Intel® Server Manager 8.40 Administrator Guide for Linux

(This page intentionally left blank.)

Table of Contents

(This page intentionally left blank.)

Introducing Intel Server Manager 8.40

Intel® Server Manager 8.40 (administrator installation)

With the growth of the computer industry, computer systems have become more complex and difficult to manage. The time spent maintaining and repairing a computer over its years of operation can increase its *Total Cost of Ownership (TCO)* far beyond the initial purchase price.

Intel Server Manager can help reduce TCO by making it easier to manage a computer and troubleshoot common computer problems. Use Intel Server Manager to:

- *View system inventory*—ISM provides extensive information about the computer's hardware and software configuration.

- *Monitor a computer's health*—ISM reports when the computer is in a warning or critical health state based on several health contributors such as temperature, voltage, free memory, and disk space.

- *Receive alerts for system events*—ISM can use various alert methods to notify you of problems.

- *Monitor real-time or historic performance*—ISM lets you monitor the performance of various system objects such as drives, processors, memory, and services. You can set alert actions to trigger notification when a specified counter crosses an upper or lower threshold a predetermined number of times.

- *Monitor current processes*—ISM lets you view current processes and statistics for each process.

- *Monitor current services*—ISM allows you to view current services and their statuses, or to set alert actions to notify you of changes to service status.

- *Remotely power off, power on, and reboot computers*—ISM enables remote power management from the administrator console for systems that support it.

- *Monitor configuration changes*—ISM can send alerts if a computer's hardware or software configuration changes. For example, you might want to know if memory is removed from a computer or if applications are added or removed. USB ports can be monitored so an alert is generated if a USB drive is accessed.

Client, server, and administrator installations

Intel Server Manager has the following modules that you can install:

- **Client**—The client installation enables an end user to view information and manage alerts for their local desktop or mobile computer. This installation allows an administrator to manage the client computer, but doesn't permit its end user to view or manage other computers.

- **Server**—The server installation enables an end user to view information and manage alerts for a local server computer. This installation allows an administrator to manage the server computer, but doesn't permit its end user to view or manage other computers.

- **Administrator**—The administrator installation enables an administrator to manage remote clients and servers on the network. This means you can view information,

generate reports, receive alerts, and power on/off other managed computers remotely. To remotely reboot, power off, or power on computers, the administrator installation must be installed on at least one computer that is attached to the network. You can manage the computers on your network from various locations by browsing to the system that hosts the administrator console using a supported browser.

Note—If you tried to run the console after installation and instead, Intel Server Manager launched this help file, you may not have a properly-configured IP address.

Running Intel Server Manager on multiple platforms

Intel Server Manager is available in versions for both Windows and Linux. Regardless of the platform on which it is installed, the administrator console can discover server computers running either Windows or Linux. An administrator console installed on a Windows platform can manage both Windows and Linux computers, but an administrator console installed on a Linux platform can manage only Linux computers. Intel Server Manager can also be viewed and run from a remote computer with a supported operating system and browser as shown in the table below.

Installation	Runs remotely in Internet Explorer on Windows	Runs remotely in Mozilla on Linux
Administrator for Windows	Yes	No
Server for Windows	Yes	No
Administrator for Linux	Yes	Yes
Server for Linux	Yes	Yes

What's new in Intel® Server Manager 8.40

New functionality in Intel Server Manager 8.40 includes:

- Support for Intel® Server Compute Blades SBXL52, SBX82, and SBX44 (managed via the Intel Chassis Management Module SBCECMM).

- Out-of-band support for Intel Carrier Grade Servers TIGPR2U and TIGPT1U.

- In-band support for the Intel® SE7230NH1-E, SE7525RP2 and SE7320EP2 Server Boards.

- Additional localization into German, Simplified Chinese, Russian, and Japanese.

- Blade chassis management modules (MMs) display as groups in the My computers list for easy management of blade servers.

- Support for Intel® EM64T platforms using SuSE Linux Enterprise 9 (Intel EM64T Edition) and Red Hat Enterprise Linux 3 Update 4 with Intel EM64T support.

Reducing total cost of ownership (TCO)

Intel Server Manager helps reduce the total cost of owning a computer by providing basic management technologies in four key areas: real-time computer health, alerting, remote computer management, and server management.
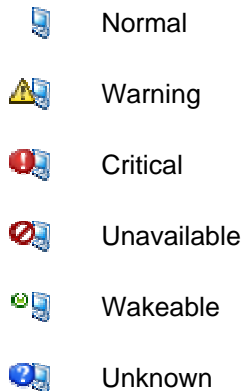
Computer health

Improper maintenance of computers can lead to emergency repairs. This tends to increase TCO by:

- Creating down time for computer users
- Creating emergency situations that require immediate attention

Use Intel Server Manager's health feature to anticipate and schedule certain maintenance tasks avoiding down time and interference with other time-sensitive work.

Intel Server Manager uses graphical icons to indicate the computer's health status. For example, the health status icons for a desktop computer are shown below:

 Normal

 Warning

 Critical

 Unavailable

 Wakeable

 Unknown

Intel Server Manager determines a computer's health by monitoring critical operating functions, such as available hard drive space, available memory, temperature, and voltage. When a health event occurs (such as low disk space), the health status changes to reflect the severity of the event. Alerts warn you of the event. A notification log also keeps track of notifications from Intel Server Manager. This early warning system can notify you of needed maintenance tasks before they become emergencies.

Alerting

Alerting plays an important role in helping to reduce TCO. The early warnings provided by Intel Server Manager enable you to resolve problems as soon as they arise, or even before they arise.

When a problem or other event occurs on a computer (for example, it's running low on disk space or the case has been opened), Intel Server Manager can notify you of the event by performing one or more *alert actions*.

Intel Server Manager can also generate alerts if a computer's hardware or software configuration changes. For example, you might want to know if memory is removed from a computer or if a certain application is installed. Or you can monitor USB ports and receive an alert if a USB drive is accessed.

Remote computer management

Intel Server Manager also helps reduce TCO by eliminating much of the travel time walking to remote computers. Depending on the layout of your network and organization, you can spend considerable time walking to computers before learning the nature of the problem or the computer's hardware and software configuration.

Intel Server Manager eliminates much of the walking around by enabling you to view detailed *system information*, create reports, and remotely reboot, power off, and power on the computer. Intel Server Manager also lets you monitor *performance* of the system.

Server management

The server module of Intel Server Manager provides support for server-specific standards and tasks, such as support for IPMI, historical and real-time performance monitoring, and remote services and processes monitoring and alerting. IPMI support lowers the total cost of ownership with automatic alerting, system shutdown and restart, and power control and asset tracking capabilities. You can see historical performance data of key server components such as memory and CPU, and you can be alerted how and when you wish when the thresholds you specify are exceeded. As an administrator, you can see what services are running on each server and determine service status.

System requirements

Note: Refer to your platform documentation to verify that the operating system versions listed below are supported on the computer you intend to install Intel Server Manager on. Some Intel Server Boards may not support the versions listed below.

Administrator computers

- Red Hat*Enterprise Linux 3 Enterprise Server Update 4 (both 32-bit and Intel EM64T Edition), Red Hat Enterprise Linux 3 Advanced Server Update 4, Red Hat Enterprise Linux 3 Workstation Update 4, SuSE*Linux Enterprise Server 9, Service Pack 1 (with Intel EM64T support)

- 512 MB RAM

- 350 MB of available hard drive space to install on Administrator computer (500 MB on the computer running Setup)

- 10-40 MB of available hard drive space to run

- A network adapter with properly configured TCP/IP
  Note: If you try to run the Intel Server Manager console after installation but it does not start (it opens this help file instead) you may have an improperly configured IP address.

- Macromedia* Flash player is required for some graphic elements to display. Adobe Acrobat* Reader is needed to view documentation. If these are not previously installed they can be downloaded as needed via an Internet connection.

- A static IP address for the computer running the Administrator console (its IP address must remain the same to ensure communication with managed computers)

- Properly configured DNS or hosts file for managing servers (please see *Getting Started with Intel Server Manager 8.40* for more information)

- Programs/RPMs--See list below

- A monitor resolution of 1024x768, 16 bit color or greater

- Telnet is required for the DPCCLI proxy server

- ftp server (required for multiple computer installation from the computer running Intel Server Manager Setup)

Note: Refer to the Getting Started with Intel Server Manager 8.40 manual for information on installing the packages, lm-sensors, and configuring the mysql and ftp users.

