



IBM Systems

IBM Director System Availability Installation and User's Guide

Version 5.10





IBM Systems

IBM Director System Availability
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 5.10 of IBM Director and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 1999, 2005. All rights reserved.

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

Contents

Figures	v	Chapter 3. Monitoring system availability	11
Tables	vii	Viewing system availability	11
About this book	ix	Changing the graph dates	12
Who should read this book	ix	Changing the settings criteria for System Availability	13
Conventions and terminology	ix	Saving the system-availability report	13
Related information	ix	Appendix A. System Availability window	15
How to send your comments	xi	Appendix B. System Availability events	19
Chapter 1. Getting started	1	Appendix C. Operating systems supported by System Availability	21
Introducing IBM Director	1	Appendix D. Notices	23
System Availability	2	Trademarks	24
Chapter 2. Installing System Availability	5	Abbreviation and acronym list	27
Installing System Availability on a Windows server	6	Glossary	31
Installing System Availability on a Linux server	6	Index	43
Installing the System Availability extension on a Windows console	7		
Installing the System Availability extension on a Linux console	7		
Installing the System Availability extension on a managed Windows system	8		
Installing the System Availability extension on a managed Linux system	9		

Figures

1. Hardware in an IBM Director environment 2

Tables

- | | | | |
|---|----|--|----|
| 1. Operating systems supported by xSeries servers | 21 | 3. Operating systems supported by System z9 and zSeries servers | 22 |
| 2. Operating systems supported by iSeries servers and System p5 and pSeries servers | 22 | 4. Abbreviations and acronyms used in IBM Director documentation | 27 |

About this book

This book provides information about installing and using IBM Director System Availability.

Who should read this book

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. Getting started

Introducing IBM Director

This topic provides an overview of IBM Director.

IBM Director is an integrated, easy-to-use suite of tools that provide you with comprehensive systems-management capabilities to help realize maximum system availability and lower IT costs. Its open, industry-standard design enables heterogeneous-hardware management and broad operating-system support, including most Intel[®] microprocessor-based systems and certain IBM **@server** System p5[®], iSeries, pSeries, System z9[®], and zSeries servers.

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

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

IBM Director environment

IBM Director is designed to manage a complex environment that contains numerous servers, desktop computers, workstations, mobile computers (notebook computers), and assorted devices. IBM Director can manage up to 5000 Level-2 systems.

An IBM Director environment contains the following groups of hardware:

- One or more servers on which IBM Director Server is installed. Such servers are called *management servers*.
- Servers, workstations, desktop computers, and mobile computers that are managed by IBM Director. Such systems are called *managed systems*.
- Network devices, printers, or computers that have Simple Network Management Protocol (SNMP) agents installed or embedded. Such devices are called *SNMP devices*.
- Additional managed objects such as platforms and chassis. Collectively, all managed systems, devices, and objects are referred to as *managed objects*.

Figure 1 on page 2 shows the hardware in an IBM Director environment.

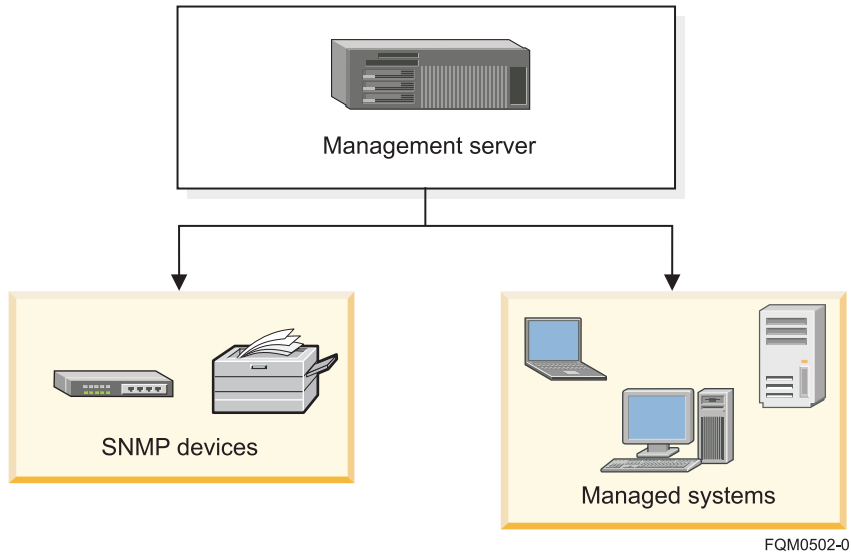



Figure 1. Hardware in an IBM Director environment

System Availability

Use the System Availability task to analyze the availability of a managed system or group. You can view statistics about managed-system uptime and downtime through reports and graphical representations.

