IBM Systems

IBM Director
Web-based Access Installation and User’s Guide

Version 5.10

IBM Systems

IBM Director
Web-based Access Installation and User's Guide

Version 5.10

Note

Before using this information and the product it supports, read the information in Appendix D, "Notices."

First Edition (October 2005)

This edition applies to version 5, release 10 of IBM Director and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this book

This book describes how to install and use Web-based Access. Web-based Access provides access to managed systems using a standard Web browser. You can access a managed system and view real-time asset information about the managed system.

Conventions and terminology

These notices are designed to highlight key information:

Note: 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 appears before the instruction or situation in which damage can occur.

Related information

This topic provides links to additional information related to IBM Director.

IBM Director resources on the World Wide Web

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

IBM Director information center

publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/diricinfo/fqm0_main.html

Updated periodically, the IBM Director information center contains the most up-to-date documentation available on a wide range of topics.

IBM Director Web site on ibm.com®

www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/

The IBM Director Web site on ibm.com has links to downloads and documentation for all currently supported versions of IBM Director. Information on this site includes:

- IBM Director 5.10 - downloads and documentation
- IBM Director 4.22 - downloads and documentation
- IBM Director 4.22 Upward Integration Modules (UIMs) - downloads and documentation
- IBM Director 4.21 - downloads and documentation
- IBM Director 4.20 - downloads and documentation
- IBM Director Hardware and Software Compatibility document - lists supported @server and IBM® xSeries® systems, as well as all supported operating systems. It is updated every 6 to 8 weeks.

- Printable documentation for IBM Director - available in Portable Document Format (PDF) in several languages

IBM Systems Software information center

www.ibm.com/servers/library/infocenter/

This Web page provides information about IBM Virtualization Engine™, IBM Director, and other topics.

IBM ServerProven® page

www.ibm.com/pc/us/compat/index.html

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

IBM Systems Management Software: Download/Electronic Support page

www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/

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

IBM Servers

www.ibm.com/servers/

This Web page on ibm.com links to information, downloads, and IBM Director extensions such as Remote Deployment Manager, Capacity Manager, Systems Availability and Software Distribution (Premium Edition) for IBM servers:

- IBM BladeCenter
- IBM iSeries™
- IBM pSeries®
- IBM xSeries
- IBM zSeries®

IBM Redbooks™

www.ibm.com/redbooks/

You can download the following documents from the IBM Redbooks Web page. You also might want to search this Web page for documents that focus on specific IBM hardware; such documents often contain systems-management material.

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

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

Remote Supervisor Adapter

Remote Supervisor Adapter overview
www.ibm.com/support/docview.wss?uid=psg1MIGR-4UKSML

This Web page includes links to the *Remote Supervisor Adapter User's Guide* and *Remote Supervisor Adapter Installation Guide*.

Remote Supervisor Adapter II overview
www.ibm.com/support/docview.wss?uid=psg1MIGR-50116

This Web page includes information about the Remote Supervisor Adapter II.

Other documents

For planning purposes, the following documents might be of interest:

- *Planning and installation guide - IBM eServer BladeCenter (Type 8677)*
- *IBM Management Processor Command-Line Utility User's Guide version 3.00*

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information. If you have any comments about this book or any other IBM Director publication, use the form for reader's comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation
Design & Information Development
Department CGFA
PO Box 12195
Research Triangle Park, NC 27709-9990
U.S.A.

Chapter 1. Web-based Access Overview

This topic contains general information about Web-based Access.

Working with managed systems using Web-based Access

You can use Web-based Access to view information about Level-1 and Level-2 managed systems, change system settings, change alert standard format (ASF) alerts, and more.

Web-based Access is useful in the following situations:

- You do not want to install IBM Director Console.
- You plan to manage only a few servers, desktop computers, or other devices.
- You want to remotely access managed systems when using a Web browser.
- You want to view the most up-to-date information about the assets, health, and operating-system state of a managed system.

If you installed Web-based Access when you installed IBM Director Agent or IBM Director Core Services, you can access the managed system by using the following Web browsers:

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

Notes:

1. Your Web browser must support Java applets.
2. For Internet Explorer to work correctly with Web-based Access, you must use 56-bit encryption or higher.
3. A message is displayed about requiring the Java Virtual Machine (JVM). Web-based Access must have the JVM installed to function correctly. If you have a copy of the Microsoft JVM, install it; otherwise, download and install the JVM from java.sun.com.
4. Systems using a Web browser to access a managed system require 64 megabytes (MB) of random access memory (RAM) to function correctly.

If IBM Director Agent is integrated by way of an upward integration module (UIM), you can use Web-based Access from the management console. For more information, see the *IBM Director Upward Integration Module Installation Guide*.

Web-based Access interface

When Web-based Access has connected to a Level-1 or Level-2 managed system, the Web-based Access program opens in your Web browser. Two panes are displayed.

The left pane lists IBM Director Agent services that are available on the managed system. The pane can contain the following pages:

Information
An expandable tree view of IBM Director Agent services that lists hardware and software information from the managed system.

Tasks An expandable tree view of IBM Director Agent services that perform systems-management and system-configuration tasks on the managed system.

When you click a service in the Information or Tasks page, the right pane lists the information or pages that are associated with the service.

Note: You can use a Web browser window to access multiple managed systems. In the **Next System** field, type the TCP/IP address or the system name of another managed system; then, press Enter. The new managed system is displayed in the Web browser.

With IBM Director Agent, you can create comma-separated-value (CSV) data files from the hardware and software data that is collected by the Web-based Access services. You can import these CSV files into simple database and spreadsheet programs and create a centralized data repository.

Complete the following steps to create a CSV file:

1. Click a service in the left pane.
2. Click the Export icon (➡).
3. In the File window, select the directory where you want to save the file.
4. Click **Save**.

Note: (Windows® Server 2003 and Microsoft® Internet Explorer only) Exporting data from a task is not supported when the Microsoft Internet Explorer Enhanced Security Configuration is enabled.

The Web-based Access online help provides definitions for the information tables and services.

Chapter 2. Installing Web-based Access

This topic describes general procedures for installing Web-based Access on a 32-bit Windows managed system.

Web-based Access is supported only on Level-2 managed systems with Windows 32-bit operating systems.

Complete the following steps to install Web-based Access on a 32-bit Windows managed system:

1. Download the Web-based Access package.
2. Extract the package files to a temporary directory.
3. Perform one of the following tasks:

Option	Description
"Installing Web-based Access (interactive installation)"	This topic describes the procedure for installing Web-based Access on a Windows managed system using the InstallShield wizard.
"Installing Web-based Access (unattended installation)" on page 4	This topic describes the procedure for installing Web-based Access on a Windows managed system using a configured response file.

Installing Web-based Access (interactive installation)

This topic describes the procedure for installing Web-based Access on a Windows managed system using the InstallShield wizard.

1. Close all applications, including any command-prompt windows.
2. Click **Start** → **Run**.
3. In the Run dialog, type the following command in the **Open** field and press **Enter**:

   ```
   download\FILES\dir5.10_wba_windows.exe
   ```

   download represents the location to which the download package was unzipped.
4. In the first panel of the IBM Director Web-based Access InstallShield Wizard, click **Next**.
5. In the second panel of the IBM Director Web-based Access InstallShield Wizard, select **I accept the terms in the license agreement**, then click **Next**.
6. In the third panel of the IBM Director Web-based Access InstallShield Wizard, complete the following steps:
   a. Ensure that the hard disk drive icon appears to the left of Web-based Access in the list box. If a different icon appears, click the icon and select **This feature, and all subfeatures, will be installed on local hard drive** from the menu.
   b. Optional: To install the Web-based Access help files, ensure that the hard disk drive icon appears to the left of Web-based Access help files.

c. Click **Next**.