Red Hat Enterprise Linux 3 (32-bit Architecture)

- bash-2.05b-29
- mozilla-1.4 (1.7 preferred)
- mysql-3.23.58-2.3 (Intel Server Manager Administrator console only)
- mysql-server-3.23.58 (Intel Server Manager Administrator console only)
- net-snmp-5.0.8-11
- openssl-0.9.7a-22.1
- perl-5.8.0-88.4
- perl-CGI-2.81-88.4
- perl-DBD-MySQL-2.1021-3 (Intel Server Manager Administrator console only)
- perl-DBI-1.32-5
- perl-Filter-1.29-3
- pygtk2-1.99.16-8
- python-2.2.3-5
- sudo-1.6.7p5-1
- sysstat-4.0.7-4
- xinetd-2.3.12-2.3E
- w3c-libwww-5.4.0-5 (required for One-boot Flash Update utility)
- lm_sensors-2.9.1
- xorg-x11-deprecated-libs-6.8.2-1.FC3.13.i386.rpm

RHEL 3 ES Update 4 (Intel EM64T Edition)

- bash-2.05b-29
- mozilla-1.4 (1.7 preferred)
- mysql-3.23.58-2.3 (Intel Server Manager Administrator console only)
- mysql-server-3.23.58 (Intel Server Manager Administrator console only)
- net-snmp-5.0.8-11
- openssl-0.9.7a-22.1
- perl-5.8.0-88.4
- perl-CGI-2.81-88.4
- perl-DBD-MySQL-2.1021-3 (Intel Server Manager Administrator console only)
- perl-DBI-1.32-5
- perl-Filter-1.29-3

- pygtk2-1.99.16-8
- python-2.2.3-5
- sudo-1.6.7p5-1
- sysstat-4.0.7-4
- xinetd-2.3.12-2.3E
- lm_sensors-2.9.1
- w3c-libwww-5.4.0-5 (required for One-boot Flash Update utility)
- xorg-x11-deprecated-libs-6.8.2-1.FC3.13.i386.rpm

SuSE Enterprise Linux 9 SP1 (Intel EMT64)

- bash-2.05b-29
- mozilla-1.5 (1.7 preferred)
- mysql-client-4.0.18 (Intel Server Manager Administrator console only)
- mysql-4.0.18-32.1 (Intel Server Manager Administrator console only)
- net-snmp-5.1-80.3
- openssl-0.9.7a-22.1
- perl-5.8.0-88.4
- perl-DBD-mysql-2.9003-22.1 (Intel Server Manager Administrator console only)
- perl-DBI-1.41-28.1
- python-2.3.3
- python-gtk-2.0.0
- python-gnome-2.0.3-2
- sudo-1.6.7p5-1
- sysstat-5.0.1-35.1
- xinetd-2.3.13-39.3
- compat-gcc-32-3.2.3-47.3 & -c++-
- compat-glibc-2.3.2-95.30
- compat-libgcc-296-2.96-132.7.2
- compat-libstdc++-matching above
- mysql-shared-4.0.18-32.1 (Intel Server Manager Administrator console only)
- w3c-libwww-5.4.0-5 (required for One-boot Flash Update utility)
- xorg-x11-deprecated-libs-6.8.2-1.FC3.13.i386.rpm (required on Intel Compute Blades)
- libstdc++-3.2.3-47.i386.rpm (Disc 2 Update 4) (required on Intel Compute Blades)
- kernel source code (required for rebuilding OFU drivers)

Security in Intel Server Manager

This topic describes how security is implemented for privacy and authentication in Intel Server Manager. Three types of security are in force as the administrator console communicates with servers and clients:

- User rights as defined in Intel Server Manager user groups

- SSL encryption of data

- Digital certificates

The following sections describe security methods used for accessing the administrator console and for managing computers from the console.

Accessing the administrator console

The Intel Server Manager administrator console is accessed through a web browser, either on the same computer as the console or from another computer. To access the console, a user must log in to the OS with root privileges. (See *User rights* for more information about user groups and rights to Intel Server Manager.)

Console access is also protected by SSL encryption. A temporary web server certificate and key pair is created at the beginning of each console session. After the session is completed this certificate and its private key are erased. This certificate/key pair is used for privacy (data encryption), but not authentication.

Remote access

When accessing the administrator console from a browser on another machine, the user can install a CBA8 root authority certificate as a trusted root certification authority in their browser's certificate store. This will enable the use of an SSL connection for console access.

If the trusted authority certificate has not been installed, a warning dialog will appear when the session is started indicating that the console's certificate chain cannot be verified. At this point the user can choose to ignore the warning or can install the root authority certificate. The root authority certificate should only be installed if the browser is to be used regularly for Intel Server Manager administrative purposes. If the administration is a one-time activity, it is simpler to ignore the warning. The CBA8 root authority certificate is used to only to verify the temporary certificates of the Intel Server Manager Management Agent. To maintain the highest level of security, it should only be installed into browsers that are used regularly for Intel Server Manager administration.

Communication between the administrator console and managed computers

Security for communications between the administrator console and managed computers is supported by the following:

- The Intel Server Manager Management Agent, installed on administrator, server, and client computers, provides SSL encryption for data by serving the console UI (as a web page) and the data to be managed.

- Any browser used to access the administrator console can install a CBA8 root certificate as a trusted root certification authority in the browser's certificate store. The root authority

certificate is used to verify the Intel Server Manager Management Agent's temporary HTTPS server certificates.

- A client authentication certificate and private key is created and installed on the administrator console. The private key remains only on the admin computer. The private key must be protected and kept safe as it grants access to all managed computers. At a minimum, users should be required to log in with administrative access to obtain this key (this is the way it is installed). The private key should be safely encrypted before it is transmitted or placed on any backup medium. The certificate is distributed to each managed computer at the time it is discovered and added to the My computers list. It requires administrative access (OS authentication to an administrator's account) on the managed computers to install an administrator's certificate on it. The administrator's certificate contains no private information and can be transmitted in the clear. Once the administrator's certificate has been installed on a managed computer, the administrator console with the private key can be used to access it.

Discovery

The discovery process does not require authentication between console and managed computers. When Intel Server Manager searches for computers that can be managed, all those not already managed by the administrator are listed on the Other computers page. The administrator then selects computers to manage from this page. (Note that to manage a computer, you must have administrative-level rights on the computer's OS. You must also have the appropriate username/password credentials for IPMI servers, chassis management modules, and legacy systems running older versions of System Manager or Client Manager).

Adding computers to be managed

When a computer is added to the list of managed computers, Intel Server Manager pushes a certificate with a public key to the managed computer. This enables secure communication between the administrator console and the managed computer.

User rights

The following Intel Server Manager groups provide user rights to Intel Server Manager without providing global rights to the computer on which it is installed. Use the operating system's tools to add members to groups and manage group membership.

Ismadmin

Includes complete and unrestricted administrator rights within Intel Server Manager, but no rights outside of Intel Server Manager.

Ismpoweruser

Includes restricted administrative rights within Intel Server Manager, but no rights outside of Intel Server Manager:

- The administrator console shows the My computers and Others computers lists and the Reports features; Management and Preferences features are not available

- Log files can be viewed but cannot be cleared or resized

- In the My computers list, user can filter and refresh the list, run reports, and export data

- In the Other computers list, user can filter and refresh the list only

Ismuser

Includes read rights within Intel Server Manager, but does not include any administrative rights. Includes no rights outside of Intel Server Manager.

Intel Server Manager documentation

After you have installed Intel Server Manager, documentation is available in two formats. Choose the format that is most convenient for you. The information is the same in each format.

1. **HTML online help**—The online help (and the Intel Server Manager product) requires TCP/IP and Mozilla 1.4 or later. You can print selected topics from the online help. If you want to print all of the documentation as a book, use the pdf format listed below.

2. **Adobe Acrobat .PDF format**—This is an electronic, printable format that requires Adobe Acrobat * Reader. (The latest free version of Adobe Acrobat Reader can be downloaded from *http://www.adobe.com.*) If Adobe Acrobat Reader is installed, you can access the guide from /usr/Intel/ism/wwwroot/help/admin/en/ismguide.pdf.

(This page intentionally left blank.)

Managing computers

Using the toolbar

On the administrator console's My computers and Other computers pages, toolbar icons give you quick access to Intel Server Manager features.