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

Icon	
Supported IBM Director objects	Level-2 managed systems
Supported operating systems	For detailed operating-system support information, see the IBM Director information center on the Web at publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html .
Availability	Extension to the IBM Director product. You can download the extension from the IBM Support Web site at www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/ .
Required hardware or hardware limitations	Designed specifically for use on xSeries and Netfinity [®] servers.
Required software	To use the function that identifies a managed system as problematic, IBM Director (version 4.1 or later) System Availability Agent must be installed on the managed system.
Required protocols	None

Required device drivers	None
Mass Configuration support	No
Scheduler support	Yes
Files associated with this task	<ul style="list-style-type: none"> • (Windows[®] only) The System Availability task uses information from the system log file; a damaged, missing, or full system log file affects this task. If you clear the system log file, all system-availability information is lost. • (Linux[®] only) The System Availability task uses information from the /var/log/messages file. • IBM Director Server stores system-availability reports in the IBM\Director\Reports\System Availability directory on the management server. You can change the location where IBM Director Server stores system-availability reports in the Settings window.
Events associated with this task	<p>System Availability</p> <p>For detailed events information, see the IBM Director information center on the Web at publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dirinfo/fqm0_main.html.</p>

Chapter 2. Installing System Availability

This topic describes the general procedure for installing the System Availability extension for IBM Director 5.10.

System Availability may be installed on both Linux on xSeries and Windows platforms. Installing System Availability is performed in several steps, each of which is described in a topic in this section.

1. Download the System Availability extension.
 - a. In a Web browser, navigate to the following Web site:
www.ibm.com/servers/eserver/xseries/systems_management/ibm_director/.
 - b. Navigate to the System Availability extension for your operating system, and download the extension files to a temporary directory.
2. Install System Availability on the management server.

Option	Description
Windows server	"Installing System Availability on a Windows server" on page 6
Linux server	"Installing System Availability on a Linux server" on page 6

3. **Optional:** Install System Availability user-interface components for IBM Director Console on remote management consoles.

Option	Description
Windows console	"Installing the System Availability extension on a Windows console" on page 7
Linux console	"Installing the System Availability extension on a Linux console" on page 7

Note: System Availability user-interface components for IBM Director Console are automatically installed on the management server when the System Availability server components are installed. It is not necessary or possible to separately install System Availability console components on a management server.

4. Install System Availability components for IBM Director Agent on managed systems.

Option	Description
Windows systems	"Installing the System Availability extension on a managed Windows system" on page 8
Linux systems	"Installing the System Availability extension on a managed Linux system" on page 9

Note: System Availability agent components are automatically installed on the management server when the System Availability server components are installed. It is not necessary or possible to separately install System Availability agent components on a management server.

Installing System Availability on a Windows server

This topic describes the procedure for installing the System Availability extension for IBM Director on a Windows management server.

Complete the following steps to install System Availability on a Windows management server:

1. Copy the downloaded installation files to a temporary directory on the machine on which you will be performing the installation.
2. Close all applications, including any command-prompt windows.
3. Click **Start** → **Run**.
4. In the Run dialog, type the following command in the **Open** field and press **Enter**:

```
download\dir5.10_sysavailserver_windows.exe
```

download represents the location into which the download package was saved.

5. In the first panel of the System Availability Server InstallShield Wizard, click **Next**.
6. In the second panel of the System Availability Server InstallShield Wizard, select **I accept the terms in the license agreement**, then click **Next**.
7. In the third panel of the System Availability Server InstallShield Wizard, click **Install**. A new panel displays the installation progress.
8. When installation has completed, click **Finish**.

Installing System Availability on a Linux server

This topic describes the procedure for installing System Availability on a Linux management server.

System Availability can only be installed on management servers running Linux for xSeries.

Complete the following steps to install System Availability on a Linux management server:

1. Copy the downloaded installation files to a temporary directory on the machine on which you will be performing the installation.
2. Stop IBM Director Server. From a command prompt, type the following command and press **Enter**:

```
/opt/ibm/director/bin/twgstop
```

3. Change to the directory in which the installation package is located. Type the following command and press **Enter**:

```
cd /download/
```

download represents the location to which the download package was saved.