7. In the fourth panel of the IBM Director Web-based Access InstallShield Wizard, specify the HTTP and HTTPS ports to use, then click **Next**.
8. In the fifth panel of the IBM Director Web-based Access InstallShield Wizard, click **Install**. A new panel displays the installation progress.
9. When installation has completed, click **Finish**.
10. In the dialog which appears, respond to the prompt to reboot the managed system. Click **Yes** to reboot immediately, or click **No** if you will reboot the managed system yourself.

The managed system must be rebooted before Web-based Access will operate.

Installing Web-based Access (unattended installation)

This topic describes the procedure for installing Web-based Access on a Windows managed system using a configured response file.

1. Configure a response file with the correct installation parameters. A response file, `\FILES\wba.rsp`, is included in the installation package. You can edit this file or copy it as a template for creating other response files. Specify the following installation parameters in the response file:
   - whether or not to install help files for Web-based Access
   - which HTTP port to use for standard communications with Web-based Access
   - which HTTPS port to use for secure communications with Web-based Access

   A sample response file follows:

```
[dirwba]=Y
;===============================================================================
; Unattended Web-based Access Installation Response File
;    A semicolon in the first column indicates a comment statement
;
;===============================================================================
;
;  The following parameter is used to install optional component.
;  Specifying Y will install help data files on the target machine.
;
;  WBAHelp = Enable this agent for Point-to-point Help Files.
;
WBAHelp = N
;
;===============================================================================
;
;The following parameters are used to configure Director's Web Server:
;
;  HTTPPort = The port number that the HTTP server uses.  Acceptable values are
;        between 1 and 65535.  The default value is 411.
;
;  HTTPSecPort = The port number that the HTTP server uses for secure
;        communication.  Acceptable values are between 1 and 65535.  The default
;        value is 423.
;
HTTPPort = 411
HTTPSecurePort=423
```

2. Save the configured response file.
3. Click **Start** → **Run**.
4. In the Run dialog, type the following command in the **Open** field and press **Enter**:

```
download\FILES\dir5.10_wba_windows.exe /s /v"/qn rsp=responsefile.rsp"
```

- `download` represents the location to which the download package was unzipped.
- `responsefile.rsp` is the complete path and filename of the response file that you created.

Chapter 3. Starting Web-based Access using a Web browser

You can use a Web-based Access on any Level-1 or Level-2 managed system that is running Windows. Web-based Access must be installed separately on top of IBM Director Core Services or IBM Director Agent.

Perform these steps to start Web-based Access on a local or remote system using a Web browser:

1. Click **Start** → **Programs** → **IBM Director Agent Browser**. The default Web browser starts and opens at the following Web address for the local system:

   http://localhost:*port_number*

   where *port_number* is the port number that is assigned for use by Web-based Access during a separate Web-based Access installation. Port number 411 is the default for initial access, and port number 423 is the default for secure access (https://localhost:423/index.html). If you used different values during configuration, you must use those values instead.
2. In the IBM Director Agent User ID and Password window, type your operating-system user ID and password.
3. (Optional) To view a remote system, type the following address in the Web browser address field:

   http://*system*:*port_number*

   where:

   - *system* is the TCP/IP address of the managed system or the system name of the managed system, as returned by DNS.
   - *port_number* is the port number that is assigned for use by Web-based Access during a separate Web-based Access installation. Port number 411 is the default for initial access, and port number 423 is the default for secure access (https://system:423/index.html). If you used different values during configuration, you must use those values instead.

   The Web browser redirects the Web address to a secure port. A security alert message might be displayed. This is normal when you are accessing a Secure Sockets Layer (SSL) Web site for the first time. IBM Director Agent uses SSL to encrypt the data stream between the system running Web-based Access and the target managed system. This security precaution ensures that others cannot easily see important information such as user login identification and passwords.
4. (Optional) If you do not want to see the security alert message each time you start Web-based Access, install the certificate for the target managed system in the Web browser.
5. Click **OK** to accept the secure connection. A second security alert message might be displayed that warns that the address was not validated by a trusted Certificate Authority. Web browsers typically use SSL to validate the identity of a Web site, but IBM Director Agent uses SSL to protect the password. You can ignore this security alert.
6. Click **Yes** to ignore the security alert message.
7. In the IBM Director Agent User ID and Password window, type the operating-system user name and password that are associated with the targeted managed system.

If the managed system is a member of a domain, it is accessible using domain accounts. You can type your user name using either of the following formats:

- *domain_name\user_name*
- *user_name@domain_name*

where *domain_name* is the name of the domain and *user_name* is your user name.

Your level of access to the managed system is determined by the group membership of the user account that you use to log in. If the user account is a member of the local Administrators group of the system, you have full access by default. If the user account is a member of the local Users group of the system, you have read access. Otherwise, access is denied. You can configure this access policy using applicable Windows administration tools.

A message stating that you must install Java™ VM might be displayed. For information about downloading and installing Java VM, go to this Web site: www.java.com.

A message stating that the Web browser requires the Java Foundation Class/Swing library (JFC/Swing) might be displayed. IBM provides JFC/Swing with IBM Director Agent. You must install JFC/Swing for your Web browser before you access IBM Director Agent data. The first time you use the Web browser for Web-based Access, a Web page is displayed. Complete the following steps to install JFC/Swing:

a. Read and follow the instructions on the Web page.
b. In the File Download window, select the **Open** check box.
c. Click **OK**.
d. Click **Save**. The JFC/Swing library is downloaded. When the installation is complete, the Download window closes.
e. Double-click the downloaded file to run the installer.
f. (Internet Explorer only) Exit Internet Explorer; then, restart Internet Explorer and start Web-based Access. If the JFC/Swing library was successfully installed, Web-based Access opens in the Web browser.

Notes:

a. (Windows XP and Windows Server 2003 only) The operating system is configured by default to deny network access to user accounts with blank passwords. You cannot access the managed system that is running Windows XP or Windows Server 2003 using such an account unless you change the security policy on the managed system. It is a best practice to leave the Microsoft default policy in place and establish secure passwords for accounts that you want to access remotely.
b. The default Guest user account on Windows systems cannot log on to a managed system using Web-based Access. Use an account with user privileges on the local system to log on to a managed system using Web-based Access.

Depending on your user account system access, you gain read/write or read-only access to IBM Director Agent on the managed system. If you have read-only access, some text boxes are unavailable, **Apply** buttons are disabled, and some functions will notify you that you do not have sufficient privilege to access them.

Chapter 4. Viewing managed-system information

The Information services gather hardware information and software information from a managed system. For most of the information services, you cannot change or configure the data that is displayed in the right pane. The Operating System service does provide some information that you can change.

The Information page might contain the following types of services:
- Inventory
- Monitor
- System

Viewing inventory information

Inventory services gather information about the operating system or physical devices that make up the managed system, such as hard disk drives, multimedia adapters, video adapters, and memory.

The following inventory services are available:
- Basic System
- Drives
- FRU Numbers
- Memory
- Multimedia
- Operating System
- Ports

Viewing basic system information

The Basic System service displays general information about the managed-system hardware and operating system.

To start the Basic System service, click **Basic System** from the expanded tree in the left pane. The information is displayed in the right pane.

Note: If a managed object does not have a particular item, the field that is associated with that item is not displayed in the right pane.

Viewing information about physical and logical drives

The Drives service displays information about the physical and logical disk drives that are installed in the managed system.

To start the Drives service, click **Drives** from the expanded tree in the left pane. The Drives notebook is displayed in the right pane and these pages:

Logical Drives

This page is displayed by default. It contains information about the logical drives that are configured on the managed system.