My computers page

Icon	Description
	Creates groups of managed computers to help you organize the systems.
	Assigns custom attributes to managed computers.
	Filters a list of computers by name, status, type, hardware, and/or custom attributes.
	Refreshes the list of managed computers with a new "snapshot" of computer status.
	Removes the selected computer(s) or group(s) from the list of managed computers.
	Generates predefined reports from inventory data.
	Exports inventory information in .XML format for the selected computer(s).
	Initiates power options (power off, power on, reboot) on selected computers.
	Configures IPMI settings for watchdog timers and the hardware events log on IPMI-compliant servers.
	Opens the manufacturer's *web interface* for a blade server chassis management module.

Other computers page

Icon Description

Discovers computers on the specified network.

Adds computers to the My computers list so they can be managed.

Filters a list of computers by name, status, computer type, or custom attributes.

Clears the Other computers list.

Refreshes the list of unmanaged computers with a new "snapshot" of computers on the network.

Discovering new computers

The first time you open the Intel Server Manager administrator version, it performs a discovery of the computers on your local subnet that are running Intel Server Manager, and populates them in the Other computers list. *Automatic discovery* updates the Other computers list periodically, but as computers are added and removed from the network, there may be periods of time when the list is outdated. You can manually perform a new discovery at any time to update the Other computers list. You must *add* newly discovered computers to the My computers list before you can manage them.

Notes:

- Because the discovery process makes multiple passes to gather information, the number of computers on the Other computers list may continue to increase for a few minutes after the initial discovery results appear.

- The number of computers that is practical to discover and display depends on network bandwidth and the administrator computer's OS and available memory. We recommend no more than 1000 computers per administrator console.

To discover new computers

1. From the main Intel Server Manager page, click **Other computers**.

2. Click on the toolbar.

3. Select **Saved addresses** or **IP address range**, then specify the required information.

4. Click **Discover**.

Depending on the size of the network, discovery may take several minutes and continues in the background. All computers will not be displayed until discovery has been completed. If you click

on the toolbar during discovery, only those computers that have been discovered will be displayed.

To save an address range to the Saved addresses list

1. From the main Intel Server Manager page, click **Other computers**.

2. Click on the toolbar.

3. Select **IP address range**, then type a range of from one to 254 computers, such as From: 192.125.125.1 To: 192.125.125.254.

4. Click **Save** to save the address or address range to the Saved addresses list box.

To delete an address range from the Saved addresses list

1. From the main Intel Server Manager page, click **Other computers**.

2. Click on the toolbar.

3. In the **Saved addresses** list box, select the network address you want to remove from the list. (Press the Ctrl key while selecting to delete multiple addresses.)

4. Click **Delete** to delete the address.

Note—This action only removes addresses from the Saved addresses list. It does not delete computers from the My computers list. To delete computers from the My computers list, select them in the My computers list and click .

Adding computers to manage

Before you can manage a computer, you must take "ownership" of it by adding it to the My computers list. When you add an in-band computer and supply proper login credentials for it, Intel Server Manager creates a certificate on the managed computer to identify it as being managed by you. The computer then appears in the My computers list.

When you remove a computer from the My computers list, it is released from your management and can be managed by another administrator.

Adding IPMI-enabled computers

When adding IPMI-enabled computers, you need to enter both the OS credentials and the IPMI password. Check and fill in an IPMI user name only if a third-party application has already configured the selected IPMI-enabled systems—otherwise, leave it blank and Intel Server Manager will use the BMC's default user account.

Adding legacy clients

If you have computers running legacy clients (older versions of Intel Server Manager), you can manage them if you have enabled the Legacy support option (either during installation or from the *Legacy support preferences* page). When you add legacy computers to be managed you must provide the administrator password for legacy management. If you select computers with both legacy and current versions of Intel Server Manager, you are allowed to add only the computers with the current version. You can then select the legacy computers separately and add them to be managed.

Adding blade servers and chassis management modules

When you add blade servers in a chassis management module (MM), some details of the process are different. You can only add the MM, not individual blade servers. No certificate is created on the MM when you add it to the My computers list. When added, the MM appears as a group in the My computers list, and individual blades are listed in the group as well as the MM. (Note that the process of adding an MM may take longer than when you add a single computer.) This is a special type of dynamic group that is not editable in the way normal groups are. In the group, individual blades are listed by bay number in the chassis and the name of the blade server.

To select and add computers from the Other computers list

1. Click **Other computers** to display the list of discovered computers that are not managed by you. (If you do not see a computer that you want to manage, you may need to *discover computers* on the network to display a current list of available computers.)

2. Select the computer you want to manage. You can select multiple computers provided they all use the same OS user name and password (and IPMI credentials, if selecting IPMI-enabled systems).

3. Click on the toolbar.

4. Click **Selected computers in list**, then click **Add**.

5. Enter the required credentials for the computer(s) you want to manage.

6. Click **Add**.

To add a specific computer by name or address

1. Click **Other computers**.

2. Click on the toolbar.

3. Click **Computer name or IP address**, then type the computer name or IP address.

4. Click **Add**.

5. Enter the required credentials for the computer you want to manage.

6. Click **Add**.

Note: You cannot use this method to add a blade chassis management module (MM). You must find the MM in the Other computers list and add it using the steps outlined above.

To add a serially-managed IPMI computer for out-of-band management

The option to add a serially-managed computer appears only if you have checked the **Enable serial management of out-of-band IPMI servers** option on the *Discovery preferences* page.

1. Click **Other computers**.

2. Click on the toolbar.

3. Click the option for adding serial managed computers.

4. Specify port, baud control, flow, and phone number (if necessary).

5. Click **Add**.

6. Enter the required credentials for the computer you want to manage.

7. Click **Add**.

To remove computers or groups from the My computers list

1. Select the computer(s) or group(s) you want to remove.

2. Click on the toolbar.

Selecting a computer to manage

The My computers page features a list of the Intel Server Manager computers and *groups* you manage and a *toolbar* for managing them. You must *add computers* to the list before you can manage them. After you have added computers to the list, each time you open the My computers page, Intel Server Manager retrieves information about the computers you manage. To manage specific computers, you can *select them* from the list. By default, the My computers list includes the following information about each computer:

- An *icon* indicating whether it is a server, desktop, mobile computer, blade, or blade chassis.

- **Computer name**—The name of the computer on the network (or "IPMI" if the computer is an out-of-band IPMI computer that has never been discovered in band).

- **Status**—The health and availability *status* of the computer. This can be Normal, Warning, Critical, Unknown, Unavailable, or Wakeable.

- **Product version**—The version of Intel Server Manager that the computer is running, or "Out of band" if the computer is IPMI-enabled and out of band.

- **Type**—The type of installation on the computer (server, desktop, mobile, IPMI-enabled system, etc.).

- **Address**—The computer address and IP address.

- **Operating System** and **OS version**—The operating system name and version.

You can sort the My computers list by clicking the column heading for the category you want to sort by, and can define *custom column headings and sortable attributes*.

To select a computer to manage

1. In the **My computers** list, click the computer you want to manage.

2. Type the user name and password to access that computer.

Understanding computer status icons

On the My computers page, each computer in the list displays an icon indicating its current status. The table below shows each icon and describes the six possible states for the computer.

Desk-top	Ser-ver	Lap-top	Blade	Blade Chassis	Description
					Unavailable—ISM is unable to communicate with the computer. This can occur when there are network issues or when the computer is in a powered off state, has been disconnected from the network, or had the ISM software removed. Unavailable computers remain in the My computers list until they are manually deleted.
					Wakeable—The computer is currently powered-off but supports remote wake-up technology such as *Wake on LAN*.
					Normal—The computer is operating normally.
					Warning—A component on the computer has exceeded a warning threshold. For example, if a hard disk is running low on available space, ISM displays a warning icon. Some health contributors (such as disk space and memory) have thresholds that you can set.
					Critical—A component on the computer has exceeded a critical threshold. For example, if the hard disk is running critically low on available space, ISM displays a Critical icon. Some health contributors (such as disk space and memory) have thresholds that you can set.
					Unknown—ISM is able to communicate with the computer, but the health status (such as normal, warning, or critical) is not known or is in the process of being obtained.

Notes:

- Each group in the My computers list also displays an icon indicating its status.

- The Wakeable status only occurs for computers that support remote wake-up technology and have been manually configured to display a status of Wakeable when powered off. Unless specifically configured to *display the Wakeable status*, computers that are powered off display a status of Unavailable or, for IPMI-enabled computers, show out-of-band status information.

Using groups

Intel Server Manager can organize computers in groups for easier management.