4. Type one of the following commands and press **Enter**:

Installation scenario	Command
Performing a new installation	<code>rpm -ivhSysAvailServer-5.10-1.i386.rpm</code>
Upgrading from a previous version	<code>rpm -Uvh --relocate /opt/ibm/director=/opt/IBM/director SysAvailServer-5.10-1.i386.rpm</code>

The installation progress is displayed.

5. Restart IBM Director Server. From a command prompt, type the following command and press **Enter**:

```
/opt/ibm/director/bin/twgstart
```

The IBM Director System Availability Server installation process installs the server, console, and agent components of System Availability on the management server.

Installing the System Availability extension on a Windows console

This topic describes the procedure for installing System Availability on a Windows management console.

System Availability should be installed on the management server before installing the console components of System Availability.

Complete the following steps to install System Availability on a Windows management console:

1. Copy the downloaded installation files to a temporary directory on the machine on which you will be performing the installation.
2. Close IBM Director Console.
3. Click **Start** → **Run**.
4. In the Run dialog, type the following command in the **Open** field and press **Enter**:

```
download\dir5.10_sysavailconsole_windows.exe
```

download represents the location to which the System Availability download package was saved.

5. In the first panel of the System Availability Console InstallShield Wizard, click **Next**.
6. In the second panel of the System Availability Console InstallShield Wizard, select **I accept the terms in the license agreement**, then click **Next**.
7. In the third panel of the System Availability Console InstallShield Wizard, click **Install**. A new panel displays the installation progress.
8. When installation has completed, click **Finish**.
9. Restart IBM Director Console.

After installing the console components of the extension, you need to install the System Availability Agent components on your managed systems.

Installing the System Availability extension on a Linux console

This topic describes installation procedures for System Availability on a Linux management console.

System Availability should be installed on the management server before installing the console components of System Availability.

Note: System Availability user-interface components for IBM Director Console are automatically installed on the management server when the System

Availability server components are installed. It is not necessary or possible to separately install System Availability console components on a management server.

Complete the following steps to install System Availability on a Linux console:

1. Copy the downloaded installation files to a temporary directory on the machine on which you will be performing the installation.
2. Close IBM Director Console.
3. Change to the directory in which the installation package is located. Type the following command and press **Enter**:

```
cd /download/
```

download represents the location to which the System Availability download package was saved.

4. Type one of the following commands and press **Enter**:

Installation scenario	Command
Performing a new installation	<code>rpm -ivhSysAvailConsole-5.10-1.i386.rpm</code>
Upgrading from a previous version	<code>rpm -Uvh --relocate /opt/ibm/director=/opt/IBM/director SysAvailConsole-5.10-1.i386.rpm</code>

The installation progress is displayed.

5. Restart IBM Director Console.

After installing the console components of the extension, you need to install the System Availability Agent components on your managed systems.

Installing the System Availability extension on a managed Windows system

This topic describes the procedure for installing System Availability on a Windows managed system.

The following prerequisites apply to this installation:

- System Availability should be installed on the management server and management console before installing the agent components of System Availability on managed systems.
- IBM Director Agent should be installed on the managed system before installing System Availability.

Note: An alternative installation method is to use Update Assistant and Software Distribution. For more information, refer to the "Creating software packages to distribute" section of the *IBM Director Systems Management Guide*.

Complete the following steps to install System Availability on a Windows managed system:

1. Copy the downloaded installation files to a temporary directory on the machine on which you will be performing the installation. The downloaded installation files are contained in a zip file. Use the `unzip` command to extract the contents to a temporary directory.
2. Click **Start** → **Run**.

3. In the Run dialog, type the following command in the **Open** field and press **Enter**:
`download\setup.exe`

`download` represents the location to which the System Availability download package was unzipped.
4. In the first panel of the System Availability Agent InstallShield Wizard, click **Next**.
5. In the second panel of the System Availability Agent InstallShield Wizard, select **I accept the terms in the license agreement**, then click **Next**.
6. In the third panel of the System Availability Agent InstallShield Wizard, click **Next**. You cannot modify the installation directory; the System Availability Agent must be installed in the same location as IBM Director Agent.
7. In the fourth panel of the System Availability Agent InstallShield Wizard, click **Install**. A new panel displays the installation progress.
8. When installation has completed, click **Finish**.

Installing the System Availability extension on a managed Linux system

This topic describes installation procedures for System Availability on a Linux managed system.