Click any row on the Logical Drives page for additional information. A pie chart shows used space and free space on the selected logical drive. Used space contains the applications and files that are on the disk, and free space is available for adding files or applications.

Physical Drives

This page displays information about the physical drives that are installed in the managed system.

Click any disk row to view whether that physical hard disk has partitions. If the selected disk has partitions, information about the partitions is displayed in the **Partition information** section of the **Physical Drives** page. The partition information is displayed as a pie chart, showing the portion of the total physical disk that is used by each partition.

Viewing FRU information

The FRU Numbers service displays information about the field-replaceable unit (FRU) components that are installed on the managed system. The FRU information is specific to the model type of the system.

Note: FRU information is available for xSeries servers that currently are supported by IBM. For more information, see Appendix B, "FRU data files," on page 29

To start the FRU Numbers service, click **FRU** from the expanded tree in the left pane. The FRU numbers information for the following system components is displayed in the right pane:

- RAID drives and tapes
- CPUs (microprocessors)
- Dual inline memory modules (DIMMs)
- Keyboard
- System board
- CD-ROM drive
- Diskette drive
- Service processor
- Fans
- Backplanes
- (Systems with a Remote Supervisor Adapter only) System board, power supplies, and PCI adapters. The availability of this information varies by the model type of the system.
- (Systems with an IBM ServeRAID™-4 adapter or later installed with ServeRAID™ firmware version 4.84 or later only) RAID physical drives and trays. This item does not include tape drives.

The FRU Numbers service uses FRU data files from the IBM Support FTP site.

Note: If the FRU Numbers service does not detect the presence of the FRU data files, some FRU information might be available from other sources for the FRU Numbers service to display. For example, if you have ServeRAID adapters, ServeRAID FRU data that is on the adapters is displayed.

Viewing memory information

The Memory service gathers information about the physical memory that is installed in the managed system and provides information about memory upgrade options that are available for the managed system.

To start the Memory service, click **Memory** from the expanded tree in the left pane. The Memory notebook is displayed in the right pane and contains these pages:

Physical Memory

This page is displayed by default. This page contains information about the physical memory that is installed in the managed system.

Notes:

1. On servers that support memory compression, the message `Note: Memory compression is enabled` is displayed in the right pane.
2. Information about total spare memory is displayed for some servers, such as the IBM xSeries 252 server.

Upgrade Options

This page displays information about (current) memory upgrade options for the managed system. If you want to install additional memory in the managed system, click the amount of memory that will be your new memory total in the **Show upgrade options for** list. Additional information about memory configuration is displayed.

Notes:

1. All of these options might not be supported. For more information, see your server documentation.
2. The Upgrade Options page recommendations default to using the smallest DIMMs possible. For example, if you have a system with four DIMM sockets that are currently filled with 128 MB DIMMs and you ask for configuration of 2 GB total RAM, the recommendation will be to populate the four DIMM sockets with 512 MB DIMMs, even though two 1 GB DIMMs is a valid recommendation also.
3. The Upgrade Options page recommendations do not take into account requirements for memory that must be added in matching banks. For example, the recommendation might suggest adding three DIMMs of different size, even if the managed system requires that pairs of equal size be added.

Viewing multimedia adapters information

The Multimedia service displays information about multimedia adapters that are installed in the managed system.

To start the Multimedia service, click **Multimedia** from the expanded tree in the left pane. The information is displayed in the right pane.

Note: If an audio or video adapter is not installed in the managed system or if information from the adapter is unavailable, the field that is associated with the missing data is not displayed.

Viewing operating-system information

To start the Operating System service, click **Operating System** from the expanded tree in the left pane. The Operating System notebook is displayed in the right pane and contains these pages:

Operating System

This page is displayed by default. It contains information about the operating system that is installed on the managed system.

Process

This page displays information about the processes or tasks that are currently running on the managed system.

Environment

This page displays information about the environment variables that are used by the operating system running on the managed system.

Drivers

This page displays information about the device drivers that are used by the managed system.

To start a device driver, select the device driver and click **Start**. To stop a device driver, select the device driver and click **Stop**. To change the start mode, click **Start Mode** and make a selection in the window that opens.

Note: You must have administrator privileges to start or stop a device driver or to update its start mode.

This table shows details that are available on the Drivers page.

Table 1. Device driver details

Item	Description
Name	The name of each device driver in the operating-system directory.
Start Mode	The start mode that is assigned to each device driver. Depending on which mode is selected, a device driver is incorporated or not incorporated into the operating environment. **Disabled** The device driver is not added to the operating environment. **Auto** The device driver is started automatically when the operating system is started. **Boot** The device driver is initialized during the operating-system startup (boot) sequence. **Manual** The device driver is started by the user. **System** The device driver is started by the IoInitSystem method.
State	The current run state of each device driver (Running or Stopped).
Command line	The complete path to the device driver (for example, c:\System Root\System32\adapti.sys). To view the complete command line, move the horizontal scroll bar to the right.

Services

This page displays information about the current state and start mode of services that are installed on the managed system. The information and configuration settings that are available on this page are the same as what is provided on the Drivers page.

Viewing input ports information

The Ports service displays information about the input and output (I/O) ports on the managed system.

To start the Ports service, click **Ports** from the expanded tree in the left pane. The information is displayed in the right pane.

Monitoring hardware and software

The Monitor services use system-monitoring hardware and software that is included with IBM Director Agent to gather data about the current operational state of the managed system, such as temperature and contents of the Windows event log on the managed system.

The following Monitor services are available:
- Event Viewer
- System Health

Monitoring events

The Event Viewer service displays the contents of the Windows event log. Applications, device drivers, operating systems, and IBM Director Agent record hardware events and software events in the Windows event logs.

To start the Event Viewer service, click **Event Viewer** from the expanded tree in the left pane. The event-log contents are displayed in the right pane.

The event log can contain a large number of entries. The Event Viewer provides event-log categories and event types to filter the event-log entries that are displayed in the Event Viewer. The Event Viewer service displays the 30 most recent event-log entries that fulfill the event-log category and event-type criteria. Depending on the filter that you select, fewer than 30 entries might be displayed.

To change the event-log category, click the category from the **Log** list that corresponds to the event-log entries that you want to display. The following event-log categories are available:

Application
(Default) Displays the 30 most recent log entries that result from application issues, faults, and problems.

System
Displays the 30 most recent log entries that result from system issues or hardware issues, faults, and problems.

Security
Displays the 30 most recent log entries that result from security problems, such as incorrect user ID or password entries and other attempted security violations.

To filter the event-log entries by event type, select the applicable check boxes at the bottom of the “Event Viewer” window. The event type provides a general description of the severity of the event. The following event types are available:

Information
Displays rows of informational entries that are related to the event-log category that you selected (Application, System, or Security).

Warning
Displays rows of warning entries that are related to the event-log category that you selected.

Error Displays logs that result from security issues, such as password or user ID failures or other access problems, or attempted security violations. It also displays log errors for application and system.

Success Audit
Displays information about successful events.

Failure Audit
Displays information about unsuccessful events.

Only event-log entries that correspond to selected check boxes are displayed in the Event Viewer. For example, if you want to view only entries that result from system errors, click **System** in the **Log** list; then, select the **Error** check box and leave the other check boxes cleared. The 30 most recent entries that fulfill these criteria are displayed.

If you select an event-type check box and no information is displayed, there are no event-log entries that correspond to the selected event type.

To display *all* the event-log entries that fulfill the event-type criteria, click **Load All Events**.

Note: The event log can contain thousands of entries. Clicking **Load All Events** can result in significant delays while the entries are loaded into the Event Viewer.