There are two types of groups:

- **Static groups** are composed of computers that you have added manually to the group. They remain in the group until they are removed or until you no longer manage them.

- **Dynamic groups** are composed of computers that meet one or more criteria. For example, a group may contain all computers that are currently in a Warning state. They remain in the group as long as they match the criteria defined for the group.

By default, Intel Server Manager has the following groups:

- **Serial IPMI devices** contains IPMI computers that can be managed over a serial connection. This group appears in the My computers list if *Enable serial management of out-of-band IPMI servers* is checked on the Discovery preferences page.

When a blade chassis management module (MM) is displayed in the My computers list, it appears as a group but cannot be edited. The group lists the MM and the blade bays in the chassis, with the names of individual blade servers in the bays. The blade servers are also listed individually in the My computers list as well as in the MM group.

To create or edit a static group

1. Click ![icon] on the toolbar.
2. Click **Static groups**.
3. To create a new group, type a name for the new group and click **Create**. If you have selected computers before doing this, click **OK** to add the selected computers to the group.
4. To rename a group, select the group from the **Rename** drop-down list and click **Rename**.
5. To add computers to a group, select the group from the **Add selected item(s) to group** drop-down list. Select the computers from the list (hold down **Ctrl** to select multiple computers), then click **Add**.

To create or edit a dynamic group

1. Click ![icon] on the toolbar.
2. Click **Dynamic groups**.
3. To create a new group, type a name for the new group and click **Create**.
4. To edit a group (including a group you have just created), select the group from the **Edit** drop-down list.
5. Select the criteria you want to use (Name, Status, Type, Hardware, and any custom attributes) from the Criteria drop-down list and click **Add new criteria**. You can specify multiple criteria by repeating this step for each criteria you want to add.
6. Set the required parameters for the specified criteria by typing in the text box or selecting check boxes.
7. Click **Save**.

Examples

- To select computers by name, select **Name**, click **Add**, then type a partial name with a wildcard, such as *serv**.
- To select computers by name and health, select **Name** and click **Add**, then select **Status** and click **Add**. Type in a partial name with a wildcard, such as *serv**, then select one or more Status options. Servers matching the name pattern that report the same health status you specified will be included in the group.

Applying custom attributes

You can *define columns and custom attributes* and apply them to the computers you manage. This allows you to sort computers by location, owner, or any other defining attribute that is useful to you. You must first define the column(s) and custom attributes you want to use, and then you can assign them to the computers to which they apply.

To assign a custom attribute

1. From the My computers list, select the computer(s) to which you want to assign a custom attribute you have defined. For example, if you've created a location column and custom attributes for the various floors in your building, you might select all of the computers located on the fourth floor.

2. Click on the toolbar.

3. From the drop-down list next to the appropriate column heading, select the attribute you want to apply to the computer(s) you've selected. If there are no column names and custom attributes from which to select, you need to define them from the *Computer lists preferences* page

4. Click **Apply**.

After you have applied custom attributes to the computers in the list, you can sort by those attributes by clicking on the appropriate column heading.

Filtering the display list

The My computers page and the Other computers page have a filter icon you can use to determine which computers appear in the list. You can filter by only one of the criteria (which may include name, status, servers, computer type, or custom attributes), or you can combine the criteria to focus on a subset of computers.

To filter the display list

1. Click on the toolbar.

2. Select the criteria you want to filter by and click **Add new criteria**.

3. Set the parameters of the specified criteria by typing in the text box and selecting checkboxes. If you filter by computer name, type the network computer name or range of computer names. You can enter wildcard characters to find certain computer names (such as serv*).

4. Click **Filter**.

5. Click to view your filtered results.

Examples

- To find a computer by name, select **Name**, click **Add**, then type in a name or partial name and a wildcard such as *server-16* or *serv**.

- In the My computers page, to find computers by partial name and health, select **Name** and click **Add**, then select **Status** and click **Add**. Type in a name or partial name such as *serv**, then select one or more Status options. (Typing in a full name will only display that computer if it reports the same health status you specified. For example, if you specified *server-16* and clicked *Critical*, the computer *server-16* will not appear in the list if it reports an OK health status to the console.)

To remove a filter and show all computers

1. Click on the toolbar to open the Filter computers view.
2. Click **Show all**.

Refreshing the computer list

Data about the computers you manage is updated periodically as Intel Server Manager takes "snapshots" of your network by performing periodic automatic discovery operations. (You can change the frequency of these background discoveries from the *Discovery preferences* page.) You can refresh the My computers list to display the computer's properties and health status as reported in the most recent snapshot.

If an IPMI-enabled system is out of band at the time of the snapshot, the health status will not reflect all health contributors for the system, but it will represent a limited number of health contributors that can be monitored by the out-of-band server's BMC.

See *Monitoring health* for information on selecting the items that contribute to the system health status.

To refresh the computer list

When you perform any of the following actions, the computer list is refreshed:

- From any page, click **My computers**.

- From the My computers page, click **Refresh** or **Delete** (if you are removing a computer from the list) on the toolbar.

- From the Other computers page, click **Refresh** on the toolbar, or click **Discovery** or **Add computers** and complete the related action.

Removing a computer from the list

The Delete button on the toolbar removes computers from the list of managed computers displayed on the My computers page. You may choose to remove a computer if another administrator will manage the computer. In addition, when you remove a computer from the network, the name of that computer is not automatically removed from the My computers list and you should delete it.

If you remove a computer from your My computers list and the computer remains on the network without being managed by another administrator, that computer may appear on the Other computers list the next time you discover computers on the network.

To remove a computer from the list

1. From the main Intel Server Manager page, click **My computers**.

2. Select the computer(s) you want to remove from the list. (Use the Ctrl and Shift keys to select multiple computers.)

3. Click ✖ on the toolbar.

Using power options

Use power options to manipulate the power state of selected computers from the administrative console. This includes powering on, powering off, and rebooting computers. When powering on or rebooting an IPMI-enabled computer, you can view that computer's boot display in a console window.

- *Rebooting or powering off a computer*

- *Powering on a computer*

- *Configuring your routers for Wake on LAN technology*

- *Viewing a console redirection window*

To use power options

1. Click **My computers**.

2. Select computer(s).

3. Click ⏻ on the toolbar.

4. Select from the following options:

    - 🖼 Reboot the selected computers

    - 🖼 Power off the selected computers

    - 🖼 Power on the selected computers

5. Click **OK**.

Rebooting or powering off a computer

There may be times when you want to remotely power off computers on the network. For example, if there is a general power outage and computers are running on UPS power, you can use the Intel Server Manager administrator to power them off gracefully before the UPS batteries fail. You can then power them back on when power is restored.

After making changes to a computer on the network, you may need to reboot the computer for changes to take effect. Using Intel Server Manager administrator, you can remotely reboot computers.

Note:

- Intel Server Manager will not power off or reboot the administrator computer. Attempting to power off or reboot the administrator computer will result in an error message.

- When you power off or reboot an IPMI server that is *out of band*, the OS does not shut down gracefully. For an out-of-band BMC you can only turn the power off or initiate a power cycle.

- The *watchdog timer* is not enabled by default for IPMI-enabled systems. Because the watchdog timer can initiate a power cycle in the event that a server hangs during remote power down or reboot, it is highly recommended that you enable the watchdog timer for any IPMI-enabled systems you may need to remotely power down or reboot.

Powering on a computer

Intel Server Manager can remotely power on a computer. For this feature to work, your remote computers must use network adapters that support remote wake-up technology, such as a BMC with IPMI capabilities or a chassis management module. On non-IPMI computers, support for *Wake on LAN* capabilities is required.

Non-IPMI computers may have remote wake-up disabled in the *BIOS* by default. You may need to enable this option in system Setup on remote computers before Intel Server Manager can power on these computers.

Wakeable computers to display a Wakeable icon in the My computers page when powered off, instead of the standard Unavailable icon . This helps you know which computers you can wake up with Intel Server Manager.

Configuring your routers for Wake on LAN technology

If your network subnets are connected with routers, ensure that the routers are configured to handle the directed IP broadcasts that Wake on LAN uses. Otherwise, Intel Server Manager's power-on feature will not work. For more information, review your router documentation or *System requirements.*

Viewing a console redirection window

When powering on or rebooting a managed IPMI server from the administrator console, you can open a console redirection window that displays the server's boot information. This can be useful if you want to verify that the server is rebooting. You can also use the console window to pause the boot process and change BIOS settings on the managed server.