The following prerequisites apply to this installation:

- System Availability should be installed on the management server and management console before installing the agent components of System Availability on managed systems.
- IBM Director Agent should be installed on the managed system before installing System Availability.

Notes:

1. System Availability agent components are automatically installed on the management server when the System Availability server components are installed. It is not necessary or possible to separately install System Availability agent components on a management server.
2. An alternative installation method is to use Update Assistant and Software Distribution. For more information, refer to the "Creating software packages to distribute" section of the *IBM Director Systems Management Guide*.

Complete the following steps to install System Availability on a Linux managed system:

1. Copy the downloaded installation files to a temporary directory on the machine on which you will be performing the installation. The downloaded installation files are contained in a tar file. Use the `tar -x` command to extract the contents to a temporary directory.
2. Stop IBM Director Agent. From a command prompt, type the following command and press **Enter**:
`/opt/ibm/director/bin/twgstop`
3. Change to the directory in which the installation package is located. Type the following command and press **Enter**:
`cd /download/`

download represents the location to which the System Availability download package was extracted.

4. Type one of the following commands and press **Enter**:

Installation scenario	Command
Performing a new installation	<code>rpm -ivhSysAvailAgent-5.10-1.i386.rpm</code>
Upgrading from a previous version	<code>rpm -Uvh --relocate /opt/ibm/director=/opt/IBM/director SysAvailAgent-5.10-1.i386.rpm</code>

The installation progress is displayed.

5. Restart IBM Director Agent. From a command prompt, type the following command and press **Enter**:
`/opt/ibm/director/bin/twgstart`

Chapter 3. Monitoring system availability

You can use the System Availability task to analyze the availability of a managed system or group. You can also use this task to view statistics about managed-system uptime and downtime through reports and graphical representations.

Viewing system availability

This topic describes how to start the System Availability task in IBM Director.

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

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

Distribution of System Outages

A pie chart representing the percentage of all system outages.

Distribution of System Uptime

A pie chart representing the percentage of all system uptime.

System Outages by Day of Week

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

System Outages by Hour of Day

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

To see the value of a specific pie chart or bar chart section, move the cursor over a specific section.

Notes:

1. (Windows operating systems that support IBM Director and are configured to adjust automatically for daylight saving time only) The event times that are specified in the system-availability report might vary by 1 hour from the event times in the Windows event viewer, because the Windows event viewer adds or subtracts one hour to adjust for daylight saving time. Because this adjustment can cause duplicate entries in the system-availability database when the time adjustment is made, System Availability does not use the daylight saving time adjustments.
2. (Linux only) On managed systems where compression of message logs is the default, turn off compression of message logs to view system-availability reports.
3. System Availability reads the message logs only if the message logs are in their default directory.
4. System Availability should run as or more often than the message logs are archived to avoid losing availability information.

The availability report is a snapshot of system availability. It provides an overall statistical summary of event and problematic details and measurements for the currently selected managed systems in a tree structure, or all managed systems if

the root of the tree is selected. Systems identified as problematic are listed in the detail section and are flagged with a red X. There are two types of reports that you can view by following these steps:

To view the availability report, click **View** → **Availability Report**.

To view a more detailed view of the availability report, right-click the graph, and then click **Detailed List of Record**.

In the System Availability window, you can detach the current view to compare and contrast different system-availability views and time frames. Click **View** → **Detach View**. The current view is separated as an independent window that does not reflect subsequent changes to the report. Closing the System Availability task closes any detached view windows.

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

Changing the graph dates

This topic describes how to specify the time period for which data is graphed in IBM Director.

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

1. In the System Availability window, click **File** → **Set Time**.
2. In the Customization of Graph Dates window, in the **Select Date Range** field, select one of the following time ranges for which you want to view data.

All Displays system-availability data from the time that System Availability was loaded on the target system up to the present day. This selection is the default.

1 week

Displays system-availability data from one previous week up to midnight of the present day.

1 month

Displays system-availability data from one previous month up to midnight of the present day.

3 months

Displays system-availability data from three previous months up to midnight of the present day.

1 year Displays system-availability data from one previous year up to midnight of the present day.

Customize

Customizes the range of time for which to display system-availability data.

Note: If you select **Customize**, type the From and To dates in the applicable fields.

3. Click **Update**.

Note: These customized settings apply only to the System Availability report that is currently open; they are not global settings applicable to all System Availability reports.