When an event log is very large, clicking **Load All Events** displays the following error message: `Loading data... please wait.` After 5 minutes, the loading stops, but only the 30 most recent event-log entries are displayed.

You can use the Event Viewer to display additional information about any event-log entry. When you double-click the log entry, a window opens, containing additional information about the event.

Monitoring system health

You can use the System Health service to check the status of all health monitors that are supported by the managed system.

To start the System Health service, click **System Health** from the expanded tree in the left pane. The information is displayed in the right pane.

IBM Director Agent automatically monitors managed systems for changes in a variety of system-environment factors, including temperature and voltage. Each monitored value has a system-health normal range. If the monitored value stays within the normal range, the assumption is that the system health is normal. However, if any of these monitored values falls outside of acceptable system-health parameters, IBM Director Agent can generate output automatically to alert the system administrator of this state change.

To configure the generated output, you must use the Health service from the Tasks page.

IBM Director Agent can generate the following alert output:

- System Health service in Web-based Access
- Indication notification message windows
- Alert messages that are sent as SNMP traps

- Alert messages that are sent as System Management Server (SMS) status messages
- CIM events
- Alert messages that are sent as Tivoli Enterprise Console® events
- Alert messages that are sent as IBM Director Server events
- Windows event-log events

System Health reports are gathered from a variety of system devices. One of these devices is the LM sensor, which performs environmental monitoring. The health reports that are available on a managed system are dependent on the availability of components that contribute to health reports. The following list shows some of the system-health event messages that can be generated and the circumstances that cause them:

Chassis intrusion
If the system chassis has been opened, a Critical system-health event is generated, regardless of the reason.

Fan failure
If the system cooling fan fails, a Critical system-health event is generated. This might be the only prediction of a temperature-related event.

Memory PFA
This is available on some servers. It indicates an IBM Predictive Failure Analysis® (PFA) event from a DIMM.

Processor PFA
This is available on some servers. It indicates a PFA event from a microprocessor.

LAN Leash
This detects whether a managed system is disconnected from the LAN, even when the computer is off. A Critical system-health event is generated if a managed system is disconnected from the LAN.

Low disk space
If free disk space is low, a Warning or Critical system-health event is generated.

Processor removed
If the microprocessor is removed from the managed system, a Warning system-health event is generated.

Temperature out of specification
If the microprocessor temperature is out of the specified range, a Warning system-health event is generated.

Voltage out of specification
If there is a dramatic change in the voltage that is supplied to any part of the managed system or if the voltage is out of the specified range, a Warning or Critical system-health event is generated.

Hard Disk Drive Predictive Failure Alert
If operational thresholds on the hard disk drive are exceeded, PFA events are generated. This information can be generated only for Self-Monitoring, Analysis, and Reporting Technology (SMART) drives.

Power Supply Failure
If the system power supply fails, a Critical system-health event is generated.

Redundant NIC
(Windows only) If a system has multiple network interface cards (NICs) that are configured for automatic failover and a failover or switchback event occurs, a Warning system-health event is generated.

NIC Failure
(Windows only) If a system NIC fails, a Critical system-health event is generated.

NIC Offline
(Windows only) If a system NIC is offline, a Warning system-health event is generated.

NIC Online
(Windows only) If a system NIC is online an Informational system-health event is generated.

Viewing system information

On a system that has a service processor or the applicable sensors, the System service displays current information about the physical devices and their environmental status.

If a server has more than one service processor, only one of the processors provides information to the System service, as follows:

- If a server has an Advanced Systems Management (ASM) processor only (either on the system board or on an ASM PCI adapter), the ASM processor provides the information. If the server also has a Remote Supervisor Adapter, the ASM processor still provides the information.
- If a server has a Remote Supervisor Adapter only, the adapter provides the information.
- If a server has an integrated system management processor (ISMP) only, the ISMP provides the information. If the server also has a Remote Supervisor Adapter, the adapter provides the information.

The following System services are available for any server that has the applicable sensors:

- Fan Speeds
- Temperatures
- Voltages

Note: The realtime sensor information that is displayed by these services corresponds to fan failure, temperature out of specification, and voltage out of specification threshold status provided by the System Health service.

The Management Processor (Mgmt Proc) Event Log service is available for Intelligent Platform Management Interface (IPMI)-based systems.

The Management (Mgmt) Processor Vital Product Data (VPD) System service is available for any server that has an ISMP, ASM, ASM PCI adapter, Remote Supervisor Adapter, or Remote Supervisor Adapter II service processor.

The following System services are available for any server that has an ASM, ASM PCI adapter, Remote Supervisor Adapter, or Remote Supervisor Adapter II service processor:

- Mgmt Proc Event Log
- Power/Restart Activity

- Server Timeouts

Note: When installing IBM Director Agent, you must select the **Management Processor Agent** check box to use the Mgmt Proc Event Log, Mgmt Processor VPD, Power/Restart Activity, and Server Timeouts services. You do not have to select the check box to use the Fan Speeds, Temperatures, and Voltages services.

Viewing the Mgmt Proc Event log

The Management Processor (Mgmt Proc) Event Log service displays entries that are currently stored in the systems-management event log, which is associated with the service processor. These entries are stored in the nonvolatile random access memory (NVRAM) on the service processor.

To start the Event Log service, click **Mgmt Proc Event Log** from the expanded tree in the left pane. The information is displayed in the right pane.

Note: All events are informational unless they are noted as Error or Warning events.

Viewing fan speed information

The Fan Speeds service displays information about fan speeds in the managed system.

To start the Fan Speeds service, click **Fan Speeds** from the expanded tree in the left pane. The information is displayed in the right pane.

Monitoring power and restart activity

The Power/Restart Activity service displays power and restart information for the managed system.

To start the Power/Restart Activity service, click **Power/Restart Activity** from the expanded tree in the left pane. The information is displayed in the right pane.

Viewing server timeouts

The Server Timeouts service displays the settings for the power-on self-test (POST), loader, operating system, and power-off delay timeouts for the managed system.

To start the Server Timeouts service, click **Server Timeouts** from the expanded tree in the left pane. The information is displayed in the right pane.

Monitoring temperatures

The Temperatures service displays the current temperature readings for various hardware components and various thresholds that are configured for the managed system. You cannot alter these thresholds. All temperature readings are in degrees Celsius.

To start the Temperatures service, click **Temperatures** from the expanded tree in the left pane. The information is displayed in the right pane.

Monitoring voltages

The Voltages service displays the current voltage readings for the system board and voltage regulator modules (VRMs) and various thresholds that are configured for the managed system. You cannot alter these thresholds. Each voltage threshold is defined as a low-high value pair.

To start the Voltages service, click **Voltages** from the expanded tree in the left pane. The information is displayed in the right pane.

Viewing Mgmt Processor Vital Product Data (VPD)

The Management (Mgmt) Processor VPD service displays information about the firmware and device driver that are currently installed for the service processor.

To start the Mgmt Processor VPD service, click **VPD Management Product Service** from the expanded tree in the left pane. The information is displayed in the right pane.

Chapter 5. Working with managed systems

You can use the services that are available on the Tasks page to manage the managed systems. Users with less than system-administrator authority can view the available pages, but only system administrators can change or update system configurations and use the available tools.

Web-based Access displays only the tasks that are associated with the components that are installed on a managed system. For example, if SNMP is not installed on a managed system, the SNMP service (under **Configuration**) is not displayed for that system. Requirements and optional installations are noted under each task heading. Certain security levels are required so that users can view or edit selected services in Web-based Access.