To view a console redirection window, the server must have Console redirection over serial port enabled in its BIOS setup. The console data is sent to the serial port. If there is a serial cable connecting the server and the administrator console, the console redirection is carried over that cable. If not, Intel Server Manager initiates a serial over LAN (SOL) connection to redirect the data from the serial port to the LAN connection. The SOL connection stays open as long as the console window is open. When the console data has finished displaying you should close the window.

To open a console redirection window

1. Select the server from the **My computers** list.

2. Click on the toolbar.

3. Check **Show console redirection window**.

4. Click **Reboot the selected computers** or **Power on the selected computers**.

Notes:

- A console window opens and a second message window opens. You can close the message window.

- After the console redirection window opens but before the console displays the boot sequence, you may see random characters in the window. These appear because the server's BMC is sending heartbeat messages, which are transmitted on the connection to the administrator console. The characters do not display while the console shows the boot display, but may reappear after the boot process has completed.

Configuring IPMI settings

Use the Configure IPMI page to apply watchdog timer and hardware event settings on servers that are IPMI-enabled. While you can configure IPMI settings on individual servers, this page allows you to configure these settings for one or more servers.

Watchdog timer settings

A server's BMC (baseboard management controller) contains a watchdog timer feature that indicates when the server is hung or unresponsive. This timer can be set to expire periodically and will initiate an action if it expires (such as power cycling). Intel Server Manager is configured to reset the timer periodically so it does not expire; if the computer becomes unavailable (for example, it is powered down or hangs), Intel Server Manager cannot reset the timer and it then expires, which initiates the action.

You can specify how much time to allow before the timer expires and select an action to perform if it does expire.

Note: You can only configure watchdog timer settings on in-band servers or servers with the WinBridge agent.

To change watchdog timer settings

1. Select the computers you want to apply the setting to.

2. Click ⬛ on the **My computers** toolbar.

3. Check **Turn on the watchdog timer** to enable the timer.

4. Specify the frequency of checking the timer (number of minutes or seconds).

5. Select an action to initiate when the watchdog timer expires.

6. Click **Apply**.

Hardware events

A server's BMC stores system event information as log entries in non-volatile memory on the BMC. Because event data is not purged from the log, when the SEL reaches its storage limit, no new entries will be created as new system events are generated. It can be useful to either clear the log or copy the data to another location before the storage is full.

The Hardware events options let you clear the BMC event log or set up an automatic backup of the data for selected computers. When backup is turned on, Intel Server Manager checks the log periodically to determine how much memory has been filled with events. When the log fills a certain percentage of memory, it is backed up to the database on the administrator computer and the memory is cleared. Backed up data is stored in the AutoSELBackup table of the administrator database.

Notes:

- You can only configure hardware events log settings for in-band servers.

- If the administrator is not on when the server needs to back up, the server computer will hold the information and send it when the administrator is powered on.

- The backup process saves only information that is contained in the SEL. Anything cleared from the SEL before backup will not be saved.

To clear the hardware event log

1. In the **My computers** list, select one or more computers.

2. Click   on the toolbar.

3. Click **Clear**, then click **OK**.

To back up the hardware event log

1. In the **My computers** list, select one or more computers.

2. Click   on the toolbar.

3. Check **Turn on hardware event backup**.

4. Select the number of hours between checks.

5. Select the percentage of memory for backing up the log.

6. Click **Apply**.

Managing computers from any browser

You can manage and view information about Intel Server Manager computers using a browser on any computer on your network (even if that computer doesn't have Intel Server Manager administrator installed). To do this,

- The remote computer must have the Intel Server Manager server software installed on it.

- The remote computer must be powered on and connected to the network.

- You must use a valid user account on the remote computer.

- You must use a *supported browser*.

Connecting to a remote computer in this manner lets you view system information and set alerts and thresholds. It does not let you transfer files, power on/off, or reboot the computer. To perform these functions, you can connect to an administrator computer and use it to manage and power on/off the remote computer. (This requires valid accounts on both the remote computer and remote administrator computer.)

To connect to a computer from a browser on the network

1. Open a supported browser.

2. In the Address window, type:

    `https://[computer name]:9593/ism/index2.cgi`

For example, https://server-cl:9593/ism/index2.cgi. If you're using a *proxy server* to access the Internet, you may need to enter the full domain name (such as https://server-cl.mycompany.com:9593/ism/index2.cgi).

9593 is the port number your browser uses to access Intel Server Manager.

If you receive an error message stating that your browser cannot open the Internet site, either the computer name or port information is incorrect.

If you receive an error message "404 NOT FOUND -- The requested object was not found on this server," you may have mistyped the **index2.cgi** portion of the address or there may be a problem with the remote installation of Intel Server Manager.

To connect to an administrator computer from a browser on the network

Using Internet Explorer on a computer that is running Windows, you can connect to administrator machines that are running either Windows or Linux. (Note that the computer from which you connect must meet the system requirement for an administrator computer. These include supported a version of Windows 2000, XP, or 2003 Server; Internet Explorer 6.x SP1 or later; Macromedia Flash; Microsoft Data Access Components (MDAC) 2.8; and a screen resolution of 1024x768 or greater. See *System requirements* for details.)

Using Mozilla on a Linux machine, you can connect only to administrator machines that are also running Linux.

1. Open a supported browser.

2. In the Address window, type:

    `https://[computer name]:9593/ism/index2.cgi?ADMIN=1`

    For example, https://sysmanager-admin.mycompany.com:9593/ism/index2.cgi?ADMIN=1.

Managing a computer that uses an older Client Manager version

The Intel Server Manager 8.40 administrator can manage computers running Intel Server Manager 8.0 and later. The My computers page displays the Intel Server Manager version in the LSM version column.

Managing system inventory

Computer summary

Intel Server Manager instantly displays the overall health of the computer with an icon:

Normal

Critical

Warning

The summary page also displays information about the computer. Items displayed may vary depending on the type of computer and the technologies supported on the computer.

- **Computer name**—The fully qualified domain name assigned to the computer.
- **Manufacturer**—The manufacturer of the computer.
- **Model**—The model number of the computer.
- **Version**—The version number of the computer.
- **Asset number**—The asset tracking number assigned to the computer. This number is sometimes assigned by the computer's manufacturer and stored in the computer's BIOS. This information is taken from the BIOS, and cannot be changed. If the field is blank, click **Asset number** and type an asset number.
- **Serial number**—The serial number of the computer.
- **BIOS version**—The version of the BIOS installed on the computer's motherboard.
- **Operating system**—The operating system currently running.
- **Version**—The operating system version, build number, and service pack release number.
- **CPU**—The type of processor installed on the motherboard.
- **Total available physical memory**—The memory capacity of the system (not including virtual memory).
- **Total hard drive space**—The size of the installed hard disk, reported in megabytes.
- **Total free hard drive space**—The amount of available hard disk space, reported in megabytes or gigabytes.
- **TCP/IP address**—The address assigned to the computer for communicating on TCP/IP networks.

For IPMI systems only, the following information is displayed:

- **Hardware platform**—Description of the platform (such as IPMI).
- **IPMI version**—The version number of IPMI.
- **IPMI SDR version**—The version number of the SDR (sensor data record).
- **BMC firmware revision**—The revision number of BMC firmware.

- **ACPI power supply**—Information about ACPI-compliant power supplies is displayed when a server is out of band.

For blade chassis and blades, the following additional information is displayed:

- **Part number**—The part number of the component.

- **FRU number**—The identifying number if the component is a field replaceable unit.

- **FRU serial number**—The serial number if the component is a field replaceable unit.

- **Manufacture date**—The date of manufacture of the component.

- **Hardware revision**—The revision number of the component.

- **Type**—The identifying type of blade chassis.

- **Firmware summary—**In a box at the bottom of the summary information, details about various types of firmware are listed, including the firmware's build ID, date released, and revision number.

To open the summary page after viewing other information

- Click **[*computer name*] summary** at the top of the left pane.

Viewing system data

Intel Server Manager can display information about the hardware and software components on the computers you manage. You can access this information with these methods:

- View all system data for a single computer

- *Export all system data* for a single computer or for selected computers

- *Use predefined system reports* to view selected system data for selected computers

Server system data

The following list describes the information generally available for Intel Server Manager server systems.

Note: Some components may not be available for some computers, depending on the computer's motherboard, Operating System, and the manufacturer's configuration of Intel Server Manager.

- *Computer summary*—Displays a summary of the computer's hardware and software information.

