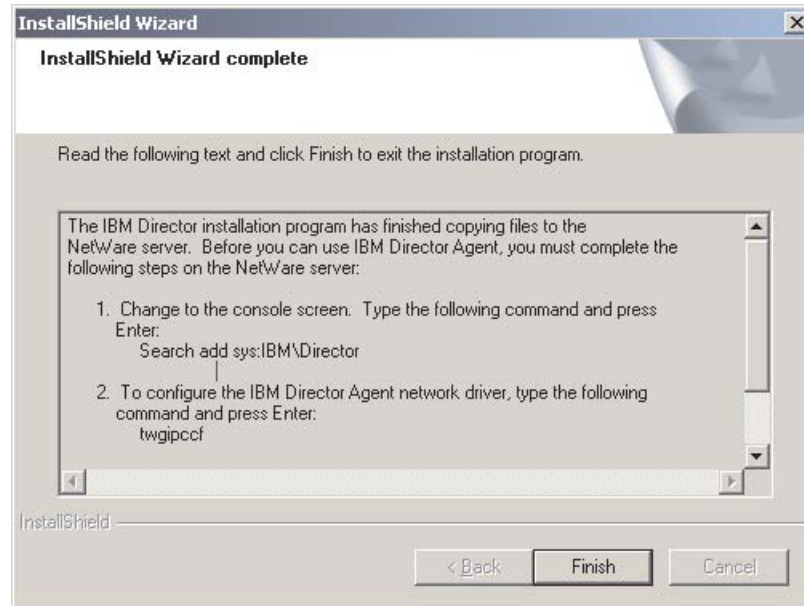


Figure 61. Installing IBM Director Agent on NetWare: “InstallShield Wizard complete” window

8. Click **Finish**.
 9. Remove the *IBM Director 4.1* CD from the CD-ROM drive.
 10. On the NetWare server, 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 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 NetWare server starts.

Installing IBM Director Agent on Caldera Open UNIX

Note: 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 4.1* 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 choose 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 4.1* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable Wake on LAN. See “Enabling Wake on LAN” on page 153.

Chapter 8. Upgrading IBM Director Agent

This chapter contains procedures for upgrading IBM Director Agent from version 3.x to version 4.1. It includes instructions for upgrading using either standard installation procedures or the IBM Director Software Distribution task.

IBM Director Agent is no longer supported on the following operating systems:

- Windows NT 4.0 Server, Enterprise Edition, Workstation, and Terminal Server
- 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 4.1 can manage systems running IBM Director Agent 3.x.

Upgrading IBM Director Agent using standard installation procedures

You can upgrade IBM Director Agent 3.x to IBM Director Agent 4.1 on the following operating systems:

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

Upgrading IBM Director Agent on Windows

This section provides 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.

Notes:

1. Before you upgrade to IBM Director Agent 4.1, ensure that you have uninstalled any Active PCI Manager components. Earlier versions of Active PCI Manager, such as versions 1.0, 1.1, and 3.1.1, are not compatible with IBM Director 4.1.
2. If you have both IBM Director Agent 3.x and IBM Director Console 3.x 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 “Upgrading IBM Director Console” on page 58.

Upgrading IBM Director Agent using the InstallShield wizard

Complete the following steps to upgrade to IBM Director Agent 4.1 on Windows:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
net stop twipc
```
2. Close all applications, including any command-prompt sessions.
3. Insert the *IBM Director 4.1* 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.

After a few moments, 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.

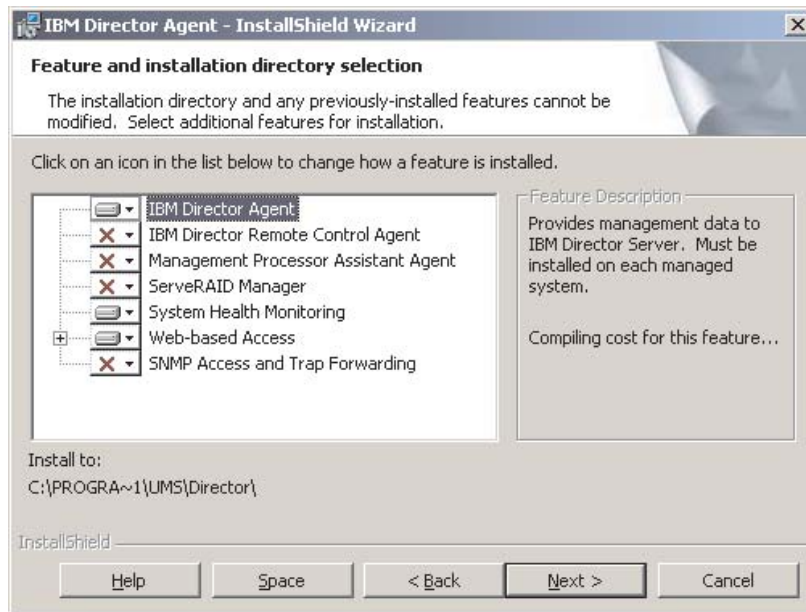




Figure 62. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window

10. IBM Director Agent and any previously-installed features are selected automatically for installation; a hard disk 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 choose install the following features:

IBM Director Remote Control Agent

Permits 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

Permits 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.

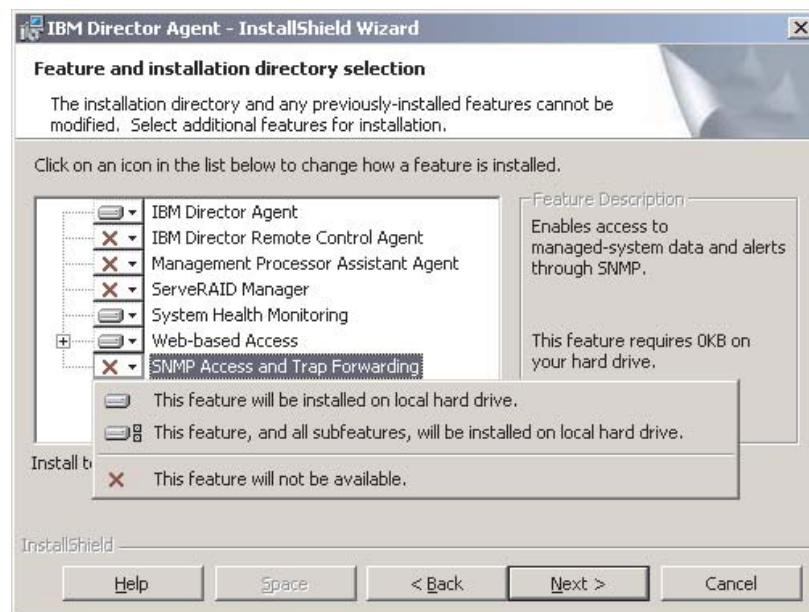


Figure 63. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window

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**.

Note: IBM Director 4.1 is installed into the same directory as where IBM Director 3.x was installed. You cannot choose an alternate location.

11. When you have selected the features you want to install, click **Next**. The “Security settings” window opens.



Figure 64. 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. 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:

- a. The managed system is automatically secured, and the **Secure – IBM Director Server must request access to manage this system** check box is unavailable.
 - b. Only management servers with encryption enabled are able to communicate with the managed system.
13. 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.
 14. Click **Next**. The “Software Distribution settings” window opens.

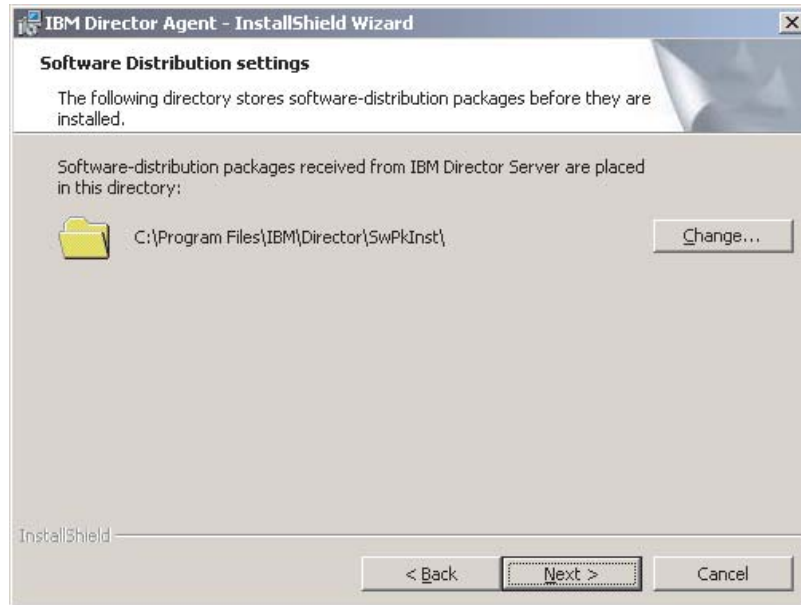


Figure 65. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window

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

15. Click **Next**. If you did not choose to install the Web-based Access feature, go to step 17 on page 100. Otherwise, the “Web-based Access information” window opens.

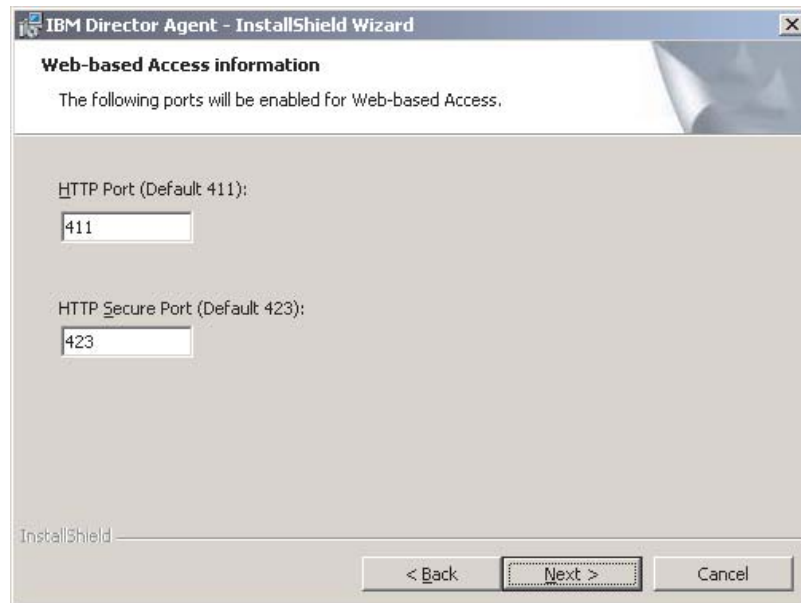


Figure 66. Upgrading IBM Director Agent on Windows: “Web-based Access information” window

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.

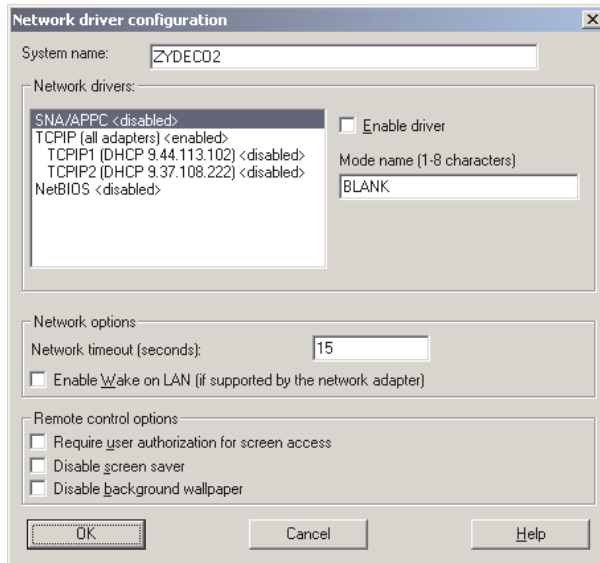


Figure 67. Upgrading IBM Director Agent on Windows: “Network driver configuration” window

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.

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 driver on a system with multiple network adapters, IBM Director Agent will receive data packets addressed to the individual adapter *only*.

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.

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.

20. If you chose 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 4.1* CD from the CD-ROM drive.
24. Click **Yes** to restart your system.

Performing an unattended upgrade of IBM Director Agent

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 to IBM Director Agent 4.1 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 4.1* 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 4.1* 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 3.x 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 4.1* 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 on page 101.
 - *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.
 11. Remove the *IBM Director 4.1* CD from the CD-ROM drive.

Upgrading IBM Director Agent on Red Hat Linux or SuSE Linux

Before you install IBM Director Agent on systems running Linux, you must install the IBM SMBus device driver for Linux, version 4.1. This driver ensures that the Asset ID and Management Processor Assistant tasks function properly.

Building and installing the IBM SMBus device driver

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. 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

Notes:

1. Before upgrading to IBM Director Agent 4.1, verify that the operating-system password encryption method is set to MD5 or DES.
2. (SuSE Linux 7.2 only) Before installing IBM Director Agent, 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)
3. If you want to use the Remote Session task on this 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.
4. For IBM Director 4.1, 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 4.1 on Linux:

1. Verify that you have installed the IBM SMBus device driver for Linux, version 4.1. See “Building and installing the IBM SMBus device driver” on page 102.
2. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
/opt/tivoliwg/bin/twgstop
```

3. Insert the *IBM Director 4.1* CD into the CD-ROM drive.
4. If the CD does not automount, go to step 5. 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.

5. 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.

6. 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.

7. 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.

8. 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 choose log file options.

Note: Be sure and select any features that were part of your IBM Director 3.x installation; if you fail to do so, the feature will be orphaned and

unnecessarily take up disk space. You always can remove unwanted features after the upgrade is completed.

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

```
/destinationdirectory/dirinstall
```

where *destinationdirectory* is the local directory to which you copied the installation script.
11. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```
12. To start IBM Director Agent, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```
13. 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.
14. Remove the *IBM Director 4.1* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable Wake on LAN. See “Enabling Wake on LAN” on page 153.

Upgrading IBM Director Agent on NetWare

Note: If the managed system running NetWare 5.x includes any of the following service processors, IBM Director Server 4.1 *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 4.1, you must upgrade to NetWare 6.0 and IBM Director Agent 4.1.

Complete the following steps to upgrade to IBM Director Agent 4.1 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 4.1* 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.

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

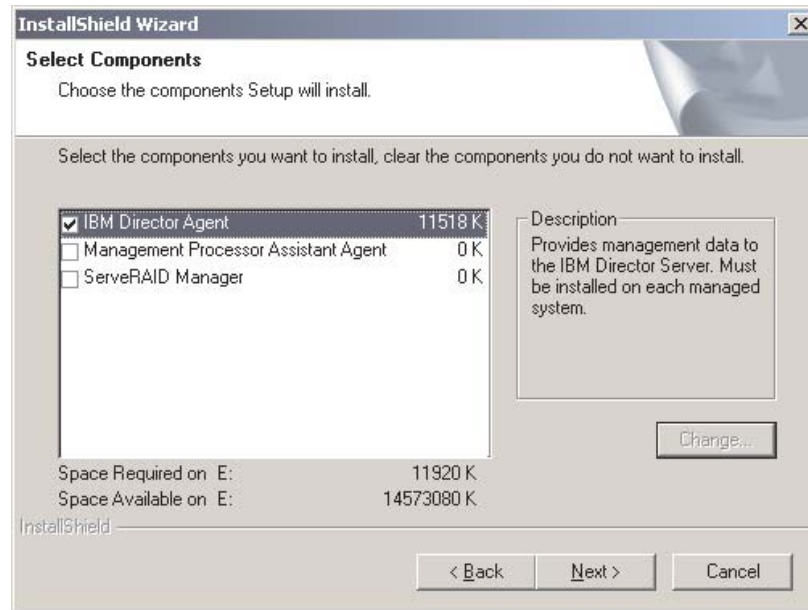


Figure 68. Upgrading IBM Director Agent on NetWare: Select Components window

- You *must* install the same features as were present in the IBM Director Agent 3.x installation. In addition, you must install IBM Director Agent 4.1 in the same directory as where IBM Director Agent 3.x was installed.

Select the check boxes for the components 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.

- Click **Finish**.
- Remove the *IBM Director 4.1* CD from the CD-ROM drive.
- On the NetWare server, start IBM Director Agent. Type the following command and press Enter:

```
load twgipc
```

Upgrading IBM Director Agent on Caldera Open UNIX

Notes:

- Before upgrading IBM Director Agent, verify that the operating-system password encryption method is set to MD5 or DES.
- The installation directory has not changed for IBM Director 4.1. Program files and user data remain in the `/opt/tivoliwg` directory.

Complete the following steps to upgrade to IBM Director Agent 4.1 on Caldera Open UNIX:

- Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
/opt/tivoliwg/bin/twgstop
```
- Insert the *IBM Director 4.1* 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 CD-ROM drive.

5. 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.

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 the IBM Director Agent features you want to install, and choose log file options.

Note: Be sure and select any features that were part of your IBM Director 3.x installation; if you fail to do so, the feature will be orphaned and unnecessarily take up disk space. You always can remove unwanted features after the upgrade is completed.

7. Save the modified installation script.

8. 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.

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 4.1* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable Wake on LAN. See “Enabling Wake on LAN” on page 153.

Upgrading IBM Director Agent using the Software Distribution task

Notes:

1. (Windows only) Before you upgrade to IBM Director Agent 4.1, ensure that you have uninstalled any Active PCI Manager components. Active PCI Manager, versions 1.0, 1.1, and 3.1.1, is not compatible with IBM Director 4.1.
2. (Linux only) Before you upgrade to IBM Director Agent 4.1 on systems running Linux, you must install the IBM SMBus device driver for Linux, version 4.1. This driver ensures that the Asset ID and Management Processor Assistant tasks function properly.

You can use the IBM Director Software Distribution task to upgrade IBM Director Agent 3.x to IBM Director Agent 4.1 on managed systems running Windows or Linux.

The following files describe IBM Director Agent 4.1 and the IBM SMBus driver:

- diragent_linux.xml
- diragent_windows.xml
- smbdriver_linux.xml

The smbdriver_linux.xml file is located in the /director/agent/linux/i386 directory on the *IBM Director 4.1* CD. See the readme.txt file for information about the location of the other XML files.

When you import the XML files into IBM Director, the Update Assistant creates software packages. Then, you can use the IBM Director Software Distribution task to distribute the packages to the managed systems.

Creating a software package

Complete the following steps to create a software package:

1. Download the IBM Director Agent 4.1 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.

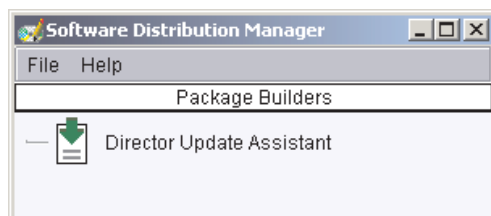


Figure 69. Creating a software package: Software Distribution Manager window



Figure 70. 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 71. Creating a software package: Director Update Assistant window

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**.

7. To select a file, click **Browse**. The IBM Update Package/Root Directory Location window opens.

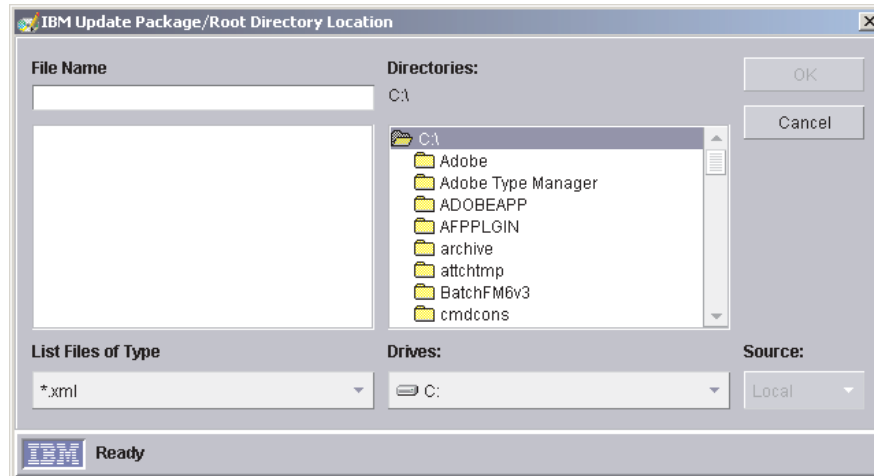


Figure 72. Creating a software package: IBM Update Package/Root Directory Location window

8. Locate the XML file and click it. The name of the XML file is displayed in the **File Name** field.

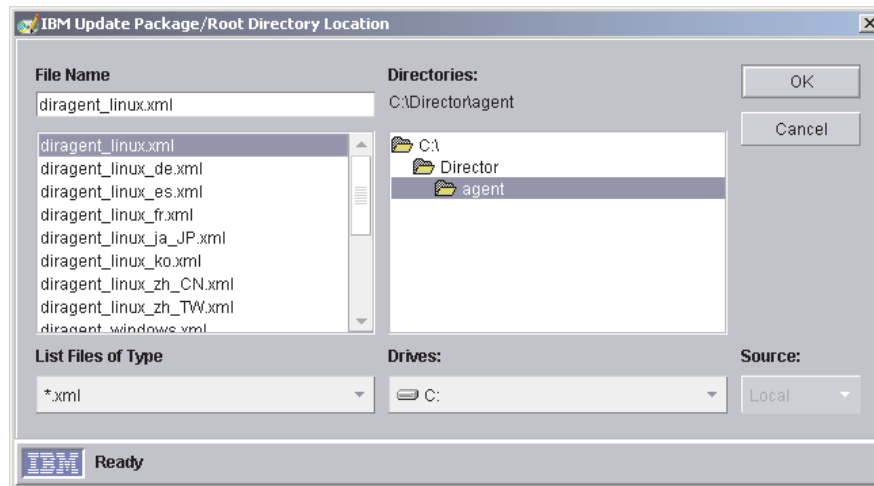


Figure 73. Creating a software package: IBM Update Package/Root Directory Location window

9. Click **OK**. The Director Update Assistant window reopens.



Figure 74. Creating a software package: Director Update Assistant window

10. Click **Next**. The second Director Update Assistant window opens.

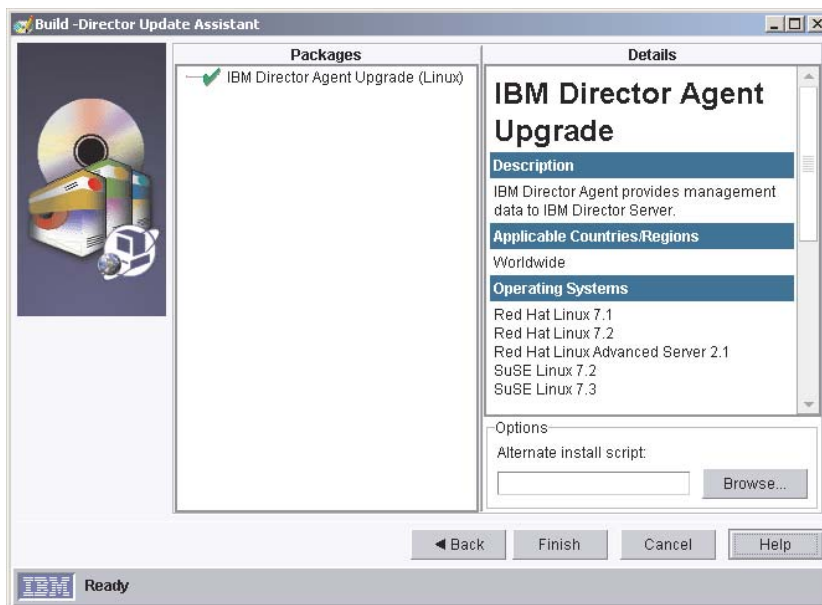


Figure 75. Creating software packages: Director Update Assistant window

11. To specify an alternative installation script or response file, click **Browse** and locate file you modified in step 2 on page 107.

Note: If you do not specify an alternative installation script or response file, IBM Director Agent 4.1 is installed with the default settings specified in the diragent.rsp file or dirinstall script.

12. Click **Finish**. As the packages are processed, a status message is displayed at the bottom of the window.
13. When the processing is completed, the software-distribution packages are displayed in the Tasks pane of IBM Director Console.

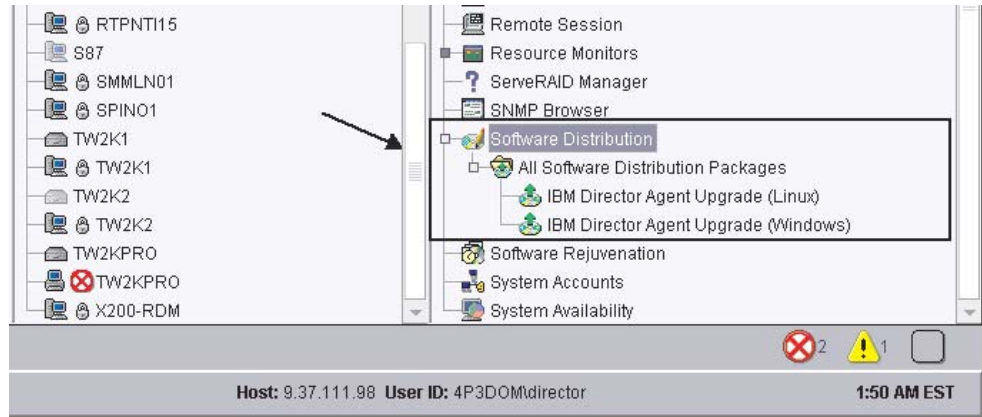


Figure 76. All Software Distributions Packages: IBM Director Agent Upgrade

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 tree.
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.

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.

A window opens.

4. When prompted “Do you wish to create a scheduled job for this task or execute immediately?”, click **Schedule** or **Execute Now**.
5. If you click **Execute Now**, the software package is distributed immediately. If you click **Schedule**, the New Scheduled Job window opens.

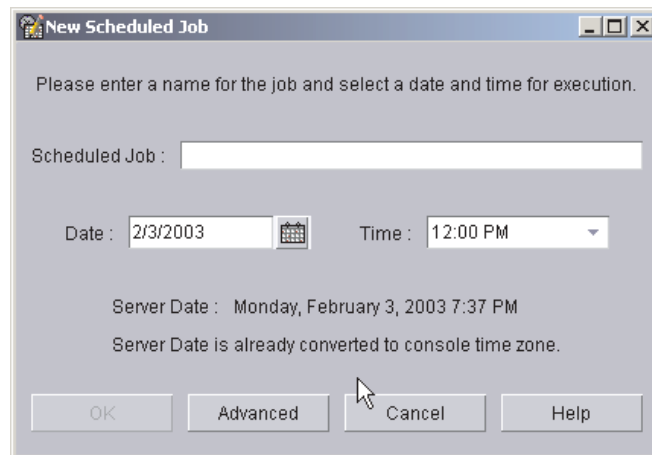


Figure 77. Scheduling the installation of a software package: New Scheduled Job window

You must enter information in the following fields:

Scheduled Job

Type a unique name for the job. This name is displayed in the Jobs pane of the Scheduler window.

Date Type the day you want the software package to be installed (MM/DD/YYYY format).

Time Type the time you want the software package to be installed.

For more information about the Scheduler task, see the *IBM Director 4.1 Systems Management Guide*.

6. Click **OK**. The Save Job Confirmation window opens.
7. Click **OK**.

Chapter 9. Configuring IBM Director 4.1

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 into 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 the above 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 4.1 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 122.

To use the Event Action Plan wizard, complete the following tasks:

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

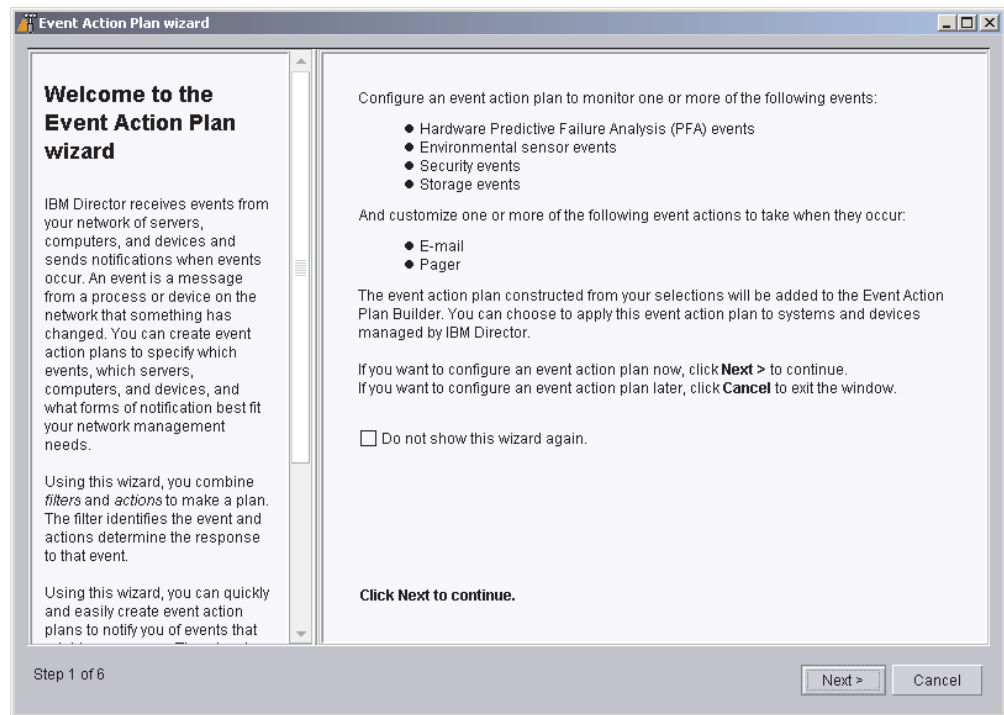


Figure 78. Event Action Plan wizard: "Welcome to the Event Action Plan wizard" window

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

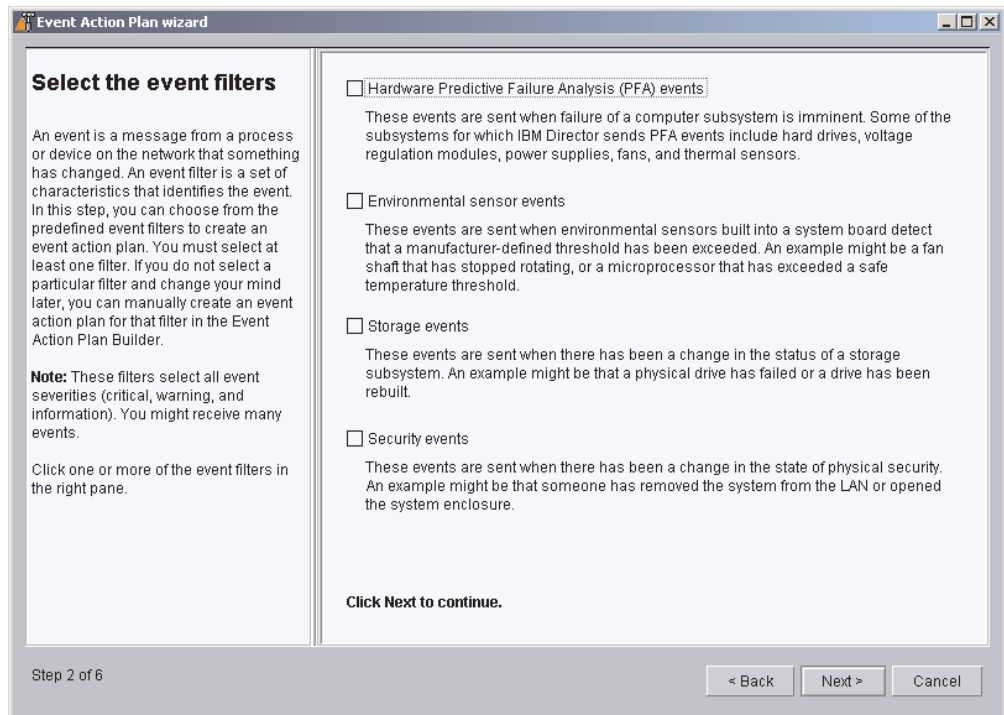


Figure 79. Event Action Plan wizard: “Select the event filters” window

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 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.

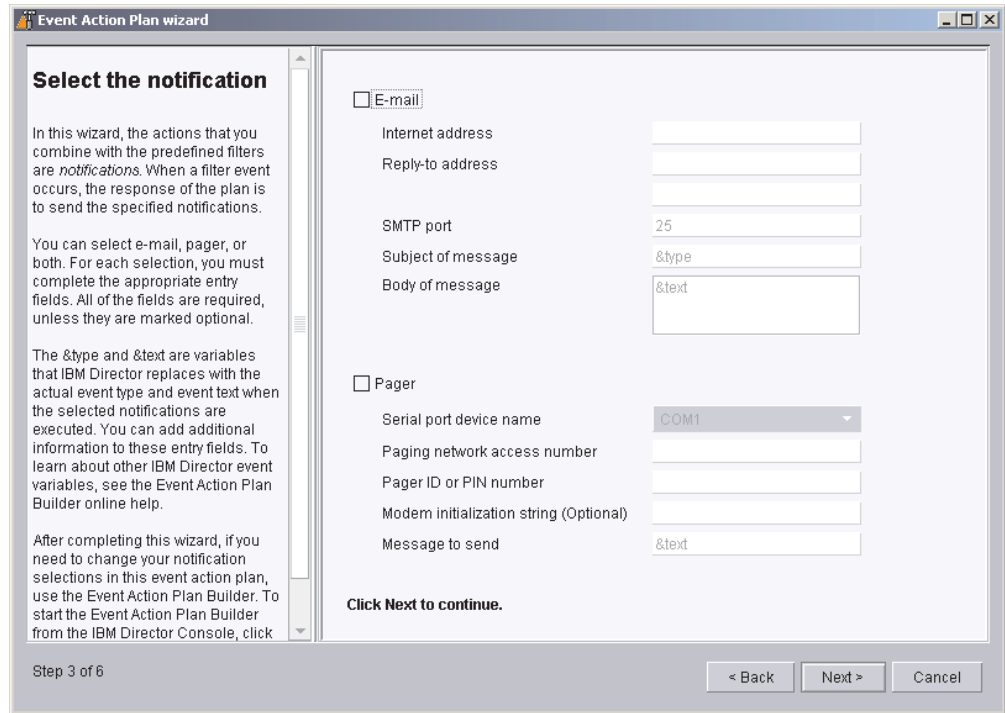


Figure 80. Event Action Plan wizard: “Select the notification” window

- If you want to be notified by e-mail when an event occurs, select the **E-mail** check box. Then complete the following entry fields:

Internet address

Type the e-mail address to which the notification will be sent.

Reply-to address

Type the e-mail address that will be displayed in the reply-to field of the e-mail.

SMTP port

Type the port number of the SMTP server. By default, the SMTP port is set to 25.

Subject of message

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.”

Body of message

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

“&type,” “&system,” “&time,” “&date,” and “&text” are event-data substitution variables. For information about other event-data substitution variables, see the *IBM Director 4.1 Systems Management Guide*.

6. If you want to be notified by pager, select the **Pager** check box. Then complete the following entry fields:

Serial port device name

Click the name of the serial port device.

Paging network access number

Type the telephone number that will be dialed when an event occurs.

Pager ID or PIN

Type the pager ID or personal identification number (PIN).

Modem initialization string (Optional)

Type the modem initialization string.

Message to send

Type the message that will be sent when an event occurs.

7. Click **Next**. The “Apply the event action plan” window opens.

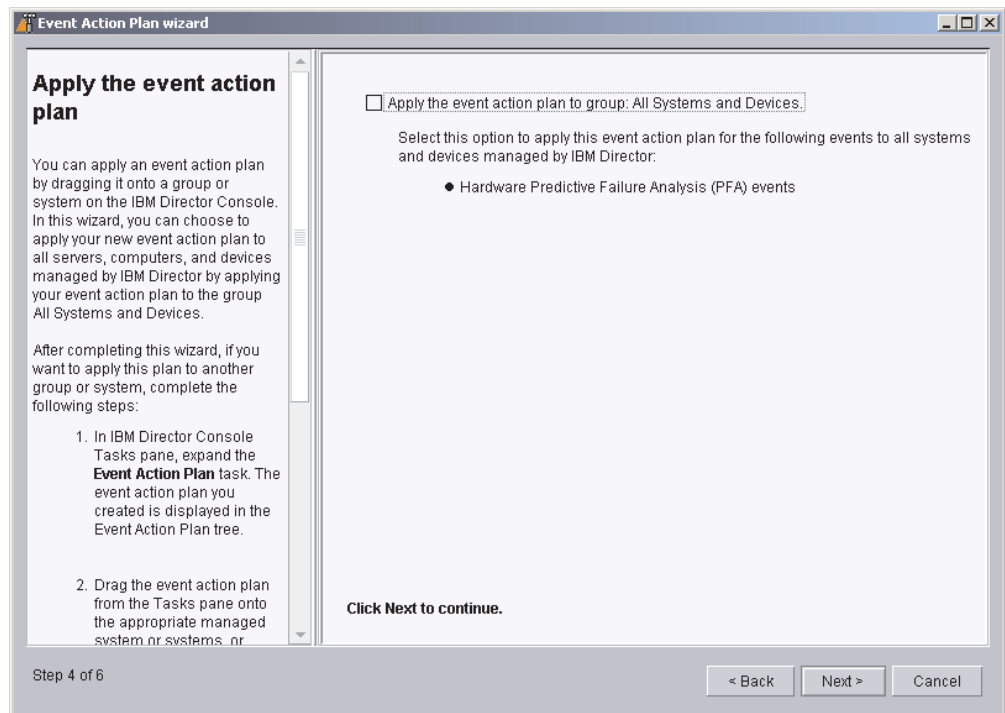


Figure 81. Event Action Plan wizard: “Apply the event action plan” window

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.

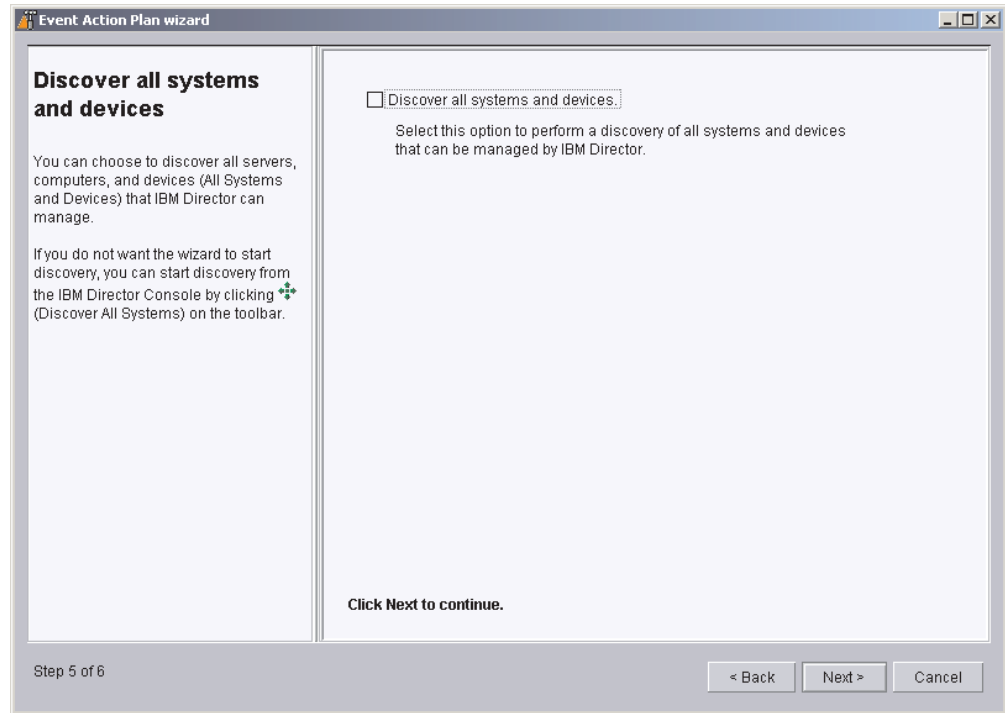


Figure 82. Event Action Plan wizard: “Discover all systems and devices” window

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.

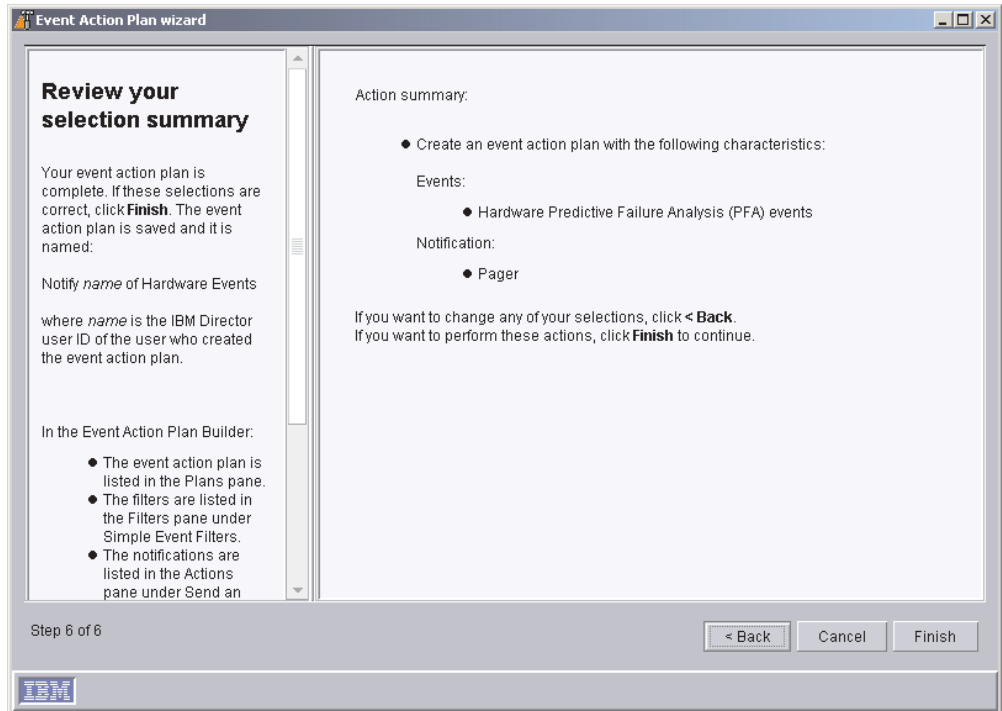


Figure 83. Event Action Plan wizard: “Review your selection summary” window

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 listen on 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 only available 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 only available for TCP/IP systems.

Broadcast relay agents

Broadcast relay allows the server to discover TCP/IP and IPX systems when the systems are not directly reachable by broadcast packets due to 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.

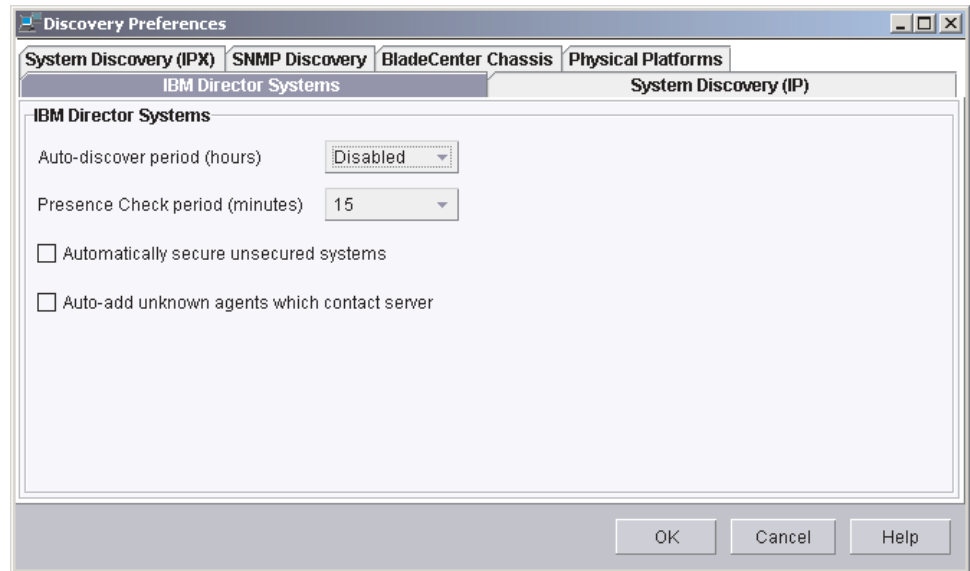


Figure 84. Discovery Preferences window

This window has six different 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

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

Manually creating a management processor object

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

- You have added an ASM PCI adapter to a server that contains an ASM processor.
- You have added 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, while the ASM PCI adapter and the Remote Supervisor Adapter serve as a gateway to the ASM interconnect network.

In order for IBM Director to manage the ASM PCI adapter or the Remote Supervisor Adapter, you must create a management processor object manually. Creating a management processor object enables you to do the following:

- 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.

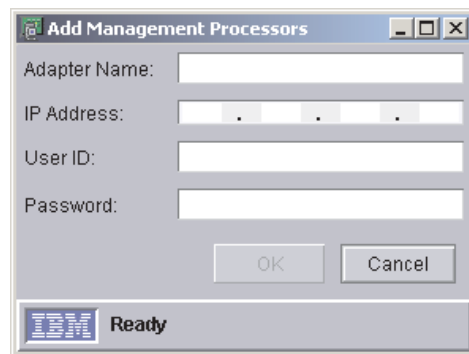


Figure 85. Add Management Processors window

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.

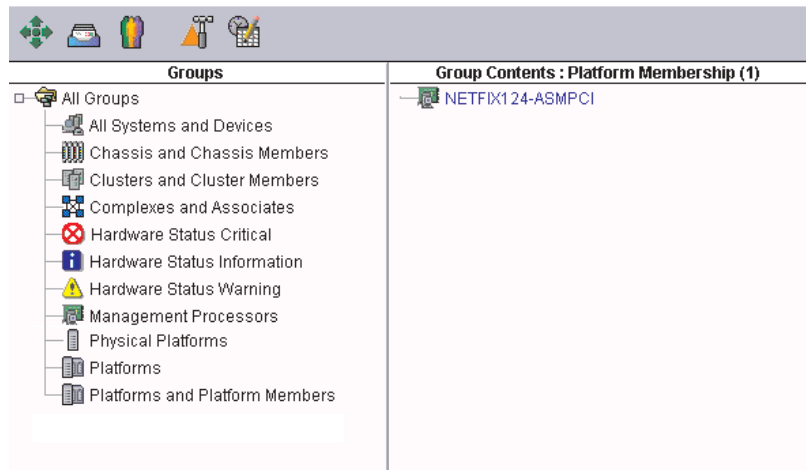


Figure 86. Management processor object displayed in the Group Contents pane

Authorizing IBM Director users

IBM Director Console uses the underlying operating-system user accounts for user-logout security. When a user logs into 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 underlying operating system. Members of the DirAdmin group have basic administrative privileges in the IBM Director environment, while 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 appropriate groups.

Once logged into IBM Director, users' ability to perform tasks depends on what access privileges they have been granted 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.

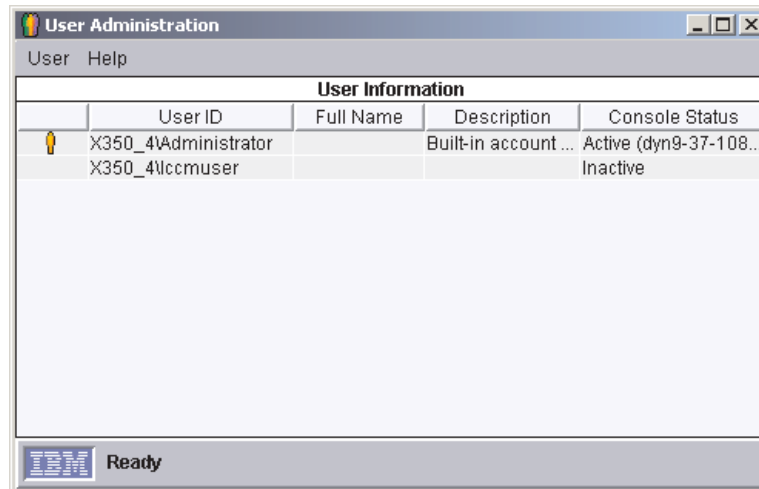


Figure 87. User Administration window

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

2. Click **User** → **User Defaults**. The User Defaults Editor opens.

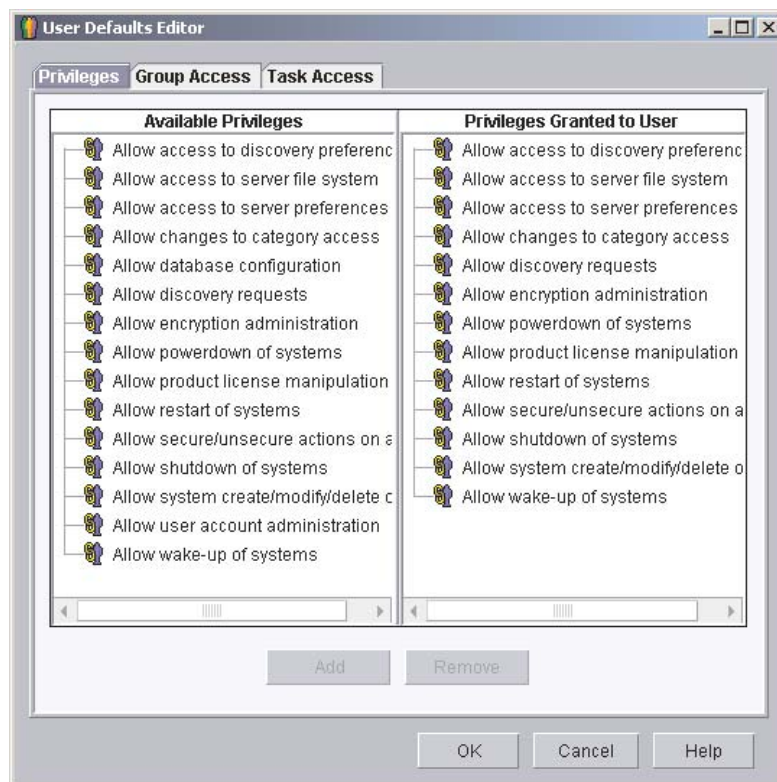


Figure 88. User Defaults Editor window

From this screen 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.

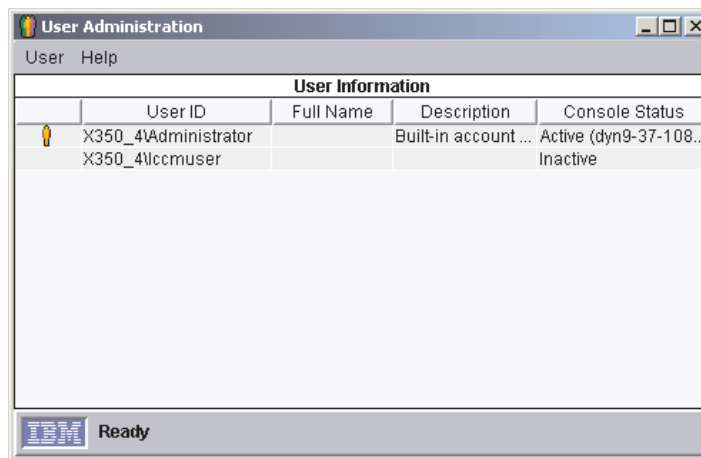


Figure 89. User Administration window

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.

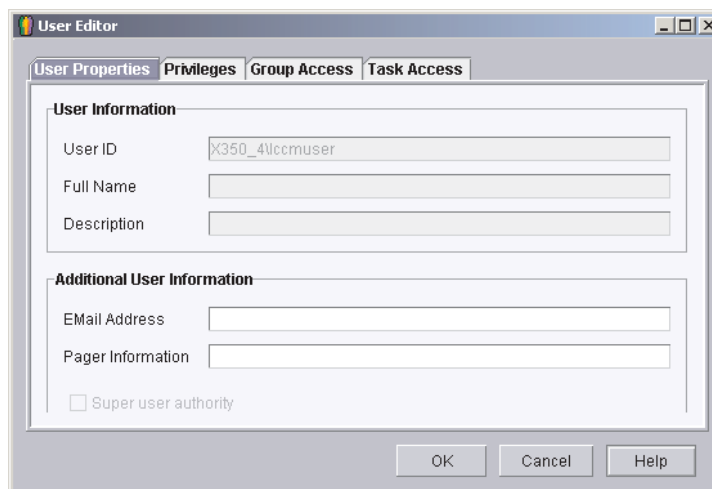


Figure 90. User Editor window: User Properties page

- 3. Click the **Privileges** tab. The Privileges page is displayed.

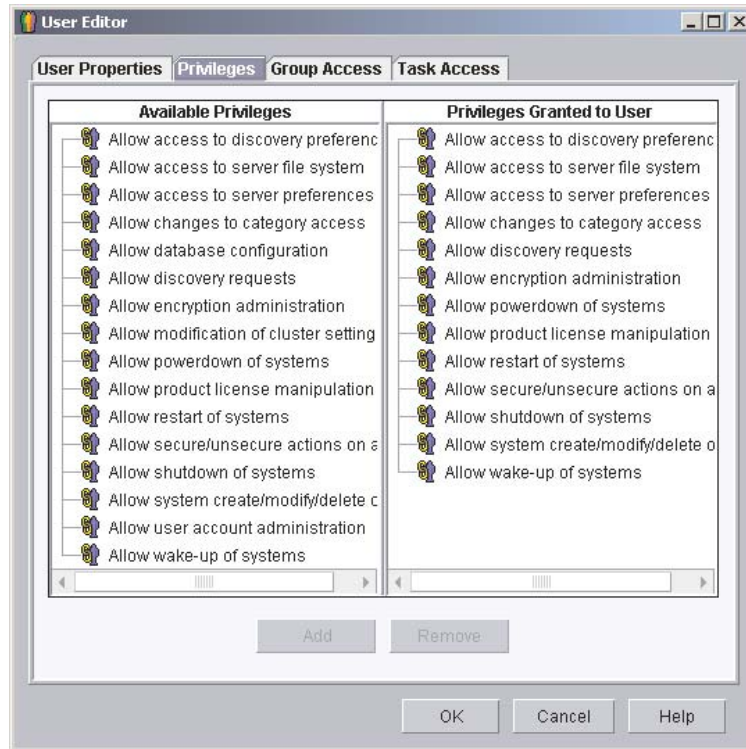


Figure 91. User Editor window: Privileges page

4. To add a privilege, click on the privilege in the **Available Privileges** pane and then click **Add**.
To remove a privilege, click on 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 92. 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.

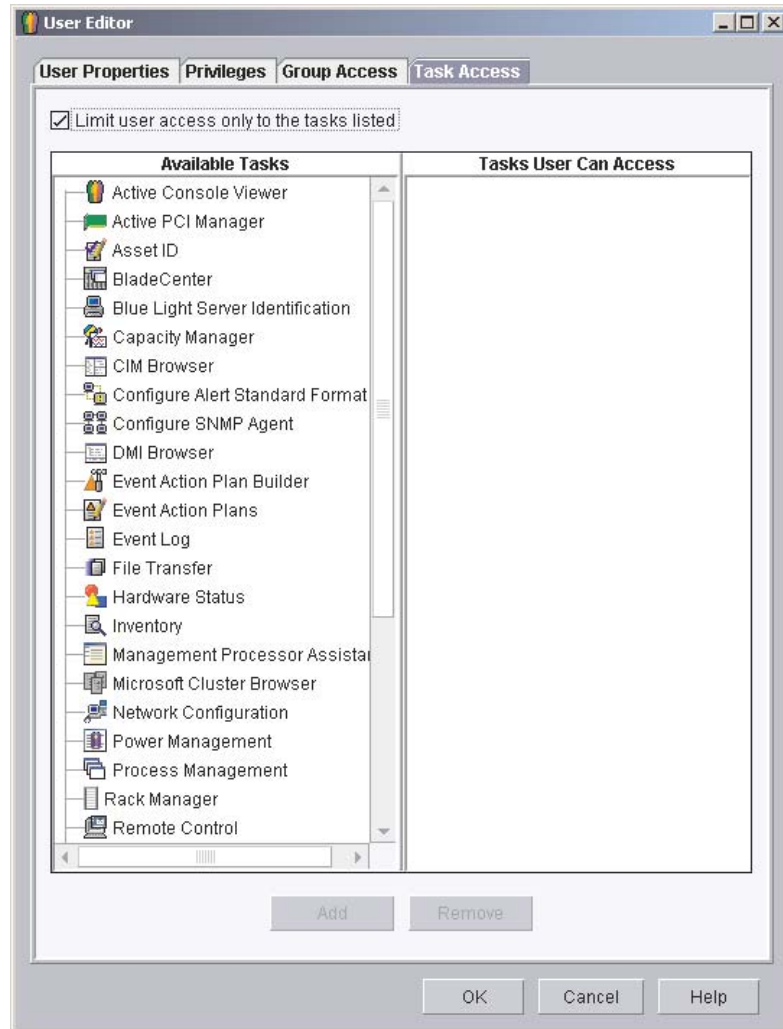


Figure 93. User Editor window: Task Access page

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	c:\Program Files\IBM\Director\data
For Linux	/opt/IBM/director/data/

where *c* 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	c:\Program Files\IBM\Director\data
For Linux	/opt/IBM/director/data/

where *c* 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 appropriate RSA or SHA certificate into the following directory:

For Windows	c:\Program Files\IBM\director\jre\lib\security\jssecacerts
For Linux	/opt/IBM/director/jre/lib/security/jssecacerts

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

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

For Windows	c:\Program Files\IBM\director\jre\bin
For Linux	/opt/IBM/director/jre/bin/keytool

where *c* is the hard disk on which IBM Director is installed. You can download information about the keytool program from <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	c:\Program Files\IBM\Director\data
For Linux	/opt/IBM/director/data/

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

6. Repeats steps 2 through 4 on page 128.

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 *c:/Program Files/IBM/Director/websrv/cgi-bin/*, where *c* 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 *c:/Program Files/IBM/Director/websrv/cgi-bin/*, where *c* 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.

Using software distribution

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.

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.

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 on page 131. 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.

Methods of software distribution

IBM Director 4.1 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 4.1 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 4.1 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 either must 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 choose 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 allows 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:

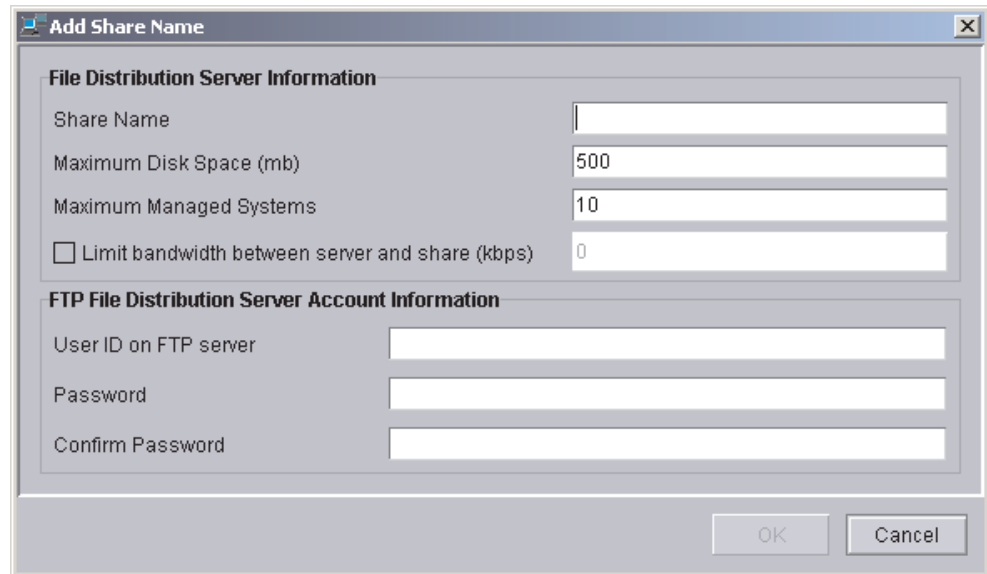
```
twgshare-a sharename
```

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 135.

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 the 'Add Share Name' dialog box. It has a title bar with a close button. The main area is divided into two 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' (empty), 'Password' (empty), and 'Confirm Password' (empty). At the bottom right are 'OK' and 'Cancel' buttons.

Figure 94. 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 (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, you must type additional information in the following fields:

User ID on FTP server

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

Password

Type the password associated with the user ID.

Confirm password