Configuring hardware and software settings

The Configuration task provides the following services:
- Asset ID™
- Date and Time
- Network
- SNMP
- System accounts

Configuring hardware information

The Asset ID service allows you to configure hardware information for the managed system.

Note:

- Any information that is entered in Asset ID fields is stored as inventory data in the IBM Director database. You can make queries, take actions, create groups, and generate reports that are based on this inventory data.
- If the managed system has EEPROM, the information is stored in the EEPROM, too. However, data space on the EEPROM is limited; therefore, the Asset ID service limits the amount of information that you can type for managed systems with EEPROM. Not all IBM systems have EEPROM. Systems that do have EEPROM include, but are not limited to, NetVista and ThinkPad computers.

To start the Asset ID service, click **Asset ID** from the expanded tree in the left pane. The Asset ID notebook is displayed in the right pane and contains these pages:

Serialization

This page is displayed by default. The information that is displayed on the page is reported from a number of sources, including but not limited to the system, the system board, hard disk drives, and the microprocessor.

You cannot edit the information on this page.

System

This page displays information about the system name, message authentication code (MAC) address, login name (“” indicates that the system is logged off), operating system, system globally unique identifier (GUID), and Remote Deployment Manager (RDM) profile.

You can edit only the **RDM Profile** field in this page.

User This page displays information about the user of the managed system.

You can edit the information in this page.

Lease This page displays the lease agreement information. You can use this page to track lease contract information, including start date, end date, term (in months), amount, and lessor. You can use the specified end date as a source for an alert.

You can edit the information in this page.

Asset This page displays inventory information about the managed system. You can use this page to track asset information, including the purchase date, last inventoried (the date of the last physical inventory of the system), and asset number. IBM Director automatically saves the date of the last inventory update for each managed system.

You can edit the information in this page.

Personalization

This page contains an edit field that you can use to type information about your users or systems. You can use this page to track any additional information about the managed system. Five fields and their labels are available for customizing. For example, you can customize a field to track the primary function of each managed system.

Note: The number of characters that you can type in these fields is limited and is affected by how many fields you choose to use. The Asset ID service provides a **Data space remaining** indicator along the bottom of the window. Use this indicator to determine how many characters you can still type. If a managed system has EEPROM, the available data space is significantly less than the available data space in a managed system that does not have EEPROM. You cannot type as many characters for a managed system with EEPROM, because space is limited on the EEPROM.

You can edit the information in this page.

Warranty

This page displays information about the warranty on the managed system. You can use this page to track warranty data for the system, including duration (in months), cost, and end date. You can use the specified end date as a source for an alert. If the warranty duration expires, you can select to have these alerts sent to your management server. The alerts are displayed in the **Other** category of the Health services page.

You can edit the information in this page.

Although the fields on these pages are labeled for specific information, you do not have to provide the specific information that is indicated by each label. The labels are suggestions for information that you can provide.

Setting the date and time

Use the Date and Time service to set the date and time that are displayed on the managed system.

To start the Date and Time service, click **Date and Time** from the expanded tree in the left pane. Separate fields for the month, day, year, and local time are displayed in the right pane.

Configuring the network

The Network service provides information about your network. This service is useful for remote configuration. To start the Network service, click **Network** from the expanded tree in the left pane. The Network notebook is displayed in the right pane and contains these pages:

IP Address
This page is displayed by default. This page contains the routing information for your network.

DNS This page displays information about Domain Name System (DNS). DNS is the distributed database system that is used to map domain names to IP addresses.

WINS This page displays information about Windows Internet Naming Service (WINS) .

If you make changes to this page, you must click **Apply** to save the changes.

Domain/Workgroup
This page displays information about the managed system and its associated domain or workgroup is also displayed on the Domain/Workgroup page.

If you make changes to this page, you must click **Apply** to save the changes.

Modem
This page displays modem information.

Configuring SNMP

The SNMP service provides the ability to work with community strings that are used in network communication and to set trap destination addresses.

To start the SNMP service, click **SNMP** from the expanded tree in the left pane. The information is displayed in the right pane.

Note: The SNMP task is displayed in the task list only if the SNMP service is installed on the operating system that is running on the managed system.

Configuring system accounts

The System Accounts service provides remote administration of user security and group security within a Windows operating system.

To start the System Account service, click **System Accounts** from the expanded tree in the left pane. The System Accounts notebook is displayed in the right pane and contains these pages:

Users This page displays a list of global users. You can review and edit users from this page.

Groups

This page displays a list of global groups. You can review and edit members within the group.

When you click an item in the user or groups list, the **Properties** and **Delete** buttons are enabled. Use the **Properties** button to edit or view user or group properties. If you make changes on these pages, you must click **Apply** to save the changes. If you click **Add**, the Add notebook is displayed in the right pane and contains these pages:

General

The page is displayed by default. You can use this page to give system users the appropriate security levels and password options.

Member Of

This page displays a group membership list. Members are listed in the left pane, and nonmember groups are listed in the right pane. Clicking the **<** and **>** buttons moves user names to and from the **Member groups** and **Non-member groups** lists.

Profile

This page allows you to configure user profiles. You must provide this information on this page.

Item	Description
Path	The network path to the user's profile folder. Type a network path in the form \\*server_name**profile_folder_name**user_name*.
Logon script	A script that is assigned to a user account that runs each time the user logs on.

Password

This page allows you to type a new password or change an existing password. You must provide this information on this page.

Item	Description
New password	This field contains the user's new password (32 character maximum, case sensitive).
Confirm password	This field must contain the same character string as the **New Password** field (32 character maximum, case sensitive).

Powering off and restarting managed systems

The Shutdown service provides the following options for shutting down a managed system.

To shutdown and power off a managed system, click the **Tools** service in the left pane, click **Tools**, and then click **Shutdown** from the expanded tree. The Shutdown options are displayed in the right pane.

Note: This option is available only on systems on which Advanced Power Management is supported and enabled.

To start the shutdown and restart the managed system without turning it off, click the **Shutdown and Power Off** service in the left pane, click **Tools**, and then click **Restart** from the expanded tree.

Updating system device drivers

The System Updates service connects to an IBM Web site that provides the latest device drivers and news about your selected managed system. This service works only if the system can access the Internet.

To start the System Updates service, click **System Updates** from the expanded tree in the left pane. The System Updates page is displayed in the right pane. A table displays information about the managed system, including model number, serial number, operating system, and version number.

To access the latest device drivers, technical information, and news about the managed system, click **Drivers**.

Saving authentication keys to a managed system

This task applies to only managed systems with ASF 2.0 capability.

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

1. Using Web-based Access, connect to the managed system.
2. Click the **Tasks** tab from the left pane.
3. Click the **ASF** from the left pane.
4. Click the **Remote Management** tab from the right pane.
5. Type the authentication keys or click the **Generate** button to automatically generate authentication keys.
6. Click **Apply** to save any entries or changes that you have made.

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

This topic describes how to configure a custom access policy for Web-based Access.

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.

To customize the access policy, complete the following steps:

1. Using Windows Explorer, select the admin4.txt file. If you installed IBM Director Agent in the default location, this file is located in the Program Files\IBM\ Director\websrv\cgi-bin directory.
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 the Program Files\IBM\ Director\websrv\cgi-bin directory.

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.

Chapter 6. Troubleshooting

Use this section to troubleshoot and resolve problems with Web-based Access.

Problems logging in to the managed system using Netscape Navigator

This problem affects Web-based Access and Netscape Navigator.

Problem

After repeated installations, there are problems logging in to the managed system using Netscape Navigator.

Investigation

When you uninstall IBM Director Agent, be sure to save the configuration data. This saves the old Secure Sockets Layer (SSL) certificate and allows the login to the IBM Director Agent Web Server to be successfully completed after IBM Director Agent is reinstalled.