- *Asset management*—Displays information about the computer's user, such as name, phone number, department, location, and position. Users with administrator rights on a computer can enter and modify this information. The computer name and an asset number may also be available.

- *BIOS*—Displays the *BIOS* manufacturer, version, date, and serial number; BIOS event log data; and allows alert configuration for POST error detection.

- *CPU*—Displays processor, speed, socket, and cache information; allows alert configuration for CPU changes.

- *Display*—Displays information about the video adapter.

- **Drives**—Displays the computer's available and used disk space, and the configured thresholds that trigger alerts if disk space is running low. The partition, *file system*, cylinder, and sector information is also provided for each hard drive, as well as serial number and *S.M.A.R.T.* information, if applicable. Allows alert configuration for drive changes, drive space, and drive failure prediction.

- **Fans**—Displays status of cooling fans installed in the computer; allows alert configuration for fans.

- **Field replaceable units**—Displays modules or components of an IPMI system which can be replaced in its entirety as part of a field service repair operation.

- **Installed applications**—Displays a list of applications installed on the computer with version, date, filename, size, and path information. Allows alert configuration for applications being added or removed.

- **Keyboard and mouse**—Displays the type of keyboard and mouse attached to the computer.

- **Memory**—Displays the computer's available and used memory (physical and virtual), sockets, and the configured thresholds that trigger alerts if memory is running low. Allows alert configuration for ECC error detection, virtual memory, and changes to memory modules.

- **Motherboard**—Displays motherboard manufacturer, model, and serial number, as well as *system slot* information.

- **Multimedia**—Displays information about the computer's multimedia devices.

- **Network**—Displays information about the computer's network adapters and drivers, *IP address* configuration, data statistics, and network connections. Allows alert configuration for addition or removal of NICs.

- **Operating system**—Displays operating system name, startup time, locale, version, and kernel.

- **Performance**—Displays current thresholds for specific parts of the system; lets you modify thresholds and select performance counters to monitor; allows alert configuration for performance.

- **Ports**—Displays the port name, *IRQ*, *I/O address*, and other information for the computer's *parallel* and *serial ports*.

- **Power supplies**—Displays the name and status of each power supply on the system.

- **Processes**—Displays a list of processes running on the system, and lets you terminate most processes.

- **Sensors**—Displays data for discrete and numeric sensors on IPMI systems.

- **Services**—Displays a list of services running on the system, and lets you select a service to generate an event should the service's status change. Also allows alert configuration.

- **Storage Devices**—Displays a list of storage devices on the system, including disk drives, tape drives, RAID arrays, DAT drives, etc.

- **Temperatures**—Displays a list of temperatures for key components of the system, and allows alert configuration for temperatures.

- **Users and groups**—Displays users and groups and their properties.

- **Voltages**—Displays a list of voltages for electrical components of the system, and allows alert configuration for voltages.

Blade and blade chassis data

The following list describes the information generally available for Intel Server Manager blade and blade chassis systems. Some components listed here may not be available for some systems, depending on the manufacturer's configuration.

- *Blade slots*—Lists the slots in a chassis and names of blades in the slots.

- **Blowers**—Displays status of blowers in blade chassis systems.

- **I/O modules**—Lists information about the I/O modules in a blade chassis.

- *Management modules*—Lists information about the management modules in a blade chassis.

- *Power domains*—Lists information about the power domains in a blade chassis.

- *Power modules*—Lists information about the power modules in a blade chassis.

- *Temperatures*—Displays a list of temperatures for key components of the blade or chassis.

- *Voltages*—Displays a list of voltages for electrical components of the blade or chassis.

To view system data

- In the left pane, click **System**, then click any of the items.

Asset management

Intel Server Manager enables you to manage and view the following user and asset information for the computer.

Contact

Contact information can be modified by a user with administrative rights.

- **Name**—The primary user's name.

- **Position**—The primary user's job position.

- **Phone number**—The primary user's phone number.

- **Location**—The primary user's location in the building.

- **Department**—The primary user's department.

System

- **Computer name**—The computer or host name.

- **Manufacturer—**The name of the company who made the computer.

- **Model**—The model number of the computer.

- **Serial number**—A serial number assigned to the motherboard by its manufacturer.

- **Asset number**—The asset tracking number assigned to the computer. This is sometimes assigned by the computer's manufacturer and stored in the computer's *BIOS*. If it is not in the BIOS, this number can be added by a user with administrative rights.

To view and edit asset information

1. Click **System**, then click **Asset management**.

2. Type new information in any edit box.

3. Click **Apply**.

Note—The asset information fields can only be edited if you are logged in with root privileges.

Management module web interface

Intel Server Manager lets you directly access the HTML user interface that is provided by the Intel Server Management Module SBCECMM to the Intel Blade Server Chassis SBCE. This interface displays detailed information about the chassis and lets you configure the chassis. Consult the *Intel® Server Management Module SBCECMM Installation and User's Guide* for details on using this interface.

To access the web interface for a blade chassis

1. Click **Utilities**, then click **Blade chassis web interface**.

Blade servers

Intel Server Manager displays information about servers and available bays in a blade chassis. This information includes:

- The numbers of the bays

- The name assigned to the blade server in the bay

- A power state value indicating whether the blade is powered on or off

To view blade server information for a blade chassis

1. Click **Blade chassis**, then click **Blade servers**.

BIOS

Intel Server Manager displays the following *BIOS* information for the computer:

- **Manufacturer**—The manufacturer of the BIOS installed on the motherboard.

- **Date**—The date of the BIOS installed on the motherboard.

- **Version**—The version of the BIOS installed on the motherboard.

- **Serial number**—The serial number of the BIOS installed on the motherboard.

You can also use this page to set alert actions for POST (power-on self test) errors that may occur when a computer boots. You can also view the BIOS event log.

BIOS event log

The log displays a list of events affecting the BIOS, including the date the event occurred and a description of the event.

To view BIOS information

- Click **System**, then click **BIOS**.

To set alert actions for POST errors

1. Click **Configure alert actions: POST error detection**.

2. Click the types of alerts you want to send and click **Apply**.

3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Chassis

Use Chassis to view whether the chassis of a computer is open or closed (supported on IPMI and some other systems). You can also turn on or off the LED indicator on an IPMI-enabled server. Turning the LED indicator on is helpful in identifying a machine among a row or rack of systems. You can also turn on the LED indicators of out-of-band IPMI computers from the administrator console.

Note: To view all available IPMI inventory information, you need SMBIOS 2.3.1 or higher.

To view chassis information

1. In the left pane, click **System**, then click **Chassis**.

To turn on the system identify LED

1. Specify the number of minutes you would like the LED turned on or off.

2. Click **On**.

To set alert actions for Chassis

1. Click **Management**, then click **Alerts**.

2. Click **Chassis** for non-IPMI enabled computers.

   or

   Click **Physical security/chassis intrusion** for IPMI-enabled computers.

3. Click the tab of the status type (OK or Warning) you want to set alerts for.

4. Click the types of alerts you want to send and click **Apply**.

5. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

CPU

ISM displays the following processor information for the computer:

CPU

- **Name**—The type of processor installed on the motherboard.

- **Description**—A specific description of the CPU.

- **Vendor ID**—A unique ID assigned to the processor which identifies its manufacturer.

- **Current speed**—The speed (measured in megahertz or gigahertz) at which the processor is currently running.

- **Maximum speed**—The maximum speed at which the CPU can run.

- **Bus speed**—The speed (in megahertz) of the bus.

- **Number of CPUs**—The number of installed physical microprocessors.

- **Number of logical CPUs**—The number of installed logical microprocessors.

Cache

- **Type**—Indicates whether the cache is internal (*primary*) or external (*secondary*) to the microprocessor.

- **Size**—The size of memory cache (measured in kilobytes) available to the processor.

- **Write policy**—The type of memory cache used, such as *write through* or *write back*.

To view processor information

- Click **System**, then click **CPU**.

To set alert actions for CPU

1. Click **Configure alert actions: CPU changes**.
2. Click the types of alerts you want to send and click **Apply**.
3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Display

Use Display to view video display information.

To view display information

- Click **System**, then click **Display**.

Drives

You can use Intel Server Manager to:
- Configure alert actions for drive space and drive changes.

- Set warning and critical thresholds for disc space alerts.

- View information about the computer's drives.

As an administrator, you can also set global thresholds that apply to the drives of all computers running Intel Server Manager. See *Using alerts* for more information.

To view drive information

- Click **System**, then click **Drives**.