Confirm the password associated with the user ID.

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 Preferences window opens.

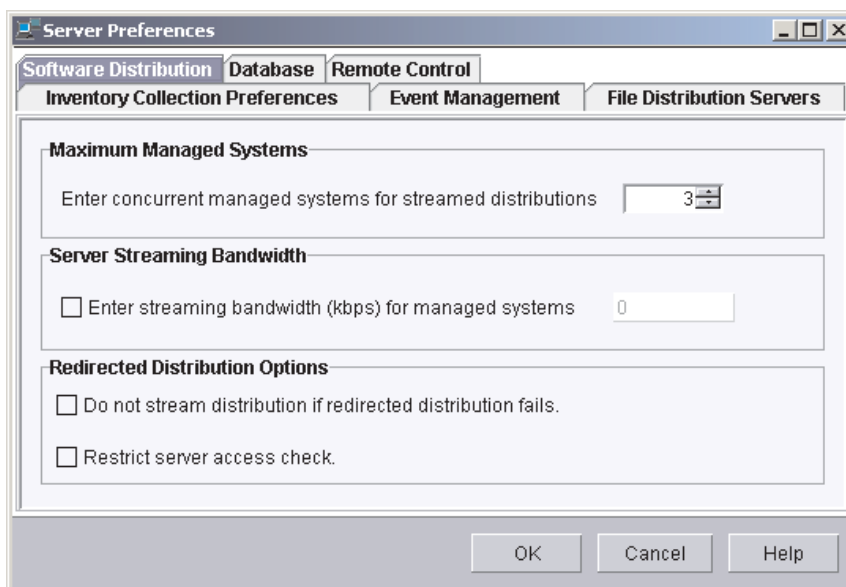


Figure 95. IBM Director Console: Software Distribution Preferences window

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 (kbps) for streaming packages from either IBM Director Server or a file-distribution server to the managed system.

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

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 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.

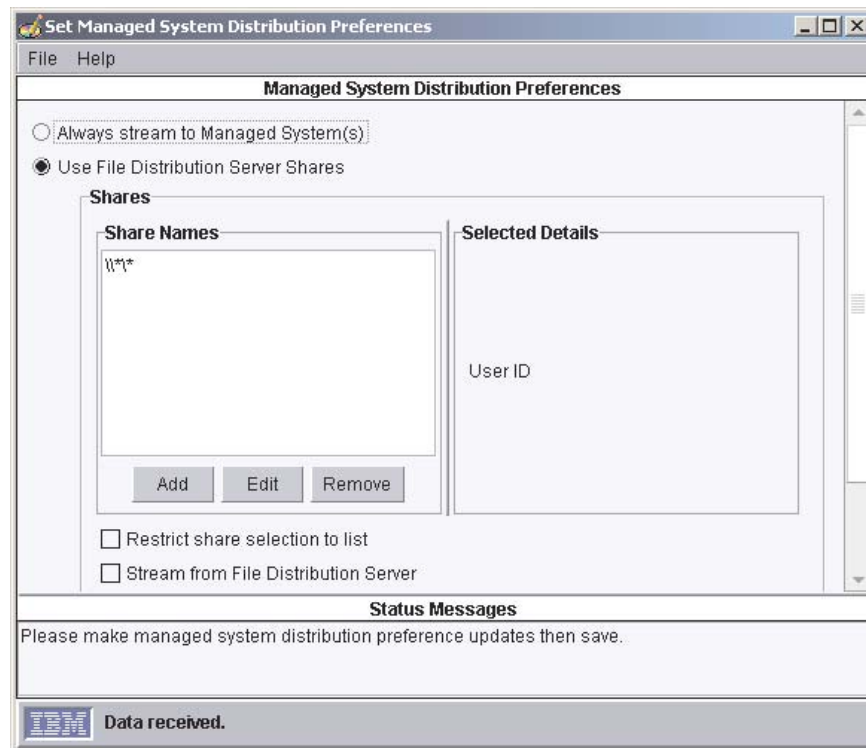


Figure 96. IBM Director Console: Managed System Distribution Preferences window

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 97. 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 (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 10. Installing the IBM Director Server Plus Pack 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 6.

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 149.

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 138. 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 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.

Note: Rack Manager does not contain an agent component. It must be installed only on the management server.

The following table lists the Server Plus Pack extensions that can be installed on managed systems and the operating systems on which they are supported.

Table 11. Supported operating systems for Server Plus Pack extensions installed on managed systems

Operating system	IBM Director Extensions
Windows 2000 Server, Advanced Server, and Datacenter Server (Service Pack 3 required)	<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 Linux Advanced Server, version 2.1 SuSE Linux, versions 7.2, 7.3, and 8.0	<ul style="list-style-type: none"> • Capacity Manager • Software Rejuvenation • System Availability
NetWare 6.0	<ul style="list-style-type: none"> • Capacity Manager
VMware ESX Server 1.5.2	<ul style="list-style-type: none"> • Capacity Manager • System Availability

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 and Caldera Open UNIX.

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 begins.
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:

- 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 on page 139 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 NetWare server 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.

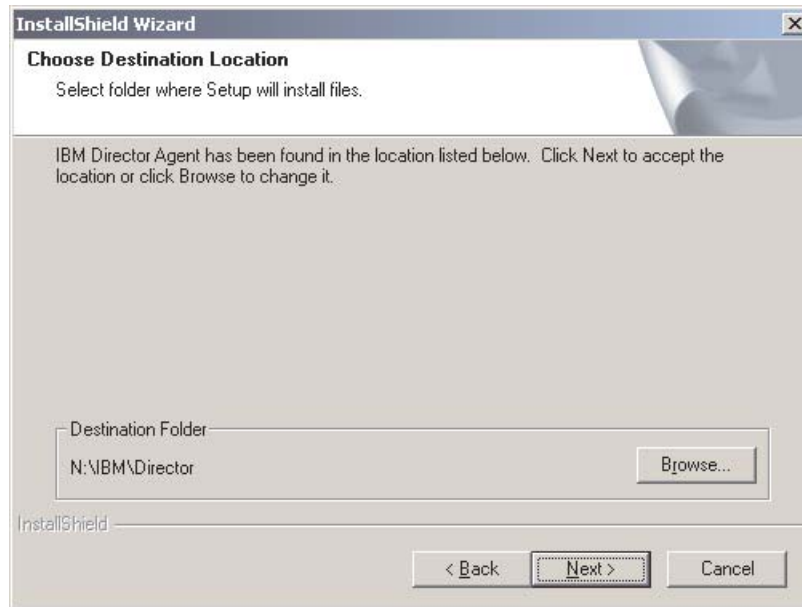


Figure 98. Installing Capacity Manager on NetWare: Choose Destination Location window

6. Click **Next**. The Start Copying Files window opens.

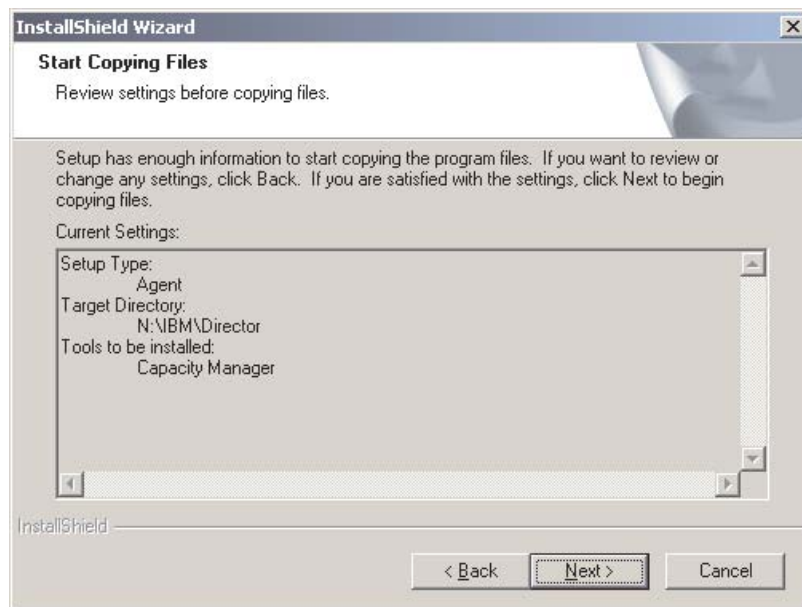


Figure 99. Installing Capacity Manager on NetWare: Start Copying Files window

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 NetWare server, 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, while 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, Update Assistant creates software packages. Then, you can use the IBM Director Software Distribution task to distribute the packages to the managed systems.

The name of the non-English XML files are similar to those listed above, with the addition of a language code. 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 appropriate 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 100. Creating a software package: Software Distribution Manager window (Standard Edition)



Figure 101. 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 102. Creating a software package: Director Update Assistant window

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**.

5. To select a file, click **Browse**. The IBM Update Package/Root Directory Location window opens.

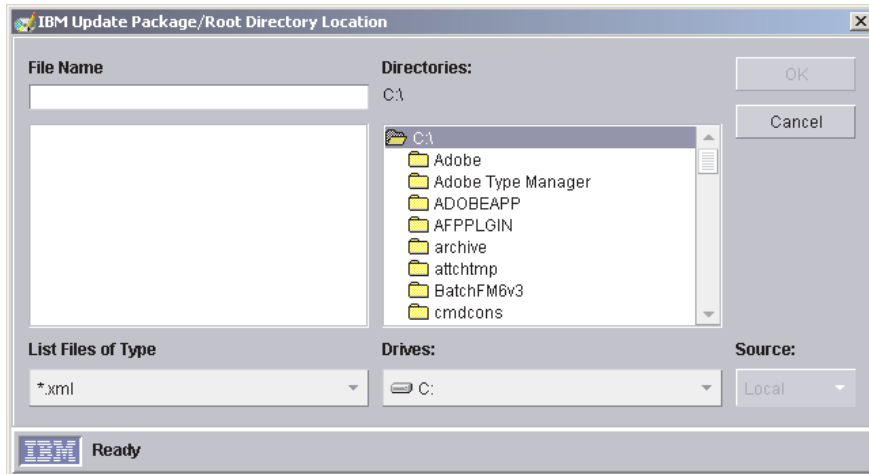


Figure 103. Creating a software package: IBM Update Package/Root Directory Location window

6. Locate the XML file and click it. The name of the XML file is displayed in the **File Name** field.

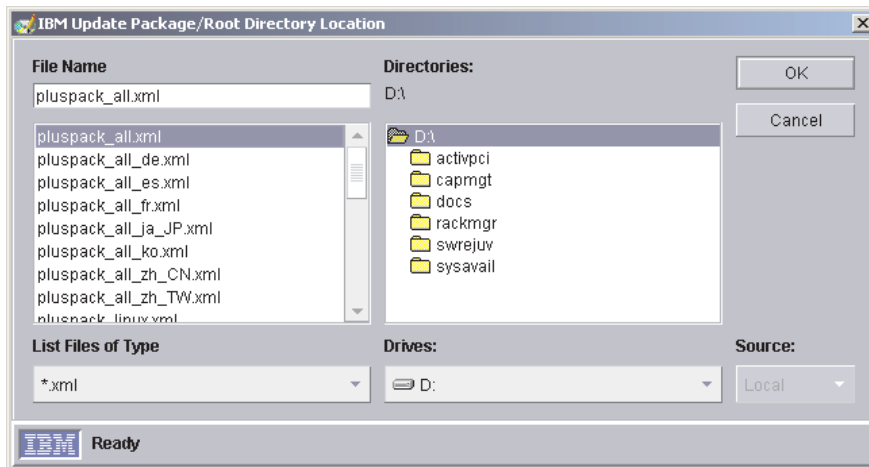


Figure 104. Creating a software package: IBM Update Package/Root Directory Location window

7. Click **OK**. The Director Update Assistant window reopens

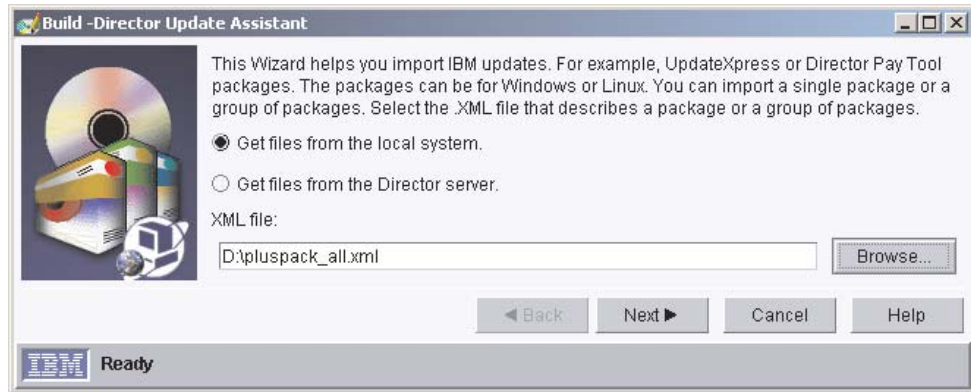


Figure 105. Creating a software package: Director Update Assistant window

8. Click **Next**. The second Director Update Assistant window opens.

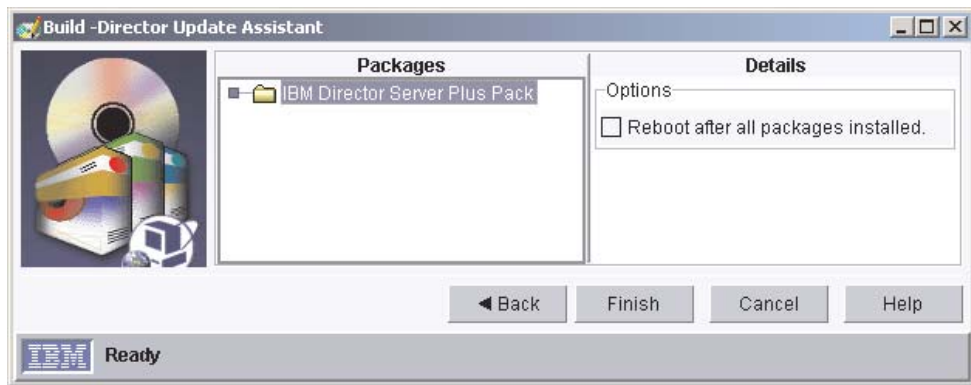


Figure 106. Creating software packages: Director Update Assistant window

9. 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 to the left of packages selected for installation; a red “X” is displayed to the left of update packages that are not selected.
To select an update package, double-click the package name.

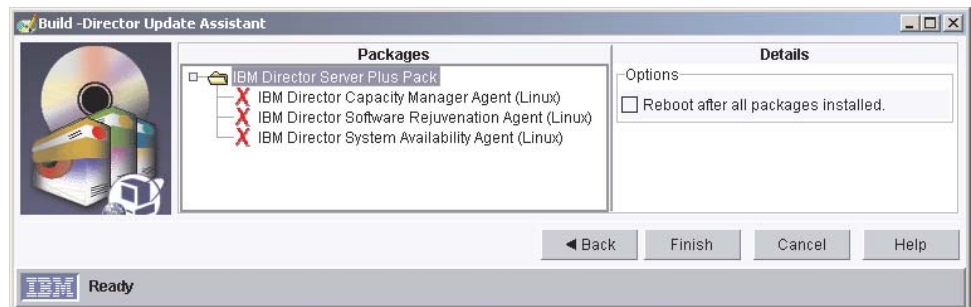


Figure 107. Creating software packages: Director Update Assistant window

- It is not necessary to select the **Reboot after all packages installed** check box. Installing the Server Plus Pack extension forces a restart, if needed.
10. Click **Finish**. As the packages are processed, a status message is displayed at the bottom of the window.

11. When the processing is completed, the software packages are displayed in the Tasks pane of IBM Director Console.

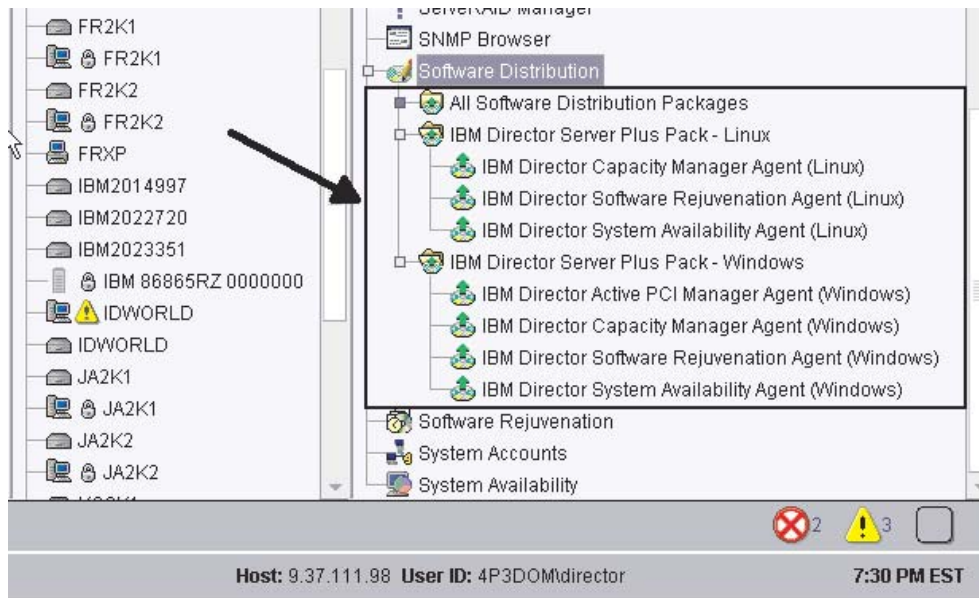


Figure 108. All Software Distributions Packages: IBM Director Server Plus Pack

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 tree.
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.

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.

A window opens.

4. When prompted “Do you wish to create a scheduled job for this task or execute immediately?”, click **Schedule** or **Execute Now**.
5. If you click **Execute Now**, the software package is distributed immediately. If you click **Schedule**, the New Scheduled Job window opens.

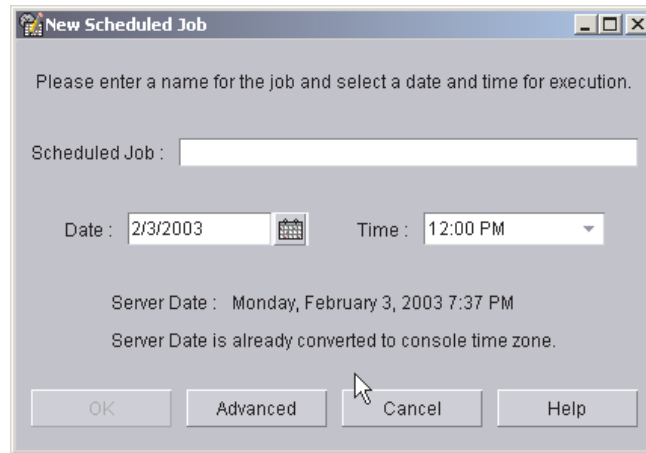


Figure 109. Scheduling the installation of a software package: New Scheduled Job window

You must enter information in the following fields:

Scheduled Job

Type a unique name for the job. This name is displayed in the Jobs pane of the Scheduler window.

Date Type the day you want the software package to be installed (MM/DD/YYYY format).

Time Type the time you want the software package to be installed.

For more information about the Scheduler task, see the *IBM Director 4.1 Systems Management Guide*.

6. Click **OK**. The Save Job Confirmation window opens.
7. Click **OK**.

Chapter 11. Modifying and uninstalling IBM Director 4.1

This chapter contains procedures for modifying and uninstalling IBM Director 4.1.

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

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.

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 26 for more information.

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 31. Steps 25 through 33 detail the process of selecting and configuring a database for use with IBM Director Server.

4. When the database installation is completed, restart IBM Director Server. Type the following command and press Enter:

```
net start twgipc
```

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.

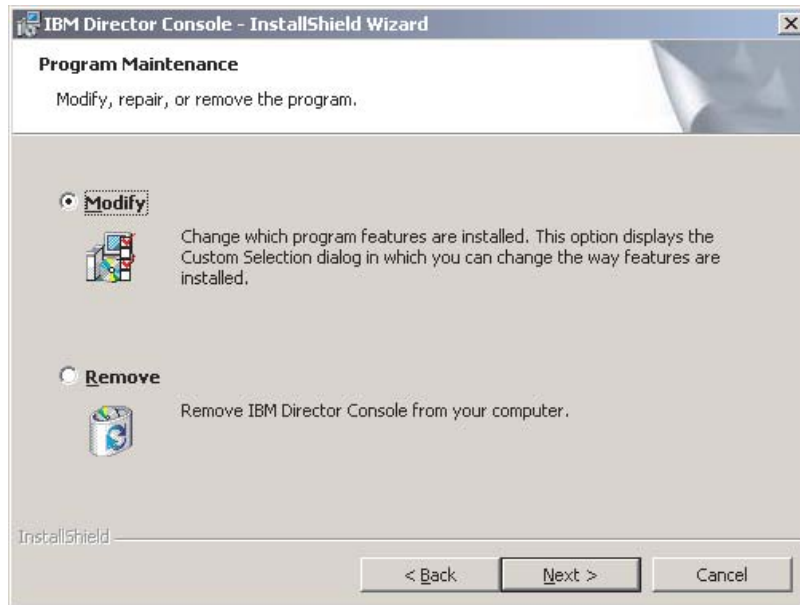


Figure 110. Program Maintenance window

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 31, “Installing IBM Director Console on Windows” on page 45, or “Installing IBM Director Agent on Microsoft Windows” on page 83.

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 26 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 onscreen instructions.
4. To restart IBM Director Server, type the following command and press Enter:
`/opt/IBM/director/bin/twgstart`

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/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 4.1* 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 4.1* 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.

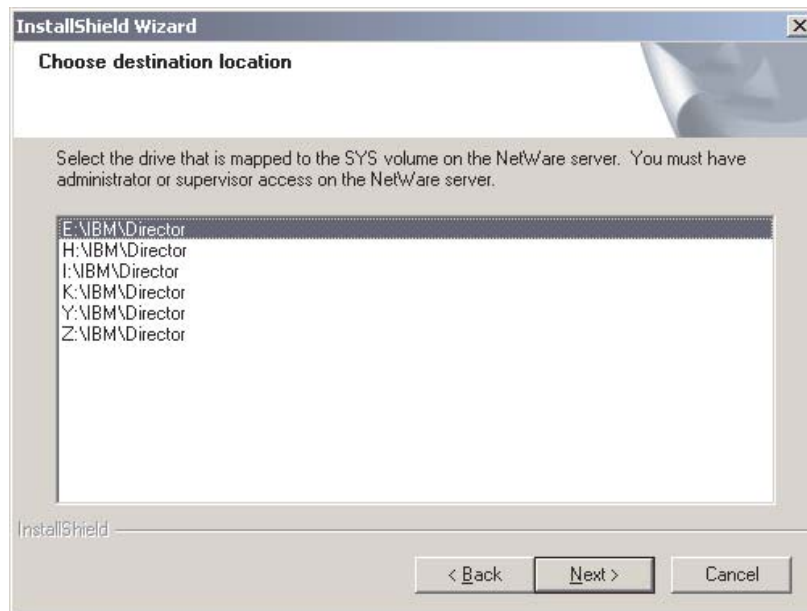


Figure 111. Modifying IBM Director Agent on NetWare: “Choose destination location” window

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

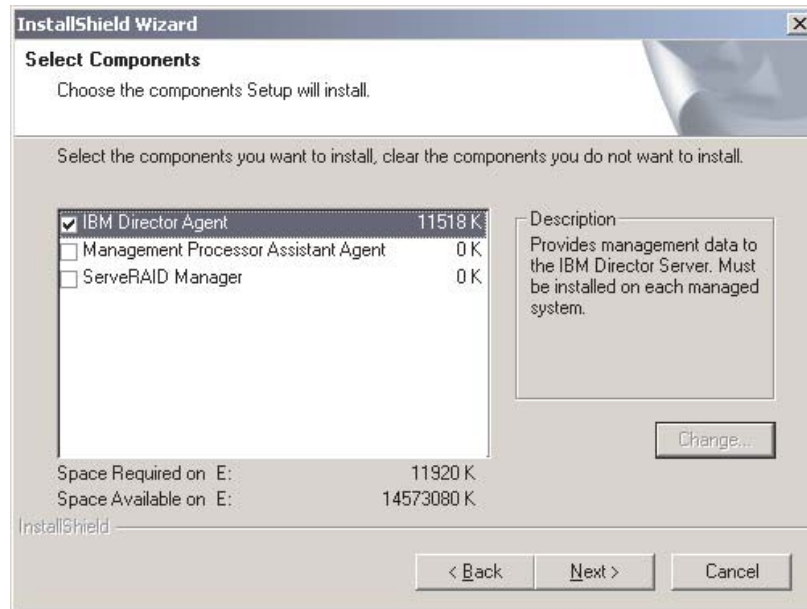


Figure 112. Modifying IBM Director Agent on NetWare: Select Components window

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 Wake on LAN, 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 4.1 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 4.1 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 4.1 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 4.1 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 4.1 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 4.1 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 to IBM Director Agent 4.1, 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 4.1 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 4.1 and `tivoliwg` if you upgraded from IBM Director Agent 3.x.

You also can use the standard `pkgm` commands.

Uninstalling IBM Director

You can use the following procedures to uninstall IBM Director.

Uninstalling IBM Director on Windows

Complete the following steps to uninstall IBM Director on Windows:

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 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:

- If installed, 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 uninstalling 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 4.1 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 4.1 and `tivoliwg` if you upgraded from IBM Director Agent 3.x. You also can use standard PKGRM commands. Consider the following:

- If installed, 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 12. 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 allows holders 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.

Once 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 what options were selected during the installation of IBM Director Agent.

By default, the files are located in the following directories.

Operating system	Directory
Windows XP and 2000	<code>c:\Program Files\IBM\Director\Data</code>
Red Hat Linux, SuSE Linux, VMware ESX	<code>/opt/IBM/director/data</code>
Caldera Open UNIX	<code>/opt/IBM/director/data</code>
NetWare	<code>c:\IBM\Director</code>

where `c` 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 what 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 decides to secure 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 a 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 XP and 2000	<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 159) into one of the following directories:

For Windows XP and 2000	<code>c:\Program Files\IBM\director\data</code>
--------------------------------	---

For NetWare	<code>c:\IBM\Director</code>
--------------------	------------------------------

where *c* is the hard disk where IBM Director Agent is installed, and IBM Director Agent is installed in the default directory.

6. Restart IBM Director Agent. From a command prompt, type one of the following commands and press Enter:

For Windows XP and 2000	<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 next to 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.

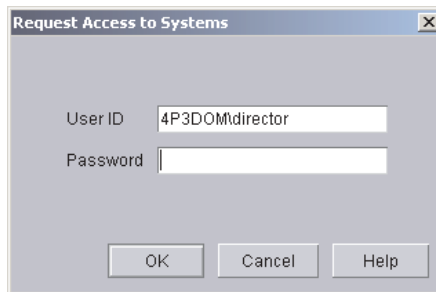


Figure 113. Request Access to Systems window

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. Stop IBM Director Agent. From a command prompt, type one of the following commands and press Enter:

For Windows XP and 2000	<code>net stop twgipc</code>
For Red Hat Linux, SuSE Linux, VMware ESX, or Caldera Open UNIX	<code>/opt/IBM/director/twgstop</code>
For NetWare	<code>unload twgipc</code>

5. Restart IBM Director Agent. Type one of the following commands and press Enter:

For Windows XP and 2000	<code>net start twgipc</code>
For Red Hat Linux, SuSE Linux, VMware ESX, and Caldera Open UNIX	<code>/opt/IBM/director/twgstart</code>
For NetWare	<code>load twgipc</code>

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:

- Setup 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.
- Setup the new server, install IBM Director Server, and copy the dsa*.pvt file from an existing trusted management server. This allows 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 which 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 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.

Chapter 13. Solving IBM Director problems

This chapter contains information about solving problems you might encounter with IBM Director 4.1.

The following table lists symptoms of problems and suggests possible solutions.

Symptom	Suggested action
Active PCI Manager	
After upgrading to IBM Director 4.1, Active PCI Manager appears to be available but does not work.	Complete the following steps to resolve the problem: <ol style="list-style-type: none"> 1. From the Add/Remove Programs window, remove all previous versions of Active PCI Manager. 2. Reinstall IBM Director 4.1. Be sure to install Active PCI Manager.
Alert Standard Format (ASF)	
(xSeries 345) ASF cannot be configured.	Complete the following steps to configure ASF on an xSeries 345: <ol style="list-style-type: none"> 1. Disable ASF from the IBM Director Agent Web-based Access or the management console. 2. Disable the network interface card for the adapter. ASF cannot be configured if the network interface card is disabled.
Common Information Model (CIM)	
When attempting to enumerate a system, large amounts of CIM data are returned causing errors in the CIM Browser.	Do not attempt to enumerate the instances of the following classes on Windows: <pre>root/cimv2:CIM_DirectoryContainsFile root/cimvw:Win32_Subdirectory</pre> These 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.
Databases	
The Microsoft Jet database is full.	Migrate to a larger database such as IBM DB2, Oracle, or Microsoft SQL.
When an Oracle database is used, errors occur during the Database Configuration process.	Configure and start the Oracle TCP/IP listener <i>before</i> starting the Database Configuration dialog. If a failure occurs, check the configuration of the TCP/IP listener.
The database application failed on a BladeCenter unit. If you change the database application after configuring the BladeCenter unit, inventory errors might occur.	To resolve this problem, use one of the following two procedures: <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.
When using Telnet to access a Linux environment through a Windows operating system, and then running the cfgdb utility, messages overlay. This is a result of a small screen size.	To resolve this problem, use the following procedure: <ol style="list-style-type: none"> 1. Set the environmental variable term to vt100 before running the cfgdb utility. 2. Maximize the Telnet window to its largest size possible.
Dialog boxes	
Tables appear too small in a pane.	Change the table settings to enlarge the table in the pane. Note: Modified table settings are not saved.

Symptom	Suggested action
Discovery	
BladeCenter discovery does not function properly when multiple network interface cards are enabled.	<p>To resolve this problem, try one of the following:</p> <ul style="list-style-type: none"> Change the network interface card that is attached to the BladeCenter chassis network. You might have to search to find the working network interface card. Disable the network interface cards that are not connected to the management module and then perform a discovery. When the discovery is completed, enable the network interface cards. You must do this each time you perform a discovery.
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>Verify that you are using the correct criteria when you create the dynamic group. Each criterion searches only the rows in the table with which it is associated. For example,</p> <ul style="list-style-type: none"> If you select a criterion of Inventory (PC)/SCSI Device/Device Type=TAPE only the managed systems that appear in at least one row in the SCSI_DEVICE table that also have a value of TAPE in the DEVICE_TYPE column are returned. If you select a criterion of Inventory (PC)/SCSI Device/Device Type ^= TAPE only the managed systems that appear in at least one row of the SCSI_DEVICE table, of which none of those rows have a value of TAPE in the DEVICE_TYPE column, are returned. This does not necessarily return all managed systems that do not have SCSI tape drives. Only managed systems that appear in a particular table and that meet the criteria for that table are returned.
Encryption	
Certain managed systems cannot be managed.	<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 are no longer able to be managed. These systems will relock after a short period of time. Request a presence check to force the managed system to relock.
Event action plans	
Group event action plans are not displayed.	<p>Verify that a managed system or group has an event action plan assigned to it:</p> <ol style="list-style-type: none"> In IBM Director Console, click Associations → Event Action Plans. In the Groups pane, click All Groups. In the Group Category Contents pane, expand each group that has an event action plan applied to it to view the event action plans that are applied to the group. <p>Event action plan associations are not displayed in the Groups pane, nor are event action plans that have been applied to a group displayed as being associated with each individual managed system that is a part of that group. The event action plan is displayed as being applied to the group only.</p>

Symptom	Suggested action
Event log message	
An event ID 2003 warning message appears in the application event log.	<p>If you are using Windows 2000 with Internet Information Services (IIS) installed, an event ID 2003 warning message might appear in the application event log when you start System Monitor and add counters. The event ID 2003 warning message appears as follows:</p> <p>The configuration information of the performance library "C:\WINNT\system32\w3ctrs.dll" for the "W3SVC" service does not match the trusted performance library information stored in the registry.</p> <p>The functions in this library are not recognized as trusted. Microsoft previously identified that this is a problem in these products.</p>
Field-replaceable unit	
FRU information does not appear when inventory is collected.	Verify that the GETFRU command can reach the IBM Support FTP site through your firewall. For the GETFRU command to succeed, the managed system must have firewall access through a standard FTP port. For more information, see Appendix B, "Obtaining FRU data files using the GETRU command," in the <i>IBM Director 4.1 Systems Management Guide</i> .
Hard disk drives geometry reporting	
The following report is created indicating that an insufficient amount of space is available on a hard disk drive: Win32_DiskDrive.Size is less than Win32_DiskPartition.Size for a removable medium that has been formatted as a single partition.	<p>The following hard disk drives are not supported by a Windows operating system:</p> <ul style="list-style-type: none"> • Optical • Iomega • Jaz <p>This is previously identified by Microsoft as a Windows Management Instrumentation (WMI) problem.</p>
Hot plugs	
When using the hot-plug feature, the status of the slot does not update.	To update the status of the hot plug, the server must be restarted. This is a limitation of the CIM provider.
IBM Director Agent	
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. The system is using a Broadcom Gigabit Ethernet network interface card.	<p>Complete the following steps to resolve this problem:</p> <ol style="list-style-type: none"> 1. Open the AUTOEXEC.NCF file. 2. Change CHECKSUM=OFF to the following: <pre>LOAD B57.LAN SLOT=10012 FRAME=ETHERNET_II NAME=B57_1_EII LOAD B57.LAN SLOT=10012 FRAME=ETHERNET_802.2 NAME=B57_1_E82</pre>

Symptom	Suggested action
IBM Director Console	
Managed systems are unavailable on the management console.	<ul style="list-style-type: none"> Verify 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 using: <ul style="list-style-type: none"> Windows: Go to twgipccf.exe and change the timeout value Linux: In the data directory, under the products install root, edit the ServiceNodeLocal.properties file. Add ipc.timeouts=x where x is the specified number of seconds. The default setting is 15 seconds. <p>If you are using UNIX or Linux and IBM Director Agent is installed in the default directory, you must restart IBM Director Agent. At a command prompt, type</p> <pre>/opt/IBM/director/bin/twgend -r</pre> <p>to stop and restart IBM Director Agent.</p>
An input/output error connecting-to-server message appears when IBM Director Console is started.	Make sure that IBM Director Server is running before starting IBM Director Console. A green circle icon in the task bar is displayed to indicate that you can start IBM Director Console. Do not attempt to start IBM Director Console if the red diamond icon (indicating that the server is not responding) or the green triangle icon (indicating that the server is still in the process of starting) appear in the task bar.
Errors occur during attempts to log on to the management server using IBM Director Console	<p>For Windows, verify that:</p> <ul style="list-style-type: none"> 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. <p>For Linux: A green circle is not displayed in the task bar, but there is a Linux command-line command that you can use called twgstat. This reports the status of the management server. You can log on to the management console when twgstat returns a status of Active. The twgstat command returns the following statuses:</p> <ul style="list-style-type: none"> 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.
A request for access fails, and the managed systems remain locked.	<ul style="list-style-type: none"> Determine whether the managed system and management server accept encrypted communications only. Ensure that the server has encryption enabled through the Encryption Administration window. If the managed system has a UNIX or Linux operating system, ensure that the password encryption method is set to Message Digest 5 (MD5).

Symptom	Suggested action
Through the use of imaging, a system was added and is displayed on the management console as a duplicate of a system that was previously added.	Verify that the Unique ID attribute is enabled.
IBM Director Server	
(Windows only) IBM Director Server does not start.	<ul style="list-style-type: none"> • Determine whether a service is failing that might prevent IBM Director Server from starting. Double-click the IBM Director icon on the task bar to determine whether there are any failing services. • Verify that the IBM Director Server service ID password and user account are valid. You always must use the same administrator password and user account for IBM Director Server and the IBM Director Server service. Complete the following steps to change the user account or password for the service: <ol style="list-style-type: none"> 1. Click Start → Programs → Administrative Tools. 2. Double-click Services. 3. Right-click IBM Director Server. 4. Select Properties. Click Log On. 5. Select the This account check box, and modify and confirm the password. 6. Click OK, and then restart the IBM Director Server service.
A problem occurs on servers running Microsoft Windows 2000 when the NetBIOS protocol is present and IBM Director is installed. Errors are generated until the event log is full.	To resolve this problem, uninstall and then reinstall the network interface card device driver.
After IBM Director Server is installed on a server running Microsoft Windows 2000 Server, an error is displayed in the event log when the server is restarted.	<p>The open procedure for service PerfDisk in the DLL C:\WINNT\System32\perfdisk.dll has taken longer than the established wait time to complete. There might be a problem with one of the following:</p> <ul style="list-style-type: none"> • The extensible counter • The service from which the counter is collecting data • The system might have been busy when the call was attempted. <p>To resolve this problem, use the REGEDIT command and modify the following key entry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance key "Open Timeout" Change the Decimal value to 30000. This gives the system enough time to complete the start up task before starting the PERF counters.</p>
IBM ThinkPad	
IBM Director Agent installation process is not completed.	When you install IBM Director Agent on a ThinkPad computer, you must restart the computer twice to complete the installation. Otherwise, Windows Management Instrumentation (WMI) does not function properly.

Symptom	Suggested action
Installation	
When installing IBM Director Server, the following message is displayed: Error 1722. There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor.	A possible reason for this error is that the display for a system running IBM Director Server or IBM Director Console must support at least 256 colors. Increase the display color palette to more than 256 colors, uninstall the previous partial install and reinstall IBM Director Server.
Java Runtime Environment (JRE) Exceptions	
Intermittent JRE exceptions occur	Verify that you have sufficient memory. Intermittent JRE exceptions might occur when you run IBM Director Console on systems that are memory constrained. Sun Microsystems previously identified that this is a problem in some products. For more information about memory requirements, see the <i>IBM Director 4.1 Installation and Configuration Guide</i> .
Mass Configuration	
When using Mass Configuration to configure Asset ID, a problem can develop if the system being configured is low on data space.	When the size of the configuration is larger than that of the data space remaining, the configuration fails without any indication that this failure occurs. This is a limitation of the data save area. Ensure that for each byte of data you have the same amount of space in your data save area.
Pre-Advanced Configuration and Power Interface (ACPI) servers (Netfinity 7000)	
When Shut Down is selected from the Start menu, a power off message is displayed.	Shutdown might fail on a Netfinity 7000 server running Windows 2000. This does not power off the system automatically.
SNMP devices	
SNMP devices are not being discovered.	Verify that: <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 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 100% of the devices. If a device has not communicated with other managed systems, the device might not be discovered.

Symptom	Suggested action
An attribute value for a MIB file cannot be changed.	Verify that: <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 you can set to be displayed in the SNMP Browser. • The compiled MIB file is associated with the value to change.
When a MIB file attribute value is set to a hexadecimal, octal, or binary value, the file fails.	Verify that all of the values have been converted and are being added in a decimal format.
SNMP traps	
Trap destinations are missing from the SNMP agent table. Note: IBM Director sends and receives SNMP traps using TCP/IP only.	A table displays only the first trap destination in the SNMP configuration interface when there are multiple communities and traps associated with each community. The IBM Director CIM-based inventory stores only the first value of an array-valued property (such as the SNMP trap destination).
Security	
Load All Events does not function.	When the security log gets very large (approximately 4000 records), clicking Load All Events produces the Loading data...please wait message. After approximately 5 minutes, the message stops, and only the 30 most recent events are displayed. The Load All Events button is not enabled.
Software Distribution	
The software package creation fails.	Check the available disk space on the management console. Packages are created on the management console before being written to the target system. If disk space is insufficient on the management console, the package creation fails.
Remote Control fails when distributing software packages to managed systems that are behind a firewall.	Remote Control and Software Distribution both use session support to increase data transmission. Session support within TCP/IP causes data to flow through a nonreserved port that is different from the one that IBM Director typically uses for communication. Most firewalls do not allow the data to be transmitted through this other port. You can disable session support by creating an INI file on the managed system. In the IBM\Director\bin directory on the managed system, create a file named tcpip.ini that contains the following command line: <code>SESSION_SUPPORT=0</code> If more than one TCP/IP option is selected in the Network Driver Configuration of the managed system, you must create an INI file for each entry. Name these files tcpip.ini, tcpip2.ini, tcpip3.ini, and so on. After creating the files, restart the managed system.
An error message is displayed when a software package is distributed using a redirector share.	The error message is: Managed System (system name) has detected that software package (package name) was not found on share (\\server\share). You can delete software packages from the management server. The redirector cache can be maintained only through the File Distribution Server Manager interface. This is accessed by right-clicking the Software Distribution task. Errors occur if you manipulate the cache through any means other than IBM Director Console.

Symptom	Suggested action
Software packages are not distributed or installed from the file-distribution servers.	Ensure that the file-distribution server is a member of the same domain as the management server or has a trust relationship with that domain.
The software package installation failed, and the location of the package must be changed.	Reinstall IBM Director Agent, and specify a different drive and directory.
Sun Java plug-ins	
After you login to Microsoft Internet Explorer, a Java security warning is displayed.	If you are using Microsoft Internet Explorer with the Sun Java plug-in for Web-based Access there are additional prompts that appear when you login to a managed system. After you login to Microsoft Internet Explorer, a Java Security Warning is displayed. Select Grant this session . The Java plug-in requires authentication information. Enter the same information that you used for the Microsoft Internet Explorer login.
Time zone	
The wrong time zone is displayed.	When the time zone is changed, a managed system does not adjust the time shown in the event viewer. Start the managed system again to show the correct time for the new time zone.
Uninstalling IBM Director	
The following message is displayed: Error 1306: Another application has exclusive access to the C:\Program Files\IBM\Director\log\esnt evt.dat	Shut down all other applications; then, click Retry . Cancel the uninstallation and restart the server. Then, start the uninstallation again.

Symptom	Suggested action
Web-based Access	
<p>Web-based Access is unavailable and an error message is displayed indicating that the page cannot be found.</p>	<p>If you install Web-based Access on a managed system that is running Apache Web Server, you must modify the Web-based Access configuration files. Web-based Access and Apache Web Server use the same default connector ports.</p> <ol style="list-style-type: none"> 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 c:\Program Files\IBM\Director\webserv\conf, where c is the hard disk drive where IBM Director is installed. 3. Change the server port: Server port="8005" You must specify a port that is not already in use by another application. 4. Change the connector port: port="8009" You must specify a port that is not already in use by another application. 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 located at c:\Program Files\IBM\Director\webserv\conf, where c is the hard disk drive where IBM Director is installed. 7. Change the connector port: port="8009" You must specify a port that is not already in use by another application. 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 located at c:\Program Files\IBM\Director\webserv\conf, where c is the hard disk drive where IBM Director is installed. 10. Change the connector port: port="8009" You must specify a port that is not already in use by another application. 11. Save the modified tomcat.conf file. 12. Restart the IBM Director Agent Web Server service.
<p>A system running Microsoft Windows XP that does not have Java installed displays a message that the Java Virtual Machine (JVM) is needed to view a managed system.</p>	<p>To resolve this problem, install Microsoft Windows XP Service Pack 1.</p>

Symptoms	Suggested actions
Windows NT	
<p>Printing problems occur when IBM Director 3.1 Agent is installed on managed systems that are using a Windows NT operating system.</p>	<p>Using a print server or printer with IBM Director 3.1 Agent installed and a Windows NT operating system might require a setup that specifically uses local queues. When the printer configuration of the management console is connected directly to a network print queue (if the printer is not associated with a port), you will probably encounter errors when printing from IBM Director Console. If printer errors are encountered, complete the following steps to set up a printer that uses a local printing queue:</p> <ol style="list-style-type: none"> 1. Set up a local device that points to the network printer. 2. Map the local LPT device to the network printer and create a local print queue. From a command prompt type <pre>NET USE LPT1: \\printer_server\printer/persistent:yes</pre> <p>Where printer_server is the network server and printer is the local printer.</p> 3. Add the local printer. 4. Specify the local device (LPT1), and configure the new printer.

Appendix A. Terminology summary and abbreviation list

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

IBM Director terminology summary

The following terminology is used in the IBM Director publications.

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

IBM Director software is made up of three main components:

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

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

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

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

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

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

Abbreviation and acronym list

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

Table 12. Abbreviations and acronyms used in IBM Director

Abbreviation or acronym	Definition
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI adapter
BIOS	basic input/output system
CIM	Common Information Model
CIMOM	CIM Object Manager
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management
CSV	comma-separated value

Table 12. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
DES	data encryption standard
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DMI	Desktop Management Interface
DNS	Domain Name System
DSA	Digital Signature Algorithm
EEPROM	electrically erasable programmable read-only memory
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	file transfer protocol
GB	gigabyte
Gb	gigabit
GUI	graphical user interface
GUID	globally unique identifier
HTML	hypertext markup language
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPX	internetwork packet exchange
ISDN	integrated services digital network
ISMP	integrated system management processor
IIS	Internet Information Services
JVM	Java Virtual Machine
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JFC	Java Foundation Classes
JRE	Java Runtime Environment
KB	kilobyte
Kb	kilobit
Kpbs	kilobit per second
KVM	keyboard/video/mouse
LAN	local area network
LED	light-emitting diode
MAC	media access control
MB	megabyte
Mb	megabit
Mbps	megabits per second
MD5	message digest 5

Table 12. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
MDAC	Microsoft Data Access Control
MHz	megahertz
MIB	Management Information Base
MIF	Management Information Format
MMC	Microsoft Management Console
MPA	Management Processor Assistant
MSCS	Microsoft Cluster Server
MST	Microsoft software transformation
NIC	network interface card
NNTP	Network News Transfer Protocol
NVRAM	nonvolatile random access memory
ODBC	Open DataBase Connectivity
OID	object ID
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PFA	Predictive Failure Analysis
RAM	random access memory
RDM	Remote Deployment Manager
RPM	Red Hat Package Manager
SID	(1) security identifier (2) Oracle system identifier
SLP	service location protocol
SMBIOS	System Management BIOS
SMI	System Management Information
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SNMP	Simple Network Management Protocol
SNA	Systems Network Architecture
SPB	software package block
SQL	Structured Query Language
SSL	secure sockets layer
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
UDP	User Datagram Protocol
UID	unique ID
UIM	upward integration module
UNC	universal naming convention

Table 12. Abbreviations and acronyms used in IBM Director (continued)

Abbreviation or acronym	Definition
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 B. Creating custom database tables for CIM, DMI, and MIF inventory data

IBM Director stores inventory data in database tables. You can customize these database tables to include inventory data from CIM, DMI, and static MIF files.

For information about setting up a managed system to generate MIF files appropriate for the inventory collector, see “Generating MIF files for inventory collection” on page 191.

To create a custom database table, you must create the following files:

Table property file

This defines the contents of a custom database table. A table property file contains the table name, the column names and column types, and other information. For information about table property file syntax, see “Creating table property files”.

Inventory extension property file

This associates IBM Director inventory collectors with the custom database tables. Without inventory extension property files, IBM Director cannot map the inventory data from the CIM, DMI, or MIF inventory collectors to your custom tables. For information about the inventory extension property file format, see “Creating inventory extension property files” on page 184.

Translated string file

(Optional) This contains the translated strings for your table property file. If you want your custom database tables translated, IBM Director uses the strings from the translated string files when appropriate. For information about translated string file format, see “Creating translated strings files” on page 186.

Note: You can supply translated strings only for languages supported by IBM Director.

After creating these files, you must copy them to specific directories on the management server. When IBM Director Server starts, it loads the table property and inventory extension property files. Then, it initializes the custom database tables defined by these files. For more information, see “Initializing custom tables” on page 188.”

Creating table property files

You can create and edit a table property file using an ASCII text editor. Table 13 on page 181 list the properties that you can use.

Table property files must be located in the UserTables directory on the management server. If you installed IBM Director in the default location, the path is c:\Program Files\IBM\Director\Data\UserTables. This directory also includes examples of table property files. The example files have the following file extension: .TWGdbt.sample.

The syntax of a property file consists of a property name and its associated value, separated by an equal sign. Each property must be on a single line. The following example defines three properties:

```
table.realname = IBM IBM Director 4.1
table.token = MyCustomTable
table.shortname = Director
```

While the parser catches most errors, some errors can be interpreted as valid properties. Simple mistakes can cause unexpected behavior. When creating a table property file, remember the following considerations:

- You must type property names in lowercase letters.
- The values for tokens, realnames, and shortnames must contain only the following characters:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_).
- Leading or trailing white space is ignored.
- Spaces within the property value are preserved.
- The first equal sign or space separates the property name and value. Any subsequent equal signs or spaces in a property definition are added to the string for that property value, except for white space which surrounds a separator.
- Use the hash character (#) to insert comments. For example, you can comment out the table.shortname property by starting the line with a hash character:
#table.shortname = Director
- If a property value exceeds a line, the remainder of the value is misinterpreted as a new property definition. For example, if the hardware.type property value is split between two lines, “with” is misinterpreted as a new property:
hardware.type = Generic workstation
with 128MB RAM.
- If a space is inserted into a property name, part of the property name is misinterpreted as its value. For example, if the table.shortname property name contains a space, “name” is misinterpreted as the property value:
table.short name = Director
- You cannot use SQL keywords for any of the values of the table properties.
- If a property is listed more than once, each successive definition overwrites the previous definition.

When a custom table property file is processed, its status is logged to a text file in the UserTables directory. This log file lists the properties as they are parsed, so you can use it to check for formatting mistakes. It also describes errors that were encountered during the processing of the file. The log file has the same name as the table property file, but the file extension is .status.

The following table lists table property file properties. Variables are italicized and have the following meanings:

- *x* is an integer representing the *x*th locale. The index *x* can start at 0 and need not be sequential.
- *y* is an integer representing the *y*th locale. The index *y* can start at 0 and need not be sequential.
- *locale* indicates the language code. It must be one of the following strings:
 - *language*
 - *language_country*
 - *language_country_variant*

where *language* is the two-letter code for the language, *country* is the two-letter code for the country, and *variant* specifies a variant code, for example, WIN for Windows.

For example, *locale* could be defined as any of the following strings:

- pt (Portuguese)
- pt_br (Brazilian Portuguese)
- pt_br_WIN (Brazilian Portuguese Windows)

Table 13. Table property file properties

Property	Required	Purpose
table.token	No	The table name used internally by the management server. If you do not specify a value for this property, it defaults to the name of the table property file, minus the file extension.
table.realname	No	The table name that is stored in the database. If you do not specify a value for this property, it defaults to the value of table.token. If you provide a translated string file, this property value is part of a key into the translated string file. The key retrieves the translated string for this property value from the translated string file. For more information, see the NLS properties in this table and “Creating translated strings files” on page 186.
table.shortname	No	A shorter table name that is stored in the database. If the database application shortens the table.realname value, this name is used.
table.displayname	No	The table name that is displayed in the Inventory Query Browser and the Dynamic Group Editor windows. If you do not specify a value for this property, it defaults to the value of table.realname. If you provide a translated string file and the table.realname property value is defined in the translated string file, then the database uses that value. Otherwise, the table.displayname property value is used. For more information, see the NLS properties in this table and “Creating translated strings files” on page 186.
table.filterprompt.alltrue	No	The string that is displayed in the Dynamic Group Editor window, when a column from this table is added to a filter. This string is displayed for the “All true (AND)” option. If you do not specify a value for this property, it is set to the default string. The default string is translated already.
table.filterprompt.anytrue	No	The string that is displayed in the Dynamic Group Editor window, when a column from this table is added to a filter. This string is displayed for the “Any true (OR)” option. If you do not specify a value for this property, it is set to the default string. The default string is translated already.

Table 13. Table property file properties (continued)

Property	Required	Purpose
table.filterprompt.alltrueforsame	No	<p>The string that is displayed in the Dynamic Group Editor window, when a column from this table is added to a filter. This string is displayed for the “All true for the same row” option.</p> <p>If you do not specify a value for this property, it is set to the default string. The default string is translated already.</p> <p>The “All true for the same row” option is displayed only if there is more than one column specified as a key value. This includes the MANAGED_OBJ_ID column (which is a key) that is added automatically by the management server. Providing more than one key in a table facilitates having multiple rows for a managed system.</p>
table.filterprompt.eachtrueatleastone	No	<p>The string that is displayed in the Dynamic Group Editor window, when a column from this table is added to a filter. This string is displayed for the “Each must be true for at least one row” option.</p> <p>If you do not specify a value for this property, it is set to the default string. The default string is translated already.</p> <p>The “Each must be true for at least one row” option is displayed only if there is more than one column specified as a key value. This includes the MANAGED_OBJ_ID column (which is a key) that is added automatically by the management server. Providing more than one key in a table facilitates having multiple rows for a managed system.</p>
nls.x.locale	No	<p>The name of a locale for which a file of translated strings is provided.</p> <p>If you do not specify a value for this property, the table.displayname and column.x.displayname property values are displayed.</p>
nls.x.filename	No	<p>The path to the file that contains the translated strings that correspond to table.realname and column.x.realname property values in the property file.</p> <p>This file corresponds to the xth locale as defined by the nls.x.locale property. The path must be relative to the directory in which the table property files are stored.</p>
column.x.token	Yes	<p>The name of a column of data used internally in IBM Director Server.</p> <p>Do not define the column MANAGED_OBJ_ID. Because it is required in every table, this column is created automatically as the first column.</p>
column.x.realname	Yes	<p>The name of column x as it is stored in the database.</p> <p>If you do not specify a value for this property, it is set to column.x.token.</p> <p>If you provide a translated string file, this property value is part of a key into the translated string file. The key retrieves the translated string for this property value from the translated string file. For more information, see the NLS properties in this table and “Creating translated strings files” on page 186.</p>

Table 13. Table property file properties (continued)

Property	Required	Purpose
column.x.shortname	No	The name of column <i>x</i> as it is stored in the database. If the database shortens the column.x.realname value, you can specify a shortened name for the database to use instead.
column.x.displayname	No	The name of column <i>x</i> as it is displayed in the Inventory Query Browser and the Filter Creation windows. If you do not specify a value for this property, it is set to column.x.realname. If you provide a translated string file and the column.x.realname property value is defined in the translated string file, then the database uses that value. Otherwise, the column.x.displayname property value is used. For more information, see the NLS properties in this table and “Creating translated strings files” on page 186.
column.x.key	No	If column <i>x</i> is a key, this value is set to True; otherwise, it is set to False.
column.x.type	Yes	The type of data stored in column <i>x</i> . You must specify one of the following types: SMALLINT, INTEGER, REAL, DOUBLE, CHAR, VARCHAR, DATE, DATETIME. The specified type <i>must</i> match the type of data returned by the CIM, DMI, or MIF collector that is displayed in this column. If you specify the CHAR or VARCHAR types, you also must specify a value for the column.x.length property.
column.x.metatype	No	The metatype of data stored in column <i>x</i> . Use the metatype to specify additional information about the data. The only supported metatype is IPAddress for CHAR columns. Use this metatype to define the CHAR column data as a TCP/IP address. This additional information is necessary for sorting and filtering.
column.x.length	Optional	When column.x.type=CHAR, it specifies the fixed length of the character field. When column.x.type=VARCHAR, it specifies the maximum length of the variable-length character field.
column.x.value.y.token	No	If column.x.type is CHAR or VARCHAR, you can specify strings that represent values of these columns. If you want to display information other than the raw collected information, use this property to specify possible strings. These strings are specified in the column.x.value.y.displayname property. If you specify a value for the column.x.value.y.token property, you also <i>must</i> define a single corresponding column.x.value.y.realname property.

Table 13. Table property file properties (continued)

Property	Required	Purpose
column.x.value.y.displayname	No	<p>The text string that is displayed to the user when the value of column <i>x</i> is the text string specified in column.x.value.y.token.</p> <p>There must be <i>only</i> one displayname for each token in each column. If you do not specify this property value, a token is displayed to the user as-is. If a column contains a value that does not match a token listed in the property file, that value is displayed to the user as-is.</p>

Creating inventory extension property files

After the management server has loaded the table property files and has defined the custom tables, the management server must associate the data collected by inventory collectors with the columns in the custom tables. These associations, called groups, are listed in the inventory extension property files that you provide. A group represents the association between one collector and one table.

You can create and edit an inventory extension property file with an ASCII text editor. The available properties that you can use are listed in Table 14 on page 185. The extension files must be in the InvExtension subdirectory of the data directory on the management server. Typically, this path is C:\Program Files\IBM\Director\data\InvExtension. This directory includes inventory extension property file examples. These example files have the .sample file extension.

A file can contain more than one group, but all the properties for a group must be in the same file. A file can be one of three types: CIM, DMI, or MIF, with the following file extensions respectively: .CIMInvExt, .DMIInvExt, or .MIFInvExt.

An inventory extension property file follows a strict syntax. You must type property names with the same mixed-case capitalization as shown.

The following table lists the properties in an inventory extension property file and their attributes. Unless noted, the properties listed are used for CIM, DMI, and MIF. The table uses the following conventions:

- *x* is an integer representing the *x*th group. The index *x* must start at 1 and be sequential within each extension file. These indices do not remain in effect across different inventory extension property files. For example, Group 1 in one file is not the same group as Group 1 in another file. These indices are used for parsing the files only.
- *y* is an integer representing the *y*th property for a group's list of attributes. The index *y* must start at 1 and be sequential within each list of attributes.

Table 14. Inventory extension property file properties

Property	Required	Purpose
Group.x.ComponentName	Yes, for DMI or MIF	The name of a component in a DMI or MIF name space from which the data is collected.
Group.x.ClassName	Yes	(CIM only) The name of a class in a CIM name space from which the data is collected. This must be the name of the “leaf” class. Do not include any names of higher-level classes. (DMI and MIF only) The name of the class in the DMI or MIF component specified in Group.x.ComponentName. Typically, class names use a Manufacturer Component Version format.
Group.x.NameSpace	Yes	The name space from which to retrieve the class name specified in the Group.x.ClassName property. You cannot use backward slashes (\) in this property.
Group.x.DbTable	Yes	The token name of the custom table in which to store the data. This property is defined by the table.token property. For more information, see Table 13 on page 181.
Group.x.Attrib.y.Property	Yes	The name of a property to collect from the class specified in the Group.x.ClassName property.
Group.x.Attrib.y.Attributeld	Yes	The numeric identifier of a property to collect from the class specified in the Group.x.ClassName property.
Group.x.Attrib.y.DbColumn	Yes	The token name of a column in the custom table in which to store the property specified by Group.x.Attrib.y.Property.
Group.x.Attrib.y.ScaleBy	No	The scaling factor for numeric values that are multiplied by the returned value. If you do not specify this property value, it is set to 1 and has no effect on the calculated value.
Group.x.Attrib.y.AdjustBy	No	The scaling factor for numeric values that are added to the returned value after the returned value is multiplied by the Group.x.Attrib.y.ScaleBy value. If you do not specify this property value, it is set to zero and has no effect on the calculated value.

By default, all collected CIM, DMI, and MIF properties are stored in the database based on the mappings in Table 15.

Table 15. Property mappings

Default database type	CIM type	DMI and MIF type
CHAR	EMPTY STRING	OCTETSTRING DISPLAYSTRING
INT	SINT8 UINT8 SINT16 UINT16 SINT32 UINT32 SINT64 UINT64 BOOLEAN	DATATYPE_0 COUNTER COUNTER64 GAUGE DATATYPE_4 INTEGER INTEGER64 DATATYPE_9 DATATYPE_10
REAL	REAL32	
DOUBLE	REAL64	
DATETIME	DATETIME	DATE

Table 15. Property mappings (continued)

Default database type	CIM type	DMI and MIF type
IGNORED	REFERENCE CHAR16 OBJECT	

Creating translated strings files

For each locale that you specify in the table property file, you must create an associated translated strings file. Translated strings files must be in the UserTables directory on the management server. Typically, this path is C:\Program Files\IBM\Director\Data\UserTables. This directory also includes translated strings file examples. These example files have the .sample file extension. For more information, see Table 16 on page 188.

The translated strings files are used to build Java resource bundles to provide internationalization and globalization support. The resource bundles contain keys and values similar to the table property files. The keys represent the table.realname, table.x.column, and other column property values. The values associated with the keys in the resource bundles are the translated strings for the custom table properties. The Inventory Query Browser and the Dynamic Group Editor windows display these translated strings.

The resource bundles have a four-level hierarchy. From top to bottom, they are:

1. A default.
2. A locale specified by a language only. For example, "pt" for Portuguese.
3. A locale specified by a language and a country. For example, "pt_br" for Brazilian Portuguese.
4. A locale specified by a language, country, and variant. For example, "pt_br_WIN" for Brazilian Portuguese Windows variant.

If a name is missing from a level-4 resource bundle, the level-3 resource bundle in the hierarchy is searched. If the name is still missing, the level-2 resource bundle is searched. Finally, if the name is still missing, the level-1 (default) resource bundle is searched.

When IBM Director Server is started, it automatically creates a translated strings file. Its filename consists of the table file name that is in the UserTables directory (without the leading path and extension) and the .defbundle extension.

IBM Director Server uses the .defbundle file to build the default resource bundle. The values in the default resource bundle are created from the displayname properties defined in the table properties files (see Table 13 on page 181).

After the resource bundles are created, IBM Director Server searches the resource bundles for the strings to display in the Inventory Query Browser and the Dynamic Group Editor windows. IBM Director Server uses the search order defined by Java internationalization and globalization support:

1. If a resource bundle is supplied that matches the current locale exactly, that bundle is used.
2. If a key is missing from that resource bundle, the resource bundles in the hierarchy are searched until a match is made for that key.

3. If no resource bundle matches the locale exactly, the current locale is generalized until it matches a resource bundle. If a variant is provided, it is removed from the locale name. Then, if a country is provided, it is removed from the locale name. Finally, if a language is provided, it is removed from the locale name.

For example, if IBM Director is run in the “pt” locale but translated strings files are provided for the “pt_br” locale. The default resource bundle, not the “pt_br” resource bundle, is used.

Complete the following steps to create a resource bundle:

1. Start IBM Director Server with the table property file in the UserTables directory. From a command prompt, change to the bin directory and type the following command:

```
net start twgipc
```

The default resource bundle file is created when IBM Director Server is initialized.

2. Stop IBM Director Server. From a command prompt in the bin directory, type the following command:

```
net stop twgipc
```

3. Make a copy of the default resource bundle for each locale that requires support. The correct keys have been created in the default resource bundle.
4. In each copy of the default resource bundle, replace the values with the translated values for a locale.

Note: The filter table prompt keys are not created in the default resource bundle because these keys have default values built into IBM Director Server.

5. Start IBM Director Server. From a command prompt in the bin directory, type the following command:

```
net start twgipc
```

The new resource bundle files are created when IBM Director Server is initialized.

If you do not want to create the translated strings file using this procedure, see the following sample of the translated strings file syntax. You must type the key statement exactly as shown. You must provide your own values to the right of each equal sign (=).

```

# Example format for a translated string file
#
# The translated string for the table name
TableName.TWGDdbUserTable?tableTokenName =
# The translated string for the column name
ColumnName.TWGDdbUserTable?tableTokenName.columnTokenName =
# The translated string for the column value
# If you specify a string for this key that contains spaces,
# you must replace the spaces with the following string: {0}
# For example, the string "Default System BIOS"
# must be specified as: Default{0}System{0}BIOS
# After the management server parses and processes the property name,
# the {0} strings are replaced with spaces.
ColumnName.TWGDdbUserTable?tableTokenName.columnValueToken =
# The translated string for the "All True" filter prompt
FilterTablePrompt.AllTrue.TWGDdbUserTable?tableTokenName =
# The translated string for the "Any True" filter prompt
FilterTablePrompt.AnyTrue.TWGDdbUserTable?tableTokenName =
# The translated string for the "All True For Same" filter prompt
FilterTablePrompt.AllTrueForSame.TWGDdbUserTable?tableTokenName =
# The translated string for the "Each True For At Least One" filter prompt
FilterTablePrompt.EachTrueForAtLeastOne.TWGDdbUserTable?tableTokenName =

```

Also, the following translated strings file examples are in the UserTables directory:

Table 16. Example translated strings files

Language	Example file extension
Default	.TWGdbt.sample
English	.en.sample
French	.fr.sample
German	.de.sample
Japanese	.ja.sample
Korean	.ko.sample
Simplified Chinese	.zh_CN.sample
Spanish	.es.sample
Traditional Chinese	.zh_TW.sample

Initializing custom tables

When IBM Director Server starts, it searches the UserTables directory on the management server. Typically, this path is c:\Program Files\Director\Data\UserTables. IBM Director Server loads all the table property files that have the file extension .TWGdbt.

IBM Director Server stores data about managed systems in two locations:

- Its own persistent storage that contains information related to the management server functions
- A third-party database management system

The custom table properties are stored in each of these locations and must be kept synchronized.

IBM Director Server processes the table property files and verifies that each file has a matching table in the management server persistent storage. If a table property file does not have a matching table, a new table is created in the database through the interface to the database management system. Subsequently, information about the table properties is created in the management server persistent storage.

If a matching table does exist in the persistent storage, the table is initialized on the management server. If a table exists in the management server persistent storage, but the table property file is missing, that table is removed from persistent storage *and* removed from the database.

Be careful about removing table property files for tables you want to retain in the database. If a table property is not processed correctly due to syntactic errors, but enough of the file is correct such that the table token name can be read, then that table is not initialized in the management server. However, the table contents in the database remain intact. As the table is initialized, warnings and errors are logged to the table status file. For more information, see “Creating table property files” on page 179.

Changing custom tables

After the management server is initialized, you cannot change a custom table. To make changes to a custom table, you must stop the management server, change the table property file, and restart the server. If the table property file has been changed since the last time the server was started, the table is changed to reflect changes made to the table property file. There are very important restrictions on the changes you can make to a table property file:

1. You can change certain properties in a table property file after that table is successfully initialized by IBM Director Server. To determine whether you can change a property, see Table 17.

Table 17. Table properties that can be changed

Property	Changeable in a table property file after that table is initialized
table.token	No
table.realname	No
table.shortname	No
table.displayname	Yes
table.filterprompt.alltrue	Yes
table.filterprompt.anytrue	Yes
table.filterprompt.alltrueforsame	Yes
table.filterprompt.eachtrueatleastone	Yes
nls.x.locale	Yes
nls.x.filename	Yes
column.x.token	No
column.x.realname	No
column.x.shortname	No
column.x.displayname	Yes
column.x.key	No
column.x.type	No

Table 17. Table properties that can be changed (continued)

Property	Changeable in a table property file after that table is initialized
column.x.metatype	Yes
column.x.length	No
column.x.value.y.token	Yes
column.x.value.y.displayname	Yes

2. You cannot delete columns.
3. You cannot change the indices of the columns.
4. You can add columns, but new columns must have a higher index than the existing columns.

If you want to make changes to table property files that are not permissible due to any of the restrictions above, you must remove the old table and recreate it with the changes. Any data in the table will be lost. Complete the following steps to remove a table:

1. Stop IBM Director Server. From a command prompt, change to the bin directory and type:

```
net stop twgipc
```
2. Use a database management tool to remove the table from the database.
3. Change the .TWGDbt file.
4. Start IBM Director Server. From a command prompt in the bin directory, type:

```
net start twgipc
```

The table is recreated using the new property file.

Complete the following steps if the database management tool cannot remove the table from the database:

1. Stop IBM Director Server. From a command prompt, change to the bin directory and type:

```
net stop twgipc
```
2. Delete the table property file for the table.
3. Start IBM Director Server. From a command prompt in the bin directory, type:

```
net start twgipc
```

When IBM Director Server does not find the table property file, it removes the table from the database.

4. Stop IBM Director Server. From a command prompt in the bin directory, type:

```
net stop twgipc
```
5. Change the table property file for the table.
6. Start IBM Director Server. From a command prompt in the bin directory, type:

```
net start twgipc
```

The table is recreated using the new property file.

Note: IBM Director Server will not start unless *all* database tables are initialized successfully, including custom tables. Therefore, errors in the table property files can cause IBM Director Server to not initialize, or cause the inventory or

database components to stop (for example, if types in the table property file do not match those of the collected data).

There are no restrictions on how you change the inventory extension property files, as long as the inventory extension property files are valid. However, you must be careful when using comments. If you comment out a group attribute property, you must change the indices for the remaining attributes so the indices of the remaining attributes start at 1 and increase sequentially. Failure to do so will cause all the attributes after the commented-out attribute to not be found.

Generating MIF files for inventory collection

The syntax of the extension files for DMI and static MIF is identical, except for the file names.

To collect data from a MIF file, you must specify how to generate the MIF file. Each managed system from which you want to collect MIF data must have an initialization file, `mifgen.ini`. You can use this file to specify the MIF generation program that updates the static MIF data and the MIF files from which to collect data. Because you can specify the MIF generation program, managed systems that use different operating systems can use different MIF generation programs to generate the static MIF files.

For managed systems running Windows, the `mifgen.ini` file is in the same directory as the file `dmiparse.dll`. Typically, this directory is `c:\Program Files\Director\Data\Tables`. Be sure to verify that the MIF generation program can execute successfully from a command line in the `bin` directory. It might be necessary to provide an absolute path to the MIF generation program.

Creating the `mifgen.ini` file

The `mifgen.ini` file uses the standard Windows INI file format:

- An INI file can contain several sections.
- Each section starts with a tag enclosed in square brackets.
- A section contains three properties: filename, command, and refresh.
- Each property is followed by an equal sign and the property value.
- A section ends when another section is started, or the file ends.
- Section tags and property names are not case sensitive.
- A section tag value must be unique among the section tag values in that file.
- Lines starting with a semi-colon are comments and are ignored by the INI file.
- Comments continue to the end of a line only.

When IBM Director Agent on a managed system is notified that MIF inventory collection is underway, it reads the `mifgen.ini` file and checks the filename, refresh, and command property values.

Filename

If you do not specify a value for the filename property, the section tag is used. If more than one section specifies the same value for the filename property, the refresh and command values from the first section that specifies that filename value are used. Filename property values are not case sensitive.

Refresh

The refresh property has only two values:

Always

The specified command is run and the specified MIF file is generated. This value is the default.

Never The specified command is run *only* if the specified MIF file does *not* exist already. That is, the file is generated once and never refreshed.

Command

If the specified command fails, the previous version of the MIF file is used if it exists. If the MIF file cannot be generated, and a previous MIF file does not exist, the inventory data collection for IBM Director Agent fails for this MIF file. Inventory data collection from other MIF files on the same managed system is not affected.

The following example is a typical section of a mifgen.ini file. In this example, genmif is not a real MIF generation program. You must supply the name of your MIF generation program.

```
[EXAMPLE ONE]
; You can insert comments in the middle of a section
; without breaking the section.
filename = bob.mif
refresh = NEVER
command = genmif bob.mif
```

A command in a section does not have to run a MIF generation program. In the following example, the command copies a previous MIF file to another location:

```
[EXAMPLE TWO]
filename = frank.mif
refresh = never
command = cp mifs\default2.mif frank.mif
```

Troubleshooting MIF file generation

If you cannot generate a MIF file successfully, verify that you can create the target MIF file. For example, there might be a read-only copy of a file with the specified filename.

If you have problems with the .MIFInvExt file, verify that:

- The Group.x.ComponentName and Group.x.ClassName properties (specified in the .MIFInvExt file) match the component name and class name attributes (in the MIF file) exactly. Be sure that the values match in capitalization and spacing.
- The Group.x.DbTable property (specified in the .MIFInvExt file) matches the table.token property (specified in the .TWGDbt file).
- The Group.x.Attrib.y.AttributeId properties (specified in the .MIFInvExt file) match the applicable attribute IDs in the MIF file.
- The Group.x.Attrib.y.DbColumn properties for the applicable MIF attributes (specified in the .MIFInvExt file) match the corresponding column.x.token properties (specified in the .TWGDbt file).
- The column.x.type properties (specified in the .TWGDbt file) are appropriate to stored values retrieved from the MIF file. For information about the default MIF attribute-to-database type mappings, see “Creating inventory extension property files” on page 184.

Appendix C. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM® products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation® system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

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

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

Using the documentation

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

Getting help and information from the World Wide Web

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

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

Software service and support

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

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

Appendix D. Notices

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

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

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

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

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

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

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

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

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

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

Edition notice

© COPYRIGHT INTERNATIONAL BUSINESS MACHINES CORPORATION, 2003.
All rights reserved.

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

Trademarks

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

Active PCI	Predictive Failure Analysis
Asset ID	Redbooks
BladeCenter	ServeRAID
DB2	ServerProven
e-business logo	SurePOS
@server	ThinkPad
IBM	Tivoli
IntelliStation	Tivoli Enterprise
Light Path Diagnostics	Tivoli Enterprise Console
Netfinity	TotalStorage
NetView	xSeries
NetVista	UpdateXpress
OS/2 WARP	Wake on LAN

Pentium is a trademark of Intel Corporation in the United States, other countries, or both.

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

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

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

Linux is a registered trademark of Linus Torvalds.

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

Index

A

- Active PCI Manager
 - hardware, supported 7
 - installing on managed systems 137
 - operating systems, supported 7, 12
 - overview 7
 - prerequisites 7, 11
 - subtasks 7
 - troubleshooting 165
- Advanced Systems Management PCI adapter
 - See ASM PCI adapter
- Advanced Systems Management processor
 - See ASM processor
- Agent
 - features
 - IBM Director Remote Control Agent 5
 - MPA Agent 5
 - ServeRAID Manager 5
 - SNMP Access and Trap Forwarding 6
 - System Health Monitoring 5
 - Web-based Access 5
 - Web-based Access help files 5
 - function 4
 - hardware requirements 11
 - license 4, 15
 - Linux, installing on
 - dirinstall script 90
 - encryption, enabling 91
 - prerequisites 89
 - SMBus device driver 90
 - Wake on LAN, enabling 91
 - modifying an installation
 - Linux 150
 - NetWare 152
 - Open UNIX 153
 - Windows 149
 - NetWare, installing on
 - features, selecting 92
 - network driver, configuring 93
 - network protocols 13
 - Open UNIX, installing on
 - dirinstall script 94
 - encryption, enabling 94
 - Wake on LAN, enabling 94
 - operating systems, supported 4, 12
 - uninstalling
 - Linux 155
 - NetWare 156
 - Open UNIX 156
 - Windows 155
 - upgrading
 - Linux 102
 - NetWare 104
 - Open UNIX 105
 - Software Distribution task, using 107
 - upgrading on Windows
 - diragent.rsp file 101
- Agent (*continued*)
 - upgrading on Windows (*continued*)
 - encryption, enabling 98
 - features, selecting 96
 - IBM Director Remote Control Agent 97, 101
 - InstallShield wizard, using 96
 - MPA Agent 97
 - network driver, configuring 100
 - securing managed system 98
 - security state, setting 98
 - ServeRAID Manager 97
 - SNMP Access and Trap Forwarding 97
 - software-distribution settings 99
 - System Health Monitoring 97
 - unattended installation, using 101
 - Wake on LAN, enabling 100
 - Web-based Access 97, 99
- Windows, installing on
 - diragent.rsp file 88
 - encryption, enabling 85
 - features, selecting 84
 - IBM Director Remote Control Agent 84, 88
 - InstallShield wizard, using 83
 - MPA Agent 84
 - network driver, configuring 87
 - securing managed system 86
 - security state, setting 85
 - ServeRAID Manager 84
 - SNMP Access and Trap Forwarding 84
 - software-distribution settings 86
 - System Health Monitoring 84
 - unattended installation, using 88
 - Wake on LAN, enabling 88
 - Web-based Access 84, 87
- alert-forwarding strategy
 - ASM PCI adapter 22
 - ASM processor 22
 - ISMP 22
 - Remote Supervisor Adapter 22
- alerts
 - in-band 5
 - ISMP and limitations 21
 - MPA Agent, role of 21
 - out-of-band 22
 - System Health Monitoring, role of 21
- APC PowerChute Extension for IBM Director 9
- Application Workload Management (Aurema) 9
- ASF, troubleshooting 165
- ASM interconnect
 - ASM PCI adapter 23
 - ASM processor 23
 - ISMP 23
 - Remote Supervisor Adapter 23
- ASM interconnect network
 - configuring 20
- ASM PCI adapter
 - alert-forwarding strategy 22
 - ASM interconnect 23

- ASM PCI adapter *(continued)*
 - configuring 121
 - management processor object, creating 120
 - MPA Agent 5
 - Netfinity servers 23, 24
 - out-of-band communication 22
 - xSeries servers 23, 24
- ASM processor
 - alert-forwarding strategy 22
 - ASM interconnect 23
 - MPA Agent 5
 - Netfinity servers 23, 24
 - out-of-band communication 22
 - out-of-band management 121
 - xSeries servers 23, 24
- Asset ID, troubleshooting 170

B

- blade servers
 - installing operating systems 65, 79
 - Remote Deployment Manager, using 65
- BladeCenter
 - chassis
 - assigning IP addresses 67
 - automatically discovering 67
 - configuring 70
 - DHCP server, using 67
 - discovering 66
 - discovery, troubleshooting 166
 - IP address conflicts 67
 - managed object 66, 68
 - manually assigning IP addresses 67, 69
 - manually discovering 68
 - deployment infrastructure
 - changing Director database 65
 - DHCP server, using 25, 66
 - illustration 25
 - IP address conflicts 25, 67
 - security 25
 - management module
 - assigning temporary IP addresses 25
 - default IP address 25
 - default user name and password 69
 - troubleshooting 165
- BladeCenter Deployment wizard
 - configuring the chassis 70
 - detect-and-deploy profile
 - creating 70, 80
 - overwriting 80
 - IP settings, configuring 76
 - management module
 - logging in to 72
 - network protocols, configuring 75
 - properties, configuring 74
 - operating systems, deploying 79
 - profile, changing name of 80
 - switch module
 - external ports, configuring 78
 - network protocols, configuring 78
 - user name and password, changing 77

- broadcast discovery 118
- broadcast relay 119

C

- Capacity Manager
 - installing on managed systems 137
 - overview 7
 - supported operating systems 12
- CIM Browser, troubleshooting 165
- Cluster Systems Management 9
- Compatibility Documents for IBM Director 4.1 12
- Console
 - features, selecting 46
 - function 4
 - hardware requirements 11
 - installing on Linux 49
 - installing on Windows
 - Active PCI Manager 47
 - Capacity Manager 47
 - InstallShield wizard, using 45
 - Rack Manager 47
 - Server Plus Pack 48
 - ServeRAID Manager 47
 - Software Rejuvenation 47
 - System Availability 47
 - unattended mode, using 48
 - license 4, 15
 - modifying an installation
 - Linux 150
 - Windows 149
 - network protocols 13
 - starting 65, 168
 - supported operating systems 4, 12
 - uninstalling
 - Linux 155
 - Windows 155
 - upgrading
 - Active PCI Manager 61
 - Capacity Manager 61
 - dircon.rsp file 62
 - features, selecting 60
 - InstallShield wizard, using 59
 - overview 58
 - Rack Manager 61
 - Server Plus Pack 62
 - ServeRAID Manager 61
 - Software Rejuvenation 61
 - System Availability 61
 - unattended mode, using 62
- custom database tables
 - changing 189
 - creating, overview of 179
 - initializing 189
 - inventory extension property files
 - creating 184
 - location of 184
 - mapping 185
 - properties of 184
 - syntax 184

- custom database tables *(continued)*
 - mifgen.ini file
 - creating 191
 - example 192
 - function 191
 - location of 191
 - table property files
 - creating 179
 - location of 179
 - log file 180
 - properties of 180
 - syntax 179
 - translated strings files
 - creating 187
 - Java resource bundles, hierarchy of 186
 - location of 186
 - overview 186
 - syntax, example of 187
- customer support xv

D

- Data Encryption Standard
 - See DES
- database
 - DB2 Universal Database
 - management server running Linux 28
 - management server running Windows 27
 - installing after Director Server is installed 149
 - Microsoft Data Engine 1.0 26
 - Microsoft Jet 4.0
 - overview 26
 - size limitations 26
 - Microsoft SQL Server 26
 - Oracle Server
 - JDBC driver 29
 - overview 29
 - PostgreSQL 29
 - SQL Server 2000 Desktop Engine 26
 - troubleshooting 165
- database server, definition 26
- DB2 Universal Database
 - management server running Linux 28
 - management server running Windows 27
- DES 17
- detect-and-deploy profile
 - creating 70
 - overwriting 80
- DHCP server 66, 67
- dialog boxes, troubleshooting 165
- Diffie-Hellman key exchange 17
- Digital Signature Algorithm 157
- DirAdmin 16, 122
- diragent.rsp file
 - customizing 89, 101
 - location 88, 101
- dircon.rsp file
 - customizing 48, 63
 - location 48, 62
- Director
 - database applications, supported 15, 26

- Director *(continued)*
 - database, function of 3
 - environment (illustration) 2
 - extensions 9
 - hardware requirements 11
 - hardware, supported 2
 - managing systems running Agent 3.x 6
 - network protocols, supported 4
 - operating systems, supported 12
 - publications xiv
 - Redbooks xv
 - security 157
 - software components (illustration) 3
 - upgrading from IBM Director 3.x 6
- Director Agent
 - See Agent
- Director Console
 - See Console
- Director Server
 - See Server
- dirinstall script
 - Agent 90
 - Console 49
 - Server 43
 - upgrade of Agent 107
- DirSuper 16, 122
- discovery
 - BladeCenter chassis 66
 - broadcast 118
 - broadcast relay 119
 - multicast 118
 - overview 118
 - setting preferences 119
 - troubleshooting 170
 - unicast 119
- discovery preferences, setting 119
- dynamic groups, troubleshooting 166

E

- eFixes xv
- Electronic Service Agent 9
- encryption
 - algorithms 17
 - enabling 17
 - performance penalty 17
 - troubleshooting 166
- Event Action Plan wizard
 - access to, restricting 124, 127
 - event action plan, applying 116
 - event action plan, naming 118
 - event filters, selecting 114
 - event substitution variables, using 116
 - notification method, selecting 115
 - systems and devices, discovering 117
- event action plans, troubleshooting 166
- extensions
 - APC PowerChute Extension for IBM Director 9
 - Application Workload Management (Aurema) 9
 - Cluster Systems Management 9
 - Electronic Service Agent 9

extensions (*continued*)
 Real Time Diagnostics 9
 Remote Deployment Manager 8
 Server Plus Pack 6
 Software Distribution (Premium Edition) 8
extensions, definition 6

F

Fault Tolerant Management Interface
 overview 7
 prerequisites 11
file-distribution servers
 configuring Director to use 133
 considerations 132
 setting up 132
FRU information, troubleshooting 167

H

hard disk drives, troubleshooting 167
help xv
help files, Web-based Access 5

I

IBM
 Active PCI Software for Microsoft Windows 7
 Director Remote Control Agent 5
 Director Remote Control, troubleshooting 171
IBM Director
 See Director
IBM Director Agent
 See Agent
IBM Director Console
 See Console
IBM Director Server
 See Server
IIS, troubleshooting 167
illustrations
 BladeCenter deployment infrastructure 25
 Director environment 2
 Director software components 3
in-band alerts
 managed systems running Linux, NetWare, or Open
 UNIX 5
 managed systems running Windows 5
 MPA Agent, role of 5
 SNMP traps 6
 System Health Monitoring, role of 5
in-band communication
 definition 20
 enabling 21
 ISMPS in servers running NetWare or Open
 UNIX 21
 MPA Agent, role of 21
InstallShield wizard
 IBM Director Agent 83
 IBM Director Console 45
 IBM Director Server 31

integrated systems management processor
 See ISMP
interprocess communication, definition 20
inventory errors, troubleshooting 65
inventory extension property files
 creating 184
 location of 184
 mapping 185
 properties of 184
 syntax 184
IP address conflicts, troubleshooting 67
ISMP
 alert-forwarding strategy 22
 ASM interconnect 23
 limitations on in-band communication 21
 MPA Agent 5
 Netfinity servers 23, 24
 out-of-band communication 22
 xSeries servers 23, 24

J

JDBC driver
 Oracle Server 29
 PostgreSQL 29
JRE exceptions, troubleshooting 170

K

keys
 files, location of 158
 origin of, determining 162
 recovering lost keys 162

L

license
 IBM Director Agent 4, 15
 IBM Director Console 4, 15
 IBM Director Server 3, 15
Linux installation
 Agent installation 89
 Console installation 49
 installing Server Plus Pack extensions 139
 modifying
 adding a feature 151
 installing the Director database 150
 overview 150
 removing a feature 151
 Wake on LAN, enabling 151
 Rack Manager installation, completing 137
 Server installation 43
 uninstalling 155

M

managed objects
 BladeCenter chassis 66
 management processor 20, 120

- managed systems
 - definition 1
 - difficulty accessing, troubleshooting 167, 168
 - distribution preferences, configuring 135
 - hardware requirements 11
 - installing the Server Plus Pack
 - manually 139
 - using Software Distribution task 142
 - securing
 - Agent installation, during 86
 - Agent upgrade, during 98
 - automatically 159
 - manually 159
 - methods 159
 - security 160
 - software distribution, troubleshooting 172
- management console
 - definition 2
 - hardware requirements 11
- management module
 - assigning temporary IP addresses 25
 - default IP address 25
- Management Processor Assistant
 - Agent 5
 - task 5
- management processor object
 - creating 20, 120
 - displayed in Console 122
 - naming 121
- management server
 - DB2 database
 - Linux installation 28
 - Windows installation 27
 - definition 1
 - hardware requirements 11
 - Rack Manager installation, completing 137
- MIB file attribute values, troubleshooting 171
- Microsoft Data Engine 1.0 26
- Microsoft Jet 4.0
 - overview 26
 - size limitations 26
 - troubleshooting 165
- Microsoft Management Console 5, 15
- Microsoft SQL Server 26
- mifgen.ini file
 - creating 191
 - example 192
 - function 191
 - location of 191
- modifying
 - Linux installation
 - adding a feature 151
 - installing the IBM Director database 150
 - overview 150
 - removing a feature 151
 - Wake on LAN, enabling 151
 - NetWare installation
 - adding a feature 152
 - limitations 152
 - Open UNIX installation
 - adding a feature 154

- modifying (*continued*)
 - Open UNIX installation (*continued*)
 - overview 153
 - removing a feature 154
 - Wake on LAN, enabling 153
 - Windows installation
 - adding a feature 149
 - installing the IBM Director database 149
 - overview 149
 - Program Maintenance window 150
 - removing a feature 149
- MPA
 - See Management Processor Assistant
- multicast discovery 118

N

- Netfinity 7000, troubleshooting 170
- NetWare installation
 - Agent installation 91
 - installing Server Plus Pack extensions 140
 - modifying
 - adding a feature 152
 - limitations 152
 - troubleshooting 167
 - uninstalling 156
- network interface card, troubleshooting 167
- network protocols 13

O

- Open UNIX installation
 - Agent installation 94
 - modifying
 - adding a feature 154
 - overview 153
 - removing a feature 154
 - Wake on LAN, enabling 153
 - uninstalling 156
- operating systems, supported 12
- Oracle Server
 - JDBC driver 29
 - overview 29
 - troubleshooting 165
- out-of-band communication
 - ASM interconnect, role of 22
 - ASM PCI adapter 22
 - ASM processor 22
 - definition 21
 - ISMP 22
 - Remote Supervisor Adapter 22

P

- planning considerations 19
- ports 13
- PostgreSQL
 - JDBC driver 29
 - overview 29
- publications xiv

R

- Rack Manager
 - completing installation on management server
 - Linux 137
 - Windows 137
 - installing on managed systems 137
 - overview 8
 - supported operating systems 12
- RAID arrays, monitoring and managing 5
- Real Time Diagnostics 9
- Redbooks xv
- Remote Deployment Manager
 - BladeCenter deployment infrastructure 25
 - installing operating systems on blade servers 65
 - overview 8
- Remote Supervisor Adapter
 - alert-forwarding strategy 22
 - ASM interconnect 23
 - configuring 121
 - firmware levels 22
 - management processor object, creating 120
 - MPA Agent 5
 - Netfinity servers 23, 24
 - out-of-band communication 22
 - xSeries servers 23, 24
- request for access, troubleshooting 168
- response file, use with Software Distribution task 107

S

- secure socket layers
 - cipher suites 16
 - enabling 128
 - overview 16
 - restricting sessions 128
- security
 - Agent-Server authentication 157
 - BladeCenter deployment infrastructure 25
 - Digital Signature Algorithm 157
 - encryption
 - algorithms 17
 - enabling 17
 - overview 17
 - performance penalty 18
 - troubleshooting 166
 - key management
 - location of files 158
 - origin of a key, determining 162
 - overview 162
 - public and private keys 158
 - recovering lost keys 162
 - managed system
 - accessing a secured system 160
 - removing access to 161
 - securing automatically 159
 - securing manually 159
 - management server, adding another 162
 - overview 16
 - secure socket layers
 - cipher suites 16

- security (*continued*)
 - secure socket layers (*continued*)
 - enabling 128
 - overview 16
 - restricting sessions 128
 - troubleshooting 171
 - user administration
 - default profile, creating 122
 - editing user privileges 124
 - Event Action Plan wizard, restricting access to 124, 127
 - group access, restricting 126
 - task access, restricting 127
 - user login 122
 - Web-based Access
 - custom access policy, configuring 129
 - overview 18
- Server
 - function 3
 - hardware requirements 11
 - license 3, 15
 - Linux, installing on
 - database, configuring 44
 - encryption, enabling 45
 - modifying an installation
 - Linux 150
 - Windows 149
 - network protocols 13
 - starting, troubleshooting 169
 - supported operating systems 3, 12
 - uninstalling
 - Linux 155
 - Windows 155
 - upgrading
 - Active PCI Manager 54
 - Capacity Manager 54
 - encryption settings 56
 - features, selecting 53
 - IBM Director Remote Control Agent 53, 58
 - MPA Agent 53
 - network driver, configuring 58
 - Oracle JDBC driver 51
 - Rack Manager 54
 - Server Plus Pack 54
 - ServeRAID Manager 53
 - SNMP Trap Access and Forwarding 53
 - Software Rejuvenation 54
 - software-distribution settings 56
 - System Availability 54
 - System Health Monitoring 53
 - Wake on LAN, enabling 58
 - Web-based Access 53, 57
 - Windows, installing on
 - Active PCI Manager 34
 - Capacity Manager 34
 - database configuration 39
 - DB2 Universal Database, configuring 40
 - encryption settings 36
 - features, selecting 33
 - IBM Director Remote Control Agent 33, 38
 - IBM Director service account 31

- Server *(continued)*
 - Windows, installing on *(continued)*
 - Microsoft SQL Server, configuring 41
 - MPA Agent 33
 - network driver, configuring 38
 - Oracle Server, configuring 41
 - Rack Manager 34
 - Server Plus Pack 34
 - ServeRAID Manager 33
 - SNMP Trap Access and Forwarding 33
 - Software Distribution settings 36
 - Software Rejuvenation 34
 - System Availability 34
 - System Health Monitoring 33
 - Wake on LAN, enabling 38
 - Web-based Access 33, 37
- Server Plus Pack
 - installation 7
 - managed systems, installing on
 - manually 139
 - using Software Distribution task 142
 - operating systems, supported 12
 - overview 6
 - purchasing 7
- Server Preferences window 133
- ServeRAID Manager 5
- ServerProven Web site 2
- service account
 - creating 16
 - definition 16
- Service Location Protocol 67
- Service Packs xv
- service processors
 - alert-forwarding strategy 22
 - ASM interconnect 22
 - communicating with Director Server
 - in-band 5
 - interprocess communication 20
 - out-of-band 22
 - over the ASM interconnect 20
 - over the LAN 20
 - identifying 20
 - in-band alerts 5
 - in-band communication
 - MPA Agent, role of 21
 - operating system 21
 - service processor type 21
 - management processor object, creating 120
 - managing 5
 - Netfinity servers 23
 - xSeries servers 23
- Slot Manager 7
- SMBIOS 11
- SMBus device driver
 - binary RPM file 89, 102
 - building and installing 89, 102
 - source RPM file 89, 102
- SNMP device, definition 1
- SNMP discovery, troubleshooting 170
- SNMP traps, troubleshooting 171

- software distribution
 - methods
 - redirected distribution 131
 - streaming from management server 131
 - overview 129
 - preferences, configuring 134
 - Server Plus Pack, installing
 - creating a software package 142
 - installing a software package 146
 - overview 142
 - XML files, location of 142
 - upgrading Agent
 - overview 107
 - software package, installing 111
 - XML files, location of 107
 - Software Distribution (Premium Edition)
 - installing on the management server
 - Linux 130
 - Windows 130
 - overview 8, 130
 - Software Distribution task, troubleshooting 171
 - software package, creating 107
 - Software Rejuvenation
 - installing on managed systems 137
 - overview 8
 - supported operating systems 12
 - SQL Server 2000 Desktop Engine 26
 - support, customer xv
 - System Availability
 - installing on managed systems 137
 - overview 8
 - supported operating systems 12
 - System Health Monitoring 5

T

- table property files
 - creating 179
 - location of 179
 - log file 180
 - properties of 180
 - syntax 179
- terminology
 - database server 26
 - extensions 6
 - in-band communication 20
 - interprocess communication 20
 - managed system 1
 - management console 2
 - management server 1
 - out-of-band communication 21
 - service account 16
 - SNMP device 1
- ThinkPad computers, troubleshooting 169
- time zone error, troubleshooting 172
- trademarks 196
- translated strings files
 - creating 187
 - Java resource bundles, hierarchy of 186
 - location of 186
 - overview 186

- translated strings files *(continued)*
 - syntax, example of 187
- Triple DES 17
- troubleshooting
 - Active PCI Manager 165
 - ASF, configuring 165
 - Asset ID 170
 - BladeCenter
 - database 165
 - discovery 166
 - cfgdb utility 165
 - CIM Browser 165
 - Console, starting 168
 - database configuration 165
 - dialog boxes 165
 - difficulty accessing managed systems 167, 168
 - discovery 166
 - dynamic groups 166
 - encryption 166
 - event action plans 166
 - FRU information 167
 - hard disk drives 167
 - IBM Director Remote Control 171
 - IIS 167
 - JRE exceptions 170
 - managed system running NetWare 6.0 167
 - MIB file attribute values 171
 - Microsoft Jet 4.0 165
 - Nefinity 7000 170
 - Oracle Server 165
 - redirected distribution of software packages 172
 - request for access 168
 - security 171
 - Server, starting 169
 - SNMP discovery 170
 - SNMP traps 171
 - Software Distribution task 171
 - Telnet 165
 - ThinkPad computers 169
 - time zone error 172
 - uninstalling 172
 - Web-based Access 173
 - Windows installation 169
- TWGshare 132

U

- unicast discovery 119
- uninstalling
 - Linux 155
 - NetWare 156
 - Open UNIX 156
 - troubleshooting 172
 - Windows 155
- upgrading
 - Active PCI Manager, troubleshooting 165
 - Agent
 - Linux 102
 - NetWare 104
 - Open UNIX 105
 - Windows 95

- upgrading *(continued)*
 - Console 58
 - Server 51
 - Software Distribution task, using 107
- upward integration 1
- user accounts
 - DirAdmin and DirSuper 16
 - management server running Linux 16
 - management server running Windows 16
 - service account 16
- user administration 122
 - default profile, creating 122
 - DirAdmin group 122
 - DirSuper group 122
 - editing user privileges 124, 125
 - Event Action Plan wizard, restricting access to 124, 127
 - group access, restricting 126
 - task access, restricting 127
- User Defaults Editor 122

W

- Wake on LAN
 - enabling on Linux 151
 - enabling on Open UNIX 153
 - enabling on Windows
 - installing Agent 88
 - installing Server 38
 - upgrading Agent 100
 - upgrading Server 58
- Web browsers 15
- Web sites
 - IBM
 - Director-related xv
 - Publications Ordering System 193
 - Redbooks xv
 - ServerProven 2
 - Support 193
 - xSeries information 193
 - Oracle Technology Network 29
 - PostgreSQL JDBC drivers 29
 - Source for Java Technology 129
- Web-based Access
 - custom access policy, configuring 129
 - help files 5
 - overview 5
 - security 18
 - Service Pack 1 for Windows XP 15, 173
 - troubleshooting
 - Java security warning 172
 - managed system running Apache Web Server 173
 - Web browsers, supported 15
- Windows installation
 - Agent installation 83
 - Console installation 45
 - installing Server Plus Pack extensions 139
 - modifying
 - adding a feature 149
 - installing the IBM Director database 149

- Windows installation (*continued*)
 - modifying (*continued*)
 - overview 149
 - removing a feature 149
 - Rack Manager installation, completing 137
 - Server installation 31
 - troubleshooting 167
 - uninstalling 155
- Windows installation, troubleshooting 169
- Wired for Management (WfM) specifications 11
- wizards
 - BladeCenter Deployment 70
 - Event Action Plan 113
 - InstallShield
 - IBM Director Agent 83
 - IBM Director Console 45
 - IBM Director Server 31

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

ASF. See alert standard format.

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

Advanced System Management (ASM) interconnect network. A network of IBM servers created by using the ASM interconnect feature. The servers are connected through RS-485 ports and standard 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 in conjunction with an ASM processor, the ASM PCI adapter acts as an Ethernet gateway, while the ASM processor retains control of the server. When used as an ASM gateway, the ASM PCI adapter can communicate with other ASM PCI adapters and ASM processors only.

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

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

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

B

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

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

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

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

configure new BladeCenter chassis when they are added to the IBM Director environment.

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

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

C

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

CIM. See Common Information Model.

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

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

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

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

D

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

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

DES. See data encryption standard.

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

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

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

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

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

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

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

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

discovery. The process by which IBM Director Server identifies and establishes connections with systems on which IBM Director Agent is installed. In a discovery

operation, the management server sends out a discovery request and waits for responses from managed systems. The managed systems wait for this request and respond to the management server.

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

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

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

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

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

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

DMI. See Desktop Management Interface.

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

dynamic group. See group, dynamic.

E

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

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

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

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

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

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

extension. See IBM Director extension.

F

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

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

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

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

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

FRU. See field-replaceable unit.

FTMI. See Fault Tolerant Management Interface.

G

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

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

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

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

GUID. See Universal Unique Identifier.

H

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

I

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

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

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

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

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

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

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

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

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

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

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

interprocess communication (IPC). A system that lets threads and processes transfer data and messages among themselves; it is used to offer services to and receive services from other programs. Interprocess communication is used to transfer data and messages

between IBM Director Server and IBM Director Agent, as well as IBM Director Server and service processors. It is also called in-band communication

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

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

IPC. See interprocess communication.

ISMP. See integrated systems management processor.

J

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

K

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

KVM. See keyboard/video/mouse.

L

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

M

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

managed device. An SMNP device managed by IBM Director.

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

managed object. An item managed by IBM Director. Managed objects include managed systems, Windows NT clusters, BladeCenter chassis, management processors, SNMP devices, multi-node servers (complexes), system partitions, physical platforms, nodes, and remote I/O enclosures. In IBM Director

Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or complex, for example).

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

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

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

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

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

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

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

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

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

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

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

Microsoft Cluster Browser task. An IBM Director task that can be used to display the structure, nodes, and resources associated with a Microsoft Cluster

Server (MSCS) cluster; determine the status of a cluster resource, and view the associated properties of the cluster resources.

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

MMC. See Microsoft Management Console.

MPA. See Management Processor Assistant.

multicast discovery. See discovery, multicast.

N

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

notification. See alert.

O

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

P

PCI. See Peripheral Component Interconnect.

PCI-X. See Peripheral Component Interconnect-Extended.

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

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

PFA. See Predictive Failure Analysis.

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

plug in. See IBM Director extension.

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

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

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

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

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

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

R

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

RDM. See Remote Deployment Manager.

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

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

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

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

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

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

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

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

S

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

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

Server Plus Pack. See IBM Director Server Plus Pack.

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

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

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

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

SLP. See service location protocol.

SMBIOS. See systems management BIOS.

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

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

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

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

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

SNMP discovery. See discovery, SNMP.

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

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

SSL. See secure sockets layer.

static group. See group, static.

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

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

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

System Health Monitoring. An IBM Director Agent feature that handles in-band communication and alert notification for managed systems running Windows. In

addition to providing active monitoring of critical system functions, it also facilitates upward integration.

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

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

T

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

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

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

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

TTL. See time to live.

U

unicast discovery. See discovery, unicast.

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

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

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

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

higher-level systems-management console, as well as collect IBM Director inventory data, and view IBM Director alerts.

UUID. See Universal Unique Identifier.

V

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

VPD. See vital product data.

W

Wake on LAN®. A technology that enables administrators to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced

Manageability Alliance and part of the Wired for Management Baseline Specification, this technology permits an administrator to remotely turn on a server. Once started, the server can be controlled across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

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



Part Number: 01R0537

Printed in U.S.A.

SC01-R053-70



(1P) P/N: 01R0537