Chinese characters might be displayed as boxes

This problem only affects systems using Traditional or Simplified Chinese.

Problem

When you open Web-based Access in a Netscape Web browser, the Chinese characters might be displayed as boxes.

Investigation

Complete the following steps to ensure that Chinese characters are displayed correctly:

1. Install the latest Java Plug-in that is available from Sun Microsystems.
2. Check the Windows Display Properties settings to make sure that they are set correctly for Chinese language display.

Web-based Access is unavailable

This problem only affects systems running Apache Web Server.

Problem

When you install Web-based Access on a managed system that is running Apache Web Server, Web-based Access is unavailable. An error message is displayed indicating that the page cannot be found.

Investigation

Web-based Access and Apache Web Server use the same default connector ports. You must modify the Web-based Access configuration files. If you installed IBM

Director Agent in the default location, these files are located in the Program Files\IBM\Director\websrv\conf directory. Complete the following steps to resolve this problem:

1. Stop the IBM Director Agent Web Server service.
2. Modify the server.xml file:
   - Change the server port to a port that is not already in use by another application. By default, the server port is set to 8005.
   - Change the connector port to a port that is not already in use by another application. By default, it is set to 8009.
3. Modify the workers.properties file. Change the connector port to a port that is not already in use by another application. By default, it is set to 8009.
4. Modify the tomcat.conf file. Change the connector port to a port that is not already in use by another application. By default, it is set to 8009.
5. Restart the IBM Director Agent Web Server service.

A Java security warning is displayed

This problem affects Web-based Access and Microsoft Internet Explorer.

Problem

After you log in to Microsoft Internet Explorer, a Java security warning is displayed.

Investigation

If you are using Microsoft Internet Explorer with the Sun Java Plug-in, additional prompts appear when you log in to a managed system. After you log in to Microsoft Internet Explorer, a Java Security Warning is displayed. Select **Grant this session**. The Java Plug-in requires authentication information. Type the same information that you used for the Microsoft Internet Explorer login.

A message is displayed stating that Java Virtual Machine is needed

This problem affects only systems running Windows XP or Windows Server 2003.

Problem

A message is displayed stating that Java Virtual Machine (JVM) is needed.

Investigation

Install a Java Virtual Machine (JVM) from Sun Microsystems.

Appendix A. Supported Web browsers for Web-based Access

The topic provides information about the Web browsers that are supported for Web-based Access.

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

- Microsoft Internet Explorer, version 4.01 or later
- Netscape Navigator, version 4.7x
- Netscape Navigator, version 7.01 or later

Notes:

1. Your Web browser must support Java applets.
2. If you are using Internet Explorer, you must use 56-bit encryption or higher.

Appendix B. FRU data files

IBM Director obtains field-replaceable unit (FRU) data files for use with some tasks.

IBM Director obtains information about the field-replaceable unit (FRU) components that are installed in a managed system from the IBM Support FTP site (ftp://ftp.software.ibm.compc/pccbbs/bp_server). The FRU information is contained in a FRU data file that is:

- Specific to the managed system server model type
- Available only for xSeries servers that currently are supported by IBM

IBM Director makes one attempt to copy the FRU data file:

For managed systems running Linux®	The copy occurs during the IBM Director Agent installation on the managed system.
For managed systems running Windows	The copy occurs the first time you restart the managed system after IBM Director Agent is installed.

For the copy to succeed, the managed system must be connected to the network and have firewall access through a standard FTP port. By default, IBM Director attempts to reach the IBM Support FTP site on FTP port 21. After IBM Director successfully copies the FRU data file to the managed system, the FRU data file is processed and the FRU information is stored in the CIM server. Then, IBM Director deletes the FRU data file from the managed system.

Appendix C. Contacting customer support

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 section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation system, and whom to call for service, if it is necessary.

Before you call

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

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *xSeries Documentation* CD or in the IntelliStation *Hardware Maintenance Manual* at the IBM Support Web site.
- Go to the IBM Support Web site at www.ibm.com/pc/support/ to check for technical information, hints, tips, and new device drivers or to submit a request for information.

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

Using the documentation

Information about your IBM xSeries or IntelliStation system and preinstalled software, if any, is available in the documentation that is included 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 www.ibm.com/pc/support/ and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi.

Getting help and information from the World Wide Web

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

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

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
MW9A/050
5600 Cottle Road
San Jose, CA 95193
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

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

AIX

AIX 5L

Alert on LAN

Asset ID

- BladeCenter
- DB2
- DB2 Universal Database
- DirMaint
- Electronic Service Agent
- Enterprise Storage Server
- eServer
- eServer logo
- FlashCopy
- HiperSockets
- i5/OS
- IBM
- IBM logo
- ibm.com
- IntelliStation
- iSeries
- Netfinity
- NetServer
- NetView
- OS/400
- POWER
- Predictive Failure Analysis
- pSeries
- RACF
- Redbooks
- ServeProven
- SurePOS
- System p5
- System z9
- Tivoli
- Tivoli Enterprise
- Tivoli Enterprise Console
- Virtualization Engine
- Wake on LAN
- xSeries
- z/VM
- zSeries

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

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

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

Abbreviations, Acronyms, and Glossary

Abbreviation and acronym list

This topic lists abbreviations and acronyms used in the IBM Director documentation.

Table 2. Abbreviations and acronyms used in IBM Director documentation

Abbreviation or acronym	Definition
AES	advanced encryption standard
APAR	authorized program analysis report
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI Adapter
BIOS	basic input/output system
CEC	Central Electronics Complex
CIM	Common Information Model
CIMOM	Common Information Model Object Manager
CP	control program
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management
CSV	comma-separated value
DASD	direct access storage device
DBCS	double-byte character set
DES	data encryption standard
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DMI	Desktop Management Interface
DMTF	Distributed Management Task Force
DNS	Domain Name System
DSA	Digital Signature Algorithm
EEPROM	electrically erasable programmable read-only memory
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	file transfer protocol
GB	gigabyte
Gb	gigabit
GMT	Greenwich Mean Time
GUI	graphical user interface
GUID	globally unique identifier
HMC	Hardware Management Console
HTML	hypertext markup language
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPMI	Intelligent Platform Management Interface
IPX	internetwork packet exchange
ISDN	integrated services digital network
ISMP	integrated system management processor
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	kilobits per second
KVM	keyboard/video/mouse
LAN	local area network
LED	light-emitting diode
LPAR	logical partition
MAC	media access control

Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
MB	megabyte
Mb	megabit
Mbps	megabits per second
MD5	message digest 5
MDAC	Microsoft Data Access Control
MHz	megahertz
MIB	Management Information Base
MIF	Management Information Format
MMC	Microsoft Management Console
MPA	Management Processor Assistant
MPCLI	Management Processor Command-Line Interface
MSCS	Microsoft Cluster Server
MST	Microsoft software transformation
NIC	network interface card
NNTP	Network News Transfer Protocol
NTP	network time protocol
NVRAM	nonvolatile random access memory
ODBC	Open DataBase Connectivity
OID	object ID
PCI	peripheral component interconnect
OSA	Open Systems Adapter
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PFA	Predictive Failure Analysis
POST	power-on self-test
PTF	program temporary fix
RAM	random access memory
RDM	Remote Deployment Manager
RPM	(1) Red Hat Package Manager (2) revolutions per minute
RSA	Rivest-Shamir-Adleman
RXE	Remote Expansion Enclosure

Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
SAS	Serial Attached SCSI
SATA	Serial ATA
SCSI	Small Computer System Interface
SFS	shared file system
SHA	Secure Hash Algorithm
SI	Solution Install
SID	(1) security identifier (2) Oracle system identifier
SLP	service location protocol
SLPD	service location protocol daemon
SMBIOS	System Management BIOS
SMI	System Management Information
SMP	symmetric multiprocessor
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SMI-S	Storage Management Initiative Specification
SNMP	Simple Network Management Protocol
SPB	software package block
SQL	Structured Query Language
SSH	Secure Shell
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
USB	Universal Serial Bus
UUID	universal unique identifier
VPD	vital product data

Table 2. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
VMRM	Virtual Machine Resource Manager
VRM	voltage regulator module
WAN	wide area network
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
WQL	Windows Management Instrumentation Query Language
XML	extensible markup language

Glossary

This glossary includes terms and definitions from:

- The *American National Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018. Definitions are identified by the symbol (A) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Committee (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- The *IBM Glossary of Computing Terms*, 1999.