Changing the settings criteria for System Availability

This topic describes how to change the System Availability settings criteria in IBM Director.

System Availability scans for problematic systems within a range of time. The time begins a specified number of days in the past (the default is 30) and ends with the current time. The number of unplanned outages that occur in this time frame is counted, and if the total number meets or exceeds the specified count, the managed system is marked as problematic. You can also specify a percentage of time in which the managed system has unplanned outages, instead of a specific number of outages, by selecting the **Percentage** check box.

1. To specify the settings criteria, click **File** → **Settings**.
2. In the Settings window, change any of the criteria; then, click **Save**.

Note: Select **Use all available data** to evaluate all persistent data available in the IBM Director Server database.

All system-availability reports that are run after you click **Save** use the new settings.

Saving the system-availability report

This topic describes how to save the current system-availability report in IBM Director.

You can save the current report as a series of HTML files to a directory on the management console. Then, you can view the report in a Web browser at a later time. You also can save the current report in XML format.

- Complete the following steps to export and save a report in HTML format:
 1. Follow the steps in the Starting the System Availability topic to generate a system-availability report.
 2. After the report is generated, click **File** → **Export Availability Report** → **Export HTML Report**.
 3. In the “Select a directory to save report files” window, type a file name and click **Select**.
 4. In the “Confirm Directory window, click **OK**. The files are saved to the location that you specified.
 5. (Windows only) In the Open saved file window, in the **File name** field, type a file name; then, click **Select** to save the report to the specified location.
 6. (Windows only) Click **Yes** to open the exported report in a Web browser immediately.
- Complete the following steps to export and save a report in XML format:
 1. Follow the steps in the Starting the System Availability topic to generate a system-availability report.
 2. After the report is generated, click **File** → **Export Availability Report** → **Export HTML Report**.
 3. In the “Select a directory to save report files” window, type a file name and click **Select**.
 4. In the Confirm Directory window, click **OK**. The files are saved to the location that you specified.

Appendix A. System Availability window

This topic describes the System Availability window in IBM Director.

Menubar

File

Export Availability Report

Export HTML Report

Saves the current report as a series of HTML and GIF files to a directory on the console machine. Time changes and system selections made in the tree view will be reflected in the report. Detached views are not part of the exported report.

To save the graphs as GIF files, System Availability creates a temporary copy of the graph in another window. This window may appear momentarily.

System Availability prompts whether you would like to open the report now. If you select to open the report now, the default browser is launched, outside of System Availability, to show the report. System Availability provides this feature only on Windows systems

The export function prompt for a directory to place the files. Because there are multiple files produced on HTML export, the option for naming the individual files is not provided. It is recommended that you select different directories to save different reports.

Export XML Report

System Availability provides XML report export capabilities that includes all the details from the System Availability report. This is to allow other XML users to gain access to the data and provide the data in a standardized format. Validity checking is not provided. Exporting the file will overwrite any existing file located in the directory. When a file instead of a directory is chosen to export reports, the parent directory of the selected file will be the destination directory.

Set Time

Allows you to customize the Information window to display data within a defined interval. All the data will be processed for the time frame chosen for Set Time - including events starting just before or ending just after this time frame.

Settings

Displays the Settings window which allows you define preferences for problematic systems.

Only look for outages in the paste: day(s)

Indicates the number of days prior that you want to scan for problematic systems. The default is 30 days. The time frame is based off the time on the agent.

Use all available data

When the check box is selected, all the availability data reported by the agent is reviewed.

Amount of unplanned outages great or equals:

Indicates the number of unplanned outages that can occur before the system is marked as problematic. The default is 1.

Percentage

When this check box is selected the unplanned outage field changes to a percentage of time that the system can be down for an unplanned outage before the system is marked as problematic.

report stale data in: day(s)

Indicates the number of days that the system can report stale data, before marking the system as problematic.

Print Prints what is currently displayed in the work area. When you print graphs, the tool tip and detail information about the graphs is not printed. You can use **Export** to generate a hardcopy of any information that is not available through **Print**.

View**Detach View**

Detaches the current tabbed selection of the Information window. The detached information window can be moved around the desktop independently of the System Availability task or the IBM Director Console. Detached windows remain a static copy of the graph and will not be changed by changing selections on the Tree View.

Distribution of System Outages

Displays a pie chart representing the percentage of all system downtime.

Distribution of System Uptime

Displays a pie chart representing the percentage of all system uptime.