To configure alert actions for disk space or disk drive changes

1. Click the alert you want to configure.

2. Click the tab of the status type (Critical, Warning, OK, and Informational) you want to set alerts for.

3. Click the types of alerts you want to send and click **Apply**.

4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

To set drive space thresholds

1. Click the drive for which you want to set thresholds.

2. Drag the colored arrows on the indicator bar or type Warning and Critical percent values in the appropriate boxes.

3. Click **Apply.**

Notes

- Used and available disk space are not updated dynamically. You can refresh them by clicking Apply or Refresh.

- You must have Macromedia* Flash installed to view the thresholds bar. You can download the Flash player at *www.macromedia.com.*

Fans

Intel Server Manager can monitor the speed for cooling fans installed in the computer if the motherboard and fans support this feature. These can include:

- Processor fans for each microprocessor installed on the motherboard

- Rear chassis fans

- Front chassis fans

- Other fans included by the computer's manufacturer

Note—Fan information will only appear if you have configured sensors.

To view fans information

- Click **System**, then click **Fans**.

Note: Fan information is not updated dynamically. You can update it by refreshing the browser window view or by clicking Fans.

To set alert actions for fan problems

1. Click **Configure alert actions: Fans**.
2. Click the tab of the status type (OK or Critical) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Field replaceable units

Intel Server Manager displays information about field replaceable units (FRUs) on managed IPMI-enabled computers.

A field replaceable unit is a module or component of the system which can be replaced in its entirety as part of a field service repair operation. Many organizations have FRU information for each major system board (such as processor board, memory board, I/O board, and so forth). The FRU data can include information such as model, asset tag, part number, and serial number. Field replaceable units can include the system board, memory devices, and drive backplanes.

To view Field replaceable unit information

- Click **System**, then click **Field replaceable units**.

Installed applications

Intel Server Manager provides a list of installed RPM packages.

To view applications information

- Click **System**, then click **Installed applications**.

To set alert actions for installed applications

1. Click **Configure alert actions: Application added or removed**.
2. Click the types of alerts you want to send and click **Apply**.
3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Keyboard and mouse

Intel Server Manager displays the following keyboard and mouse information for the computer:

Keyboard

- **Description**—The type of keyboard attached to the computer.
- **Layout**—The keyboard layout selected in the operating system, such as US, French (Standard), or German (Standard).

Mouse

- **Description**—The type of mouse attached to the computer.
- **Connector type**—The type of connector used to attach the keyboard to the computer, such as PS/2, Micro-DIN, USB or DB-9.
- **Three-button mouse emulated—**Whether or not the mouse is three-button-emulated.

To view keyboard/mouse information

- Click **System**, then click **Keyboard and mouse**.

Management modules

Intel Server Manager displays the following information about management modules for a blade chassis:

- Name of the module.
- Bay number in the chassis
- MAC address assigned to the module
- IP Address assigned to the module
- Power state (on or off)
- Serial number of the module
- Part number of the module
- Manufacturer name

In addition, details about firmware in modules are listed, including:

- Type of firmware
- Build ID
- Firmware file name
- Date the firmware was released
- Revision number

To view management module information for a blade chassis

1. Click **Blade chassis**, then click **Management module**.

Memory

You can use Intel Server Manager to:

- View information about available physical and swap memory, as well as memory that is cached or buffered.
- View memory module information, such as socket type, size, and speed.
- Configure memory alerts
- Set thresholds for virtual memory alerts

To view memory or memory module information

1. Click **System**, then click **Memory**.
2. Open **Memory information** or **Memory modules**.

To set alert actions for memory

1. Click **Configure alert actions** for the type of alert you want to configure.
2. Click the tab of the status type (OK, Warning, Critical, or Informational) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

To set virtual memory thresholds

1. Click **System**, then click **Memory**.
2. Open **Set thresholds: Virtual memory**.
3. Drag the colored arrows to adjust the Warning and Critical thresholds.

    or

    Type percentage numbers directly in the **Warning threshold** and **Critical threshold** boxes.
4. Click **Apply** to change the thresholds.

Notes

- Used and free space are not updated dynamically. You can refresh them by clicking Apply or Refresh.
- You must have Macromedia* Flash installed to view the thresholds bar. You can download the Flash player at *www.macromedia.com*.

Motherboard

Intel Server Manager displays information about a computer's motherboard and system slots.

Motherboard information

- **Manufacturer**—The manufacturer of the computer's motherboard.
- **Version**—The version of the computer's motherboard.
- **Serial number**—The serial number of the motherboard.
- **Product Name**—The motherboard's product name.

System slots

- **Description**—The type of expansion slots available on the computer's motherboard, such as *ISA*, *EISA*, *MCA*, *PCI*, or *PCMCIA*.
- **Location**—The physical location of the system slot.
- **Slot width**—The bus width of the expansion slot, such as 16-bit or 32-bit.
- **Status**—Indicates if the slot is available or currently in use.

Note—The computer may have two expansion slots (such as an ISA slot and a PCI slot) that share the same opening in the computer's case and can't be used at the same time.

To view motherboard information

- Click **System**, then click **Motherboard**.

Multimedia

Intel Server Manager displays sound device information for the computer.

To view multimedia information

- Click **System**, then click **Multimedia**.

Network

Intel Server Manager displays the following network information for a computer. Note that the information displayed may vary slightly depending on the computer and operating system.

Network information

- **Number of network adapters—**The number of network adapters for each network device.
- **Node (MAC) address—**The computer's unique six-byte hexadecimal *MAC address.*
- *TCP/IP address***—**The four-byte address assigned to the computer for communicating on TCP/IP networks.
- *Subnet mask***—**The four-octet number (such as 255.255.255.0) that is paired with an IP address. This number tells an IP router which octets in the IP address are the network ID and which octets are the node ID.

- **Default gateway—**The IP address of the router that is configured as a default gateway for *packets* leaving the network.
- *DNS servers—*The IP address for each Domain Name Service (DNS) server on your network. You may have more than one.

Network aggregate statistics

- **Bytes received**—The number of bytes received by the computer.
- **Bytes sent**—The number of bytes transmitted from the computer.
- **Packets received—**The total number of network packets received at the computer since startup.
- **Packets sent—**The number of network packets transmitted from the computer since startup.
- **Receive errors—**The number of times since startup that the computer was unable to receive a packet.
- **Send errors—**The number of times since startup that the computer was unable to transmit a packet.

Persistent network connections

- **Mount point—**The file system location where the device is attached to the network.
- **Type—**The type of network connection.
- **Size—**The size of the network drive.
- **Used space—**The amount of disk space unavailable for use on the network drive.
- **Free space—**The amount of space available for use on the network drive.
- **Used space %**—Used space as a percentage of total space.

To view network information

- Click **System**, then click **Network**.

To set alert actions for NIC addition or removal

1. Click **Configure alert actions: NIC added or removed**.
2. Click the types of alerts you want to send and click **Apply**.
3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Operating system

Intel Server Manager displays the following information about the computer's operating system:

- **Name—**The operating system currently running.
- **Startup time—**The date and time the operating system was started.

- **Locale—**The language of the operating system.
- **Version**—The operating system version, build number, and service pack release number.
- **Kernel**—The Linux kernel currently running.

To view operating system information

- Click **System**, then click **Operating system**.

PCI Hot Plug Devices

Intel Server Manager allows you to check the status for devices installed into PCI Hot Plug Slots in the managed server.

Note: Currently, only Intel® Server Board SE7520AF2 and Intel Server Board Set SE8500HW4 running Microsoft Windows supports PCI Hot Plug slots. Check the Intel Server Manager Release Notes for the latest information on platform support.

PCI Hot Plug Slots

Intel Server Manager allows you to check the status of PCI Hot Plug slots on the managed server.

Note: Currently, only Intel® Server Board SE7520AF2 and Intel Server Platforms SR4850HW4 and SR6850HW4 running Microsoft Windows supports PCI Hot Plug slots. Check the Intel Server Manager Release Notes for the latest information on platform support.

Performance

The Intel Server Manager Performance page lets you monitor the performance of various system objects. You can monitor specific hardware components, such as drives, processors, and memory, or you can monitor OS components, such as processes or bytes/sec transferred by the system's Web server. The Performance page includes a graph that displays real-time or historical data for a counter. You can also acknowledge alerts received for a counter and stop monitoring a performance counter by deleting it from the list of monitored counters.