To view other IBM glossary sources, see IBM Terminology at www.ibm.com/ibm/terminology.

A

Advanced Encryption Setting (AES)
A block cipher algorithm, also known as Rijndael, used to encrypt data transmitted between managed systems and the management server, which employs a key of 128, 192, or 256 bits. AES was developed as a replacement for DES.

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

Advanced System Management (ASM) interconnect network
A network of IBM servers created by using the ASM interconnect feature. The servers are connected through RS-485 ports. When servers containing integrated system management processors (ISMPs) and ASM processors are connected to an ASM interconnect network, IBM Director can manage them out-of-band.

Advanced System Management (ASM) PCI adapter
An IBM service processor that is built into the Netfinity® 7000 M10 and 8500R servers. It also was available as an option that could be installed in a server that contained an ASM processor. When an ASM PCI adapter is used with an ASM processor, the ASM PCI adapter acts as an Ethernet gateway, while the ASM processor retains control of the server. When used as a gateway service processor, the ASM PCI adapter can communicate with other ASM PCI adapters and ASM processors only.

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

a Remote Supervisor II must serve as the gateway service processor.

alert A message or other indication that identifies a problem or an impending problem.

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

alert-forwarding profile
A profile that specifies where remote alerts for the service processor should be sent.

alert standard format (ASF)
A specification created by the Distributed Management Task Force (DMTF) that defines remote-control and alerting interfaces that can best serve a client system in an environment that does not have an operating system.

anonymous command execution
Execution of commands on a target system as either *system account* (for managed systems running Windows) or *root* (for managed systems running Linux). To restrict anonymous command execution, disable this feature and always require a user ID and password.

ASF See *alert standard format*.

ASM interconnect gateway
See *gateway service processor*.

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

B

basic input/output system (BIOS)
The code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BIOS See *Basic Input/Output System*.

blade server
An IBM @server BladeCenter server. A high-throughput, two-way, Intel® Xeon-based server on a card that supports symmetric multiprocessors {SMP}.

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

bottleneck
A place in the system where contention for a resource is affecting performance.

C

chassis
The metal frame in which various electronic components are mounted.

chassis detect-and-deploy profile
A profile that IBM Director automatically applies to all new BladeCenter chassis when they are discovered. The profile settings include management module name, network protocols, and static IP addresses. If Remote Deployment Manager (RDM) is installed on the management server, the chassis detect-and-deploy profile also can include deployment policies.

CIM See *Common Information Model*.

Common Information Model (CIM)
An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

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 cryptographic algorithm designed to encrypt and decrypt data using a private key.

database server
The server on which the database application and database used with IBM Director Server are installed.

deployment policy
A policy that associates a specific bay in a BladeCenter chassis with an RDM noninteractive task. When a blade server is added to or replaced in the bay, IBM Director automatically runs the RDM task.

DES See *Data Encryption Standard*.

Desktop Management Interface (DMI)
A protocol-independent set of application programming interfaces (APIs) that were defined by the Distributed Management Task Force (DMTF). These interfaces give management application programs standardized access to information about hardware and software in a system.

Diffie-Hellman key exchange
A public, key-exchange algorithm that is used for securely establishing a shared secret over an insecure channel. During Phase II negotiations, the Diffie-Hellman group prevents someone who intercepts your key from deducing future keys that are based on the one they have.

digital signature algorithm (DSA)
A security protocol that 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.

discovery
The process of finding resources within an enterprise, including finding the new location of monitored resources that were moved.

DMI See *Desktop Management Interface*.

E

enclosure
A unit that houses the components of a storage subsystem, such as a control unit, disk drives, and power source.

event An occurrence of significance to a task or system, such as the completion or failure of an operation. There are two types of events: alert and resolution.

event action
The action that IBM Director takes in response to a specific event or events.

event-action plan
A user-defined plan that determines how IBM Director will manage certain events. An event action plan comprises one or more event filters and one or more customized event actions.

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 to which the filter is assigned.

extension
See *IBM Director extension*.

F

field-replaceable unit (FRU)
An assembly that is replaced in its entirety when any one of its components fails. In some cases, a FRU may contain other FRUs.

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 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*.

G

gateway service processor
A service processor that relays alerts from service processors on an Advanced

System Management (ASM) interconnect network to IBM Director Server.

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

GUID See *Universal Unique Identifier*.

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, and IPX.

IBM Director Console
A component of IBM Director software. When installed on a system, it provides a graphical user interface (GUI) for accessing 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 includes systems, BladeCenter chassis, software, SNMP devices.

IBM Director extension
A tool that extends the functionality of IBM Director. Some of the IBM Director extensions are Capacity Manager, ServeRAID Manager, Remote Deployment Manager, Software Distribution.

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

IBM Director service account
The Windows operating-system account associated with the IBM Director Server service.

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

integrated system management processor (ISMP)
A service processor built into the some xSeries servers. The successor to the Advanced System Management (ASM) processor, the ISMP does not support in-band communication in systems running NetWare. For IBM Director Server to connect out-of-band to an ISMP, the server containing the ISMP must be installed on an ASM interconnect network. A Remote Supervisor Adapter or a Remote Supervisor Adapter II must serve as the gateway service processor.

interprocess communication (IPC)
1) The process by which programs communicate data to each other and synchronize their activities. Semaphores, signals, and internal message queues are common methods of interprocess communication. 2) A mechanism of an operating system that allows processes to communicate with each other within the same computer or over a network. It also is called in-band communication

inventory-software dictionary
A file that tracks the software installed on managed systems in a network.

IPC See *interprocess communication*.

ISMP See *integrated system management processor*.

J

job A separately executable unit of work defined by a user, and run by a computer.

L

Level-0 managed system
An IBM or non-IBM server, desktop computer, workstation, or mobile computer, that can be managed by IBM Director but does not have any IBM Director software installed on it.

Level-1 managed system
An IBM or non-IBM server, desktop computer, workstation, and mobile computer that has IBM Director Core Services installed. IBM Director uses IBM Director Core Services to communicate with and administer the Level-2 managed system. IBM Director Core Services includes the SLP instrumentation, the IBM Director Agent SLP service type, and Common Information Model (CIM).

Level-2 managed system
An IBM or non-IBM server, desktop computer, workstation, or mobile computer that has IBM Director Agent installed. IBM Director Agent provides managed systems with the full complement of IBM Director Agent function that is used to communicate with and administer the Level-2 managed system. The function of a Level-2 managed system varies depending on the operating system and platform.

light path diagnostics
A technology that provides a lighted path to failed or failing components to expedite hardware repairs.

M

MAC address
See media access control (MAC) address.

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

managed object
An item managed by IBM Director. In IBM Director Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or scalable system, for example).

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

managed system
A system that is being controlled by a given system management application, for example, a system managed by IBM Director.