Availability Report

Provides a snapshot of system availability. It provides measurements for the currently selected systems in the Tree View (or all systems if the root of the tree is selected).

System Outages by Day of Week

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

System Outages by Hour of Day

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

Toolbars

display options

Distribution of System Outages

Displays a pie chart representing the percentage of all system downtime.

Distribution of System Uptime

Displays a pie chart representing the percentage of all system uptime.

System Outages by Day of Week

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

System Outages by Hour of Day

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

Graph icon

Displays the currently selected graph option.

Report icon

Displays the availability report.

Detach window icon

Detaches the current information window to a separate window for easy comparison with other graphs.

Fields**Tree structure**

Displays managed systems to work with.

Right pane

The information window that displays a graph or a report of system availability.

Appendix B. System Availability events

The System Availability events occur when System Availability identifies a managed system as problematic. A problematic system is one that has had too many unplanned outages over a specified period of time or a managed system that fails to report data to IBM Director Server or has availability data that is too old. When a system-availability report is generated, managed systems that meet the criteria that you specify as being problematic are flagged as such and an event is generated.

Event source

This event is generated by the System Availability Agent that is installed on a Level-2 managed system. A prerequisite for the System Availability Agent is IBM Director Agent.

Details

If you select the **System Availability** check box in the Event Filter Builder tree, the event filter will process all of the event types that are specified in the System Availability subtree.

Event type	Event text	Severity	Category	Extended attributes
System Availability	Not applicable	Not applicable	Not applicable	None

You can choose to select specific event types that are displayed under the System Availability node in the Event Filter Builder tree. The event filter will process only the event types that you select.

Event type	Event text	Severity	Category	Extended attributes
Problematic System	A problematic system has been detected.	Critical	Alert	None

Appendix C. Operating systems supported by System Availability

This topic provides information about the operating systems supported by the System Availability task.

Management-server support

This task is supported by IBM Director Server when installed on servers running the following operating systems:

- Linux on xSeries
- Windows

Managed-object support

The following tables list the operating systems that this task supports for managed objects. Managed objects can include IBM xSeries, iSeries™, System p5 and pSeries, and System z9 and zSeries hardware. Managed systems are a subset of managed objects that use different levels of IBM Director support. This task can be used on Level-2 managed systems only. These managed systems must be xSeries and Netfinity servers.

Table 1. Operating systems supported by xSeries servers

Operating system	Level 2
Editions of Windows for 32-bit systems:	
<ul style="list-style-type: none"> • Windows 2000, Advanced Server, Datacenter, Professional, and Server Editions • Windows XP Professional Edition • Windows Server 2003, Datacenter, Enterprise, Standard, and Web Editions 	Yes
Editions of Windows for 64-bit systems:	
<ul style="list-style-type: none"> • Windows Server 2003, Datacenter, Enterprise, Standard, and Web x64 Editions • Windows XP Professional x64 Edition • Windows Server 2003, Datacenter and Enterprise 64-bit Itanium Editions 	No
Versions of Linux for 32-bit systems:	
<ul style="list-style-type: none"> • Red Hat Enterprise Linux AS, ES, and WS, version 3.0 • Red Hat Enterprise Linux AS, ES, and WS, version 4.0 • SUSE LINUX Enterprise Server 8 for x86 • SUSE LINUX Enterprise Server 9 for x86 • VMware ESX Server, versions 2.1, 2.5, and 2.51, Console • VMware ESX Server, versions 2.1, 2.5, and 2.51, guest operating systems • VMware GSX Server, versions 3.1 and 3.2, Console • VMware GSX Server, versions 3.1 and 3.2, guest operating systems 	Yes
Versions of Linux for 64-bit systems:	

Table 1. Operating systems supported by xSeries servers (continued)

Operating system	Level 2
<ul style="list-style-type: none"> • Red Hat Enterprise Linux AS, ES, and WS, version 3.0, for AMD64 and EM64T • Red Hat Enterprise Linux AS, ES, and WS, version 4.0, for AMD64 and EM64T • Red Hat Enterprise Linux AS, version 3.0, for Intel Itanium • Red Hat Enterprise Linux AS, version 4.0, for Intel Itanium • SUSE LINUX Enterprise Server 8 for AMD64 • SUSE LINUX Enterprise Server 8 for Itanium Processor Family • SUSE LINUX Enterprise Server 9 for AMD64 and EM64T • SUSE LINUX Enterprise Server 9 for Itanium Processor Family 	No
Other operating systems supported by xSeries servers:	
Microsoft Virtual Server (guest operating system)	Yes
NetWare, version 6.5	No