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 system-management functions. It configures the chassis and switch modules, communicates with the blade servers and all I/O modules, multiplexes the keyboard/video/mouse (KVM), and monitors critical information about the chassis and blade servers.

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

media access control (MAC) address
In a local area network, the protocol that determines which device has access to the transmission medium at a given time.

N

nonvolatile random-access memory (NVRAM)
Random access memory (storage) that retains its contents after the electrical power to the machine is shut off.

notification
See *alert*.

NVRAM
See *nonvolatile random-access memory*.

O

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

P

partition
See *scalable partition*.

PCI See *Peripheral Component Interconnect*.

PCI-X See *Peripheral Component Interconnect-X*.

Peripheral Component Interconnect (PCI)
A standard for connecting attached devices to a computer.

Peripheral Component Interconnect-X (PCI-X)
An enhancement to the Peripheral Component Interconnect (PCI) architecture. PCI-X enhances the Peripheral Component Interconnect (PCI) standard by doubling the throughput capability and providing additional adapter-performance options while maintaining backward compatibility with PCI adapters.

PFA See *Predictive Failure Analysis*.

physical platform
An IBM Director managed object that represents a single physical chassis or server that has been discovered through the use of the Service Location Protocol (SLP).

plug-in
A software module, often written by a third party, that adds function to an existing program or application such as a Web browser. See *IBM Director extension*.

POST See *power-on self-test*.

power-on self-test
A series of internal diagnostic tests activated each time the system power is turned on.

Predictive Failure Analysis (PFA)
A scheduled evaluation of system data that detects and signals parametric degradation that might lead to functional failures.

private key
1) In secure communication, an algorithmic pattern used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to decrypt messages that were encrypted by the corresponding public key. The private key is kept on the user's system and is protected by a password. 2) The secret half of a cryptographic key pair that is used with a public key algorithm. Private keys are typically used to digitally sign data and to decrypt data that has been encrypted with the corresponding public key.

public key
1) In secure communication, an algorithmic pattern used to decrypt messages that were encrypted by the corresponding private key. A public key is also used to encrypt messages that can be decrypted only by the corresponding private key. Users broadcast their public keys to everyone with whom they must exchange encrypted messages. 2) The non-secret half of a cryptographic key pair that is used with a public key algorithm. Public keys are typically used to verify digital signatures or decrypt data that has been encrypted with the corresponding private key.

R

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

remote I/O enclosure
An IBM Director managed object that represents an expansion enclosure of Peripheral Component Interconnect-X (PCI-X) slots, for example, an RXE-100 Remote Expansion Enclosure. The enclosure consists of one or two expansion kits.

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

resolution
The occurrence of a correction or solution to a problem.

resource-monitor threshold
The point at which a resource monitor generates an event.

RXE Expansion Port
The dedicated high-speed port used to connect a remote I/O expansion unit, such as the RXE-100 Remote Expansion Enclosure, to a server.

S

scalable node
A physical platform that has at least one SMP Expansion Module. Additional attributes are assigned to a physical platform when it is a scalable node. These additional attributes record the number of SMP Expansion Modules, SMP Expansion Ports, and RXE Expansion ports on the physical chassis.

scalable object
An IBM Director managed object that is used with Scalable Systems Manager. Scalable objects include scalable nodes, scalable systems, scalable partitions, and remote I/O enclosures that are attached to scalable nodes.

scalable partition
An IBM Director managed object that defines the scalable nodes that can run a single image of the operating system. A scalable partition has a single, continuous memory space and access to all associated adapters. A scalable partition is the logical equivalent of a physical platform. Scalable partitions are associated with scalable systems and comprise only the scalable nodes from their associated scalable systems.

scalable system
An IBM Director managed object that consists of scalable nodes and the scalable partitions that are composed of the scalable nodes in the scalable system. When a scalable system contains two or more scalable nodes, the servers that they represent must be interconnected through their SMP Expansion Modules to make a multinode configuration, for example, a 16-way xSeries 455 server made from four scalable nodes.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Service Location Protocol (SLP)
In the Internet suite of protocols, a protocol that identifies and uses network hosts without having to designate a specific network host name.

service processor
A generic term for Remote Supervisor Adapters, Advanced System Management processors, Advanced System Management PCI adapters, and integrated system management processors (ISMPs). These hardware-based management processors used in IBM Netfinity and xSeries servers work with IBM Director to provide hardware status and alert notification.

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.

SNMP Access and Trap Forwarding
An IBM Director Agent feature that enables SNMP to access managed-system data. When installed on a managed system, this feature enables SNMP-based managers to poll the managed system and receive its alerts. If System Health Monitoring is installed on the managed system also, hardware alerts can be forwarded as SNMP traps.

SNMP device
A network device, printer, or computer that has an SNMP device installed or embedded.

SQL See *Structured Query Language*

SSL See *Secure Sockets Layer*.

static partition
A view-only scalable partition.

sticky key
An input method that enables the user to press and release a series of keys sequentially (for example, Ctrl+Alt+Del), yet have the keys behave as if they were pressed and released at the same time. This method can be used for those who require special-needs settings to make the keyboard easier to use.

Structured Query Language (SQL)
A standardized language for defining and manipulating data in a relational database.

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
The computer and its associated devices and programs.

System Health Monitoring
An IBM Director Agent feature that provides active monitoring of critical system functions, including system temperatures, voltages, and fan speeds. It also handles in-band alert notification for managed systems running Windows and some managed systems running Linux.

system variable
A user-defined keyword and value pair that can be used to test and track the status of network resources. System variables can be referred to wherever event-data substitution is allowed.

systems management BIOS (SMBIOS)
A key requirement of the Wired for Management (WfM) 2.0 specification. SMBIOS extends the system BIOS to support the retrieval of management data required by the WfM specification. To run IBM Director Agent, a system must support SMBIOS, version 2.2 or later.

T

target system
A managed system on which an IBM Director task is performed.

time to live (TTL)
A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

triple data encryption standard (DES)
A block cipher algorithm that can be used to encrypt data transmitted between managed systems and the management server. Triple DES is a security enhancement of DES that employs three successive DES block operations.

TTL See *time to live*.

U

universal unique identifier (UUID)
A 128-bit character string guaranteed to be globally unique and used to identify components under management.

uptime
The time during which a system is working without failure.

upward integration
The methods, processes and procedures that enable lower-level systems-management software, such as IBM Director Agent, to work with higher-level systems-management software, such as Tivoli Enterprise™ or Microsoft SMS.

upward integration module
Software that enables higher-level systems-management software, such as Tivoli Enterprise or Microsoft Systems Manager Server (SMS), to interpret and display data provided by IBM Director Agent. This module also can provide enhancements that 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)
Information that uniquely defines the system, hardware, software, and microcode elements of a processing system.

VPD See *vital product data*.

W

Wake on LAN®
A technology that enables a user 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, users of this technology can remotely turn on a server and control it across the network, thus

saving time on automated software installations, upgrades, disk backups, and virus scans.

walk An SNMP operation that is used to discover all object instances of management information implemented in the SNMP agent that can be accessed by the SNMP manager.

Windows Management Instrumentation (WMI)
An application programming interface (API) in the Windows operating system that enables devices and systems in a network to be configured and managed. WMI uses the Common Information Model (CIM) to enable network administrators to access and share management information.

WMI See *Windows Management Instrumentation*.

WMI Query Language (WQL)
A subset of the Structured Query Language with minor semantic changes to support Windows Management Instrumentation.

WQL See *WMI Query Language*.

Index

Readers' Comments — We'd Like to Hear from You

IBM Systems
IBM Director
Web-based Access Installation and User's Guide
Version 5.10

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Dept. CGFA
PO Box 12195
Research Triangle Park, NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in USA