Table 2. Operating systems supported by iSeries servers and System p5 and pSeries servers

Operating system	Level 2
<ul style="list-style-type: none"> • AIX 5L, Version 5.2 • AIX 5L, Version 5.3 • i5/OS, Version 5 Release 3 • Red Hat Enterprise Linux AS, version 3.0, for IBM POWER • Note: System p5 and pSeries servers require Red Hat Enterprise Linux AS, version 3.3 or later, for IBM POWER • Red Hat Enterprise Linux AS, version 4.0, for IBM POWER • SUSE LINUX Enterprise Server 8 for IBM POWER • SUSE LINUX Enterprise Server 9 for IBM POWER 	No

Table 3. Operating systems supported by System z9 and zSeries servers

Operating system	Level 2
<ul style="list-style-type: none"> • Red Hat Enterprise Linux AS, version 4.0, for IBM System z9, zSeries and S/390 • SUSE LINUX Enterprise Server 9 for IBM System z9, zSeries and S/390 	No

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.

Abbreviation and acronym list

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

Table 4. 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

Table 4. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
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
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

Table 4. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
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
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

Table 4. Abbreviations and acronyms used in IBM Director documentation (continued)

Abbreviation or acronym	Definition
UIM	upward integration module
UNC	universal naming convention
USB	Universal Serial Bus
UUID	universal unique identifier
VPD	vital product data
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

A

- abbreviation list 27
- acronym list 27
- availability of managed systems and groups 11

B

- BladeCenter
 - documentation ix
- books ix

C

- compatibility documents ix
- customer support ix

D

- documentation ix
- downloading ix
 - compatibility documents ix
 - hardware compatibility information ix
 - IBM Director code ix
 - IBM Director publications ix
 - systems-management software ix
- downtime, system 2, 11

E

- environment (illustration) 1
- event
 - System Availability 19

F

- files
 - HTML 13
 - XML 13

G

- glossary 31

H

- hardware
 - failure events 19
- hardware compatibility ix
- help, IBM Director resources ix
- HTML files
 - system-availability report 13

I

- IBM Director Agent
 - Linux, compression of message logs 11
- IBM Director Hardware and Software Compatibility document ix
- IBM Director windows
 - System Availability window 15
- IBM eServer Information Center ix
- IBM systems-management software
 - downloading ix
 - overview ix
- IBM Web sites
 - eServer Information Center ix
 - Redbooks ix
 - ServerProven ix
 - Support ix
 - Systems Management Software ix
 - xSeries Systems Management ix
- illustrations
 - IBM Director environment 1
- interim fixes ix

L

- legal notices 23
- log files, system 2

M

- managed systems
 - definition 1
- management server
 - definition 1
- message logs, compression 11

O

- operating system
 - compatibility ix
- outages
 - identifying system 2, 11

P

- publications ix

R

- Redbooks ix
- related information ix
- Remote Supervisor Adapter
 - documentation ix
- reports
 - frequency of outages 11
 - system
 - availability 11
 - outages 11

- reports (*continued*)
 - system (*continued*)
 - uptime 11

S

- service packs ix
- service processors
 - documentation ix
- SNMP devices
 - definition 1
- System Availability
 - changing
 - graph dates 12
 - settings criteria 13
 - comparing and contrasting views 11
 - HTML file 13
 - management server support 21
 - operating systems, supported 21
 - saving report 13
 - starting 11
 - system outages 2
 - XML file 13
- System Availability events 19

T

- tasks
 - System Availability 2, 11
- terminology
 - managed system 1
 - management server 1
 - SNMP device 1
- trademarks 24

U

- uptime, system 2, 11

W

- Web site
 - IBM Director resources ix
 - IBM Redbooks ix
 - IBM ServerProven ix
 - IBM Support ix
 - IBM Systems Management Software ix
 - IBM xSeries Systems Management ix

X

- XML files
 - system-availability report 13

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

IBM Systems
IBM Director System Availability
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Complete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to find	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to understand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Well organized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicable to your tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.



Fold and Tape

Please do not staple

Fold and Tape



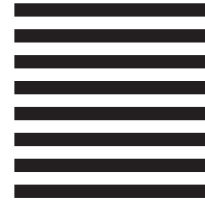
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

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



Printed in USA