In order to monitor a performance counter you must first select the counter, which adds it to the list of *monitored counters*. When you do this you also specify the frequency for polling the item and set performance thresholds and the number of violations that are allowed before an alert is generated.

You can set alert actions to trigger notification when a performance counter crosses an upper or lower threshold a predetermined number of times.

To view a performance graph for a monitored counter

1. Click **System**, then click **Performance**.
2. Click **Performance graph**.

3. From the **Counters** drop-down list, select the counter you for which want to see a performance graph.

4. Select **View real-time data** to display a graph of real-time performance.

> or

Select **View historical data** to display a graph showing performance over the period you specified (Keep history) when selecting the counter.

Notes

- The horizontal axis represents time that has passed.

- The vertical axis represents the units you are measuring, such as bytes/sec (when monitoring file transfers, for example), percentage (when monitoring percentage of the CPU that is in use), or bytes available (when monitoring hard drive space).

- The line height is not a fixed unit. The height of the line changes relative to the extremes in the data; for one counter the vertical axis might represent 1 to 100 and for another it might represent 1 to 500,000. When the data varies across a wide extreme, minimal changes can appear as a flat line.

- Selecting another counter refreshes the graph and resets the units of measurement.

- Click [icon] to clear and restart the graph.

- Click **Reload counters** to refresh the list with any new objects, instances, or counters.

To stop monitoring a performance counter

1. Click **System**, then click **Performance**.

2. Click **Monitored performance counters**.

3. Check the counter(s) you want to stop.

> or

Click **Select all** to select all current counters.

4. Click **Delete**.

To acknowledge an alert for a performance counter

1. Click **System**, then click **Performance**.

2. Click **Monitored performance counters**.

3. Check the counter for which you have received an alert.

4. Click **Acknowledge**.

To set a performance alert action

1. Click **Configure alert actions: Performance**.

2. Click the tab of the status type (OK or Warning) you want to set alerts for.

3. Click the types of alerts you want to send and click **Apply**.

4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Note—You must *select a counter* or counters to monitor before alerting can take place.

Ports

Intel Server Manager displays the following port information for the computer.

Serial ports

- **Name**—The name of the *serial port*, such as 1 or 2.
- **IRQ**—The *interrupt request* number assigned to the serial port, such as 3 or 4.
- **I/O address**—The starting memory address (represented in *hexadecimal*) designated for the input/output of data from the serial port.
- **Baud rate**—The default baud rate of data transfer for the serial port.

Parallel ports

- **Name**—The name of the *parallel port*, such 1.
- **IRQ**—The IRQ assigned when the parallel port is accessed.
- **DMA**—The Direct Memory Access assigned when the parallel port is accessed.
- **I/O address**—The starting memory address (represented in hexadecimal) designated for the input/output of data from the parallel port.

To view ports information

- Click **System**, then click **Ports**.

Power domains

Intel Server Manager displays information about power domains in a blade chassis. This includes the following general information about each power domain:
- Name of the power domain
- Status of the power domain
- Bays in the chassis and their power usage
- Oversubscription policy for the domain
- Total power budget for the domain (in watts)
- Amount of power reserved (in watts)
- Amount remaining (in watts)
- Power in use (in watts)

In addition, details about power consumption of each power domain are given, including:

- Names of components within the domain

- Status of each component

- Current usage of each component

- Minimum and maximum power usage for each component (in watts)

To view power domain information for a blade chassis

1. Click **Blade chassis**, then click **Power domains**.

Power modules

Intel Server Manager displays the following general information about power modules in a blade chassis:

- Bay in the chassis that contains the module

- Date of manufacture of the power module

- Revision number of the module

- Serial number of the module

- Part number of the module

- Power module manufacturer name

To view power module information for a blade chassis

1. Click **Blade chassis**, then click **Power modules**.

Power supplies

Use Power supplies to view the name and status of each power supply on a server. You can also set alert actions to trigger notification if a power cord is connected or disconnected, a power supply is added or removed, or a power supply fails.

To view power supply information

- Click **System**, then click **Power supplies**.

To set alert actions for power supplies

1. Click **Configure alert actions: Power supplies**.

2. Click the tab of the status type (Informational, OK, Warning, or Critical) you want to set alerts for.

3. Click the types of alerts you want to send and click **Apply**.

4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Processes

Use the Processes page to view a list of current processes and related statistics on the selected machine.

Information about processes is listed in the following columns:

- **Name**—The name of the executable file of the process.
- **User—**The common name of the user who started the process.
- **PID—**Process Identification Number. A unique number assigned to each process.
- **CPU Time**—The percentage or amount of time used by the process.
- **Memory usage**—The amount of memory the process is using.
- **Virtual size**—The size of virtual memory taken by the process on the hard disk.

To view current processes

- Click **System**, then click **Processes**.

Sensors

Use the Sensors page to view data on all the sensors of an IPMI system. Each sensor's information is taken from a Sensor Data Record (SDR), which is stored in the Sensor Data Repository. An SDR defines and completely describes a sensor, including the sensor's default initialization settings that the Baseboard Management Controller (BMC) uses at system initialization. The sensor data for many components is also displayed on the component's System page (such as Fans, Temperatures, and so forth).

Two types of sensors are displayed: *discrete sensors*, which can contain up to 15 possible states; and *numeric sensors* that return a numeric reading. Sensor data can include:

- **Type**—The classification of the sensor.
- **Description**—Additional information about the sensor.
- **Status**—The current operating state of the sensor.
- **Value**—The quantity and measurement of the type.

Notes

- The Intel Server Manager administrator database must have the correct BMC password to retrieve information from an out-of-band node. If the BMC password is not correct, the status for the node's sensors will display as "Unavailable."
- You may be prompted for the BMC password when you change thresholds or restore default thresholds for a numeric sensor. Some BMCs require that the password be supplied before making this change.

To view sensor information

1. Click **System**, then click **Sensors**.
2. Click the sensor for which you want more detailed information.

To change thresholds for a numeric sensor

1. Click **System**, then click **Sensors**.

2. Click the sensor for which you want to change thresholds.

3. Change upper and lower thresholds.

4. Click **Apply**.

Services

You can use Intel Server Manager to view the services on your computer and their statuses, or to set alert actions to notify you of changes to service status.

For each service on your computer, Intel Server Manager displays the service name, the run levels for which it is registered, and its current status. The check box beside each service indicates whether you're monitoring that service. If a monitored service stops or starts, an alert event is generated.

In the Status column there are three options:

[no icon]	Service is running
⚠	Warning: service is not running correctly
❓	Unknown: Intel Server Manager cannot determine the status of the service

To view the currently running services

- Click **System**, then click **Services**.

To set a service alert action

1. Select the services you want to monitor by checking the service name, then click **Apply**.

2. Click **Configure alert actions: Services**.

3. Click the tab of the status type (OK or Warning) you want to set alerts for.

4. Click the type of alert you want to send, then click **Apply**.

5. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Storage devices

Use Storage to view information about storage devices on a server, such as hard drives, tape drives, media changers, DAT drives, SCSI enclosures, and *RAID* devices.

Devices are listed by *SCSI* controller type. You can view the status of individual devices under a SCSI type, and for some device types you can view individual components (for example, for a device with multiple slots, you can view the status of each slot in more detail).

Device information can include safety-related physical sensor readings for items such as fans, temperature, power supplies, alarms, and doors (open or closed).

RAID arrays are treated as one device but the status page contains information about individual drives. If one drive fails or is removed, the RAID array shows failed; it then can be rebuilt as a new RAID array

Events such as disk failure generate pop-up alert windows with details that identify the device, controller, and channel for quick identification of the device.

Note: IDE and SATA drives which are run on add-in controller cards will appear as SCSI devices.

To view storage device information

- Click **System**, then click **Storage devices**.

Temperatures

Use Temperatures to monitor the temperature of vital components in your system. The data comes from the location of the temperature sensor inside the computer. The data is represented numerically and visually with a thermometer image. The columns of data are as follows:

- **Name**—The name of the component being monitored.

- **Maximum**—The maximum temperature the component can have before its performance is compromised (as determined by the manufacturer).

- **Last**—The temperature reading of the component taken from the last background scan. If this column has a substantially different value than the Current column, there may be a sudden change in the computer's health.

- **Current**—The current temperature of the component. If this column shows a value of zero, the computer is out of band (IPMI servers only).

Note—Temperature information will only appear if you have configured sensors.

To view temperature information

1. Click **System**, then click **Temperatures**.
2. Click the component for which you want more detailed information.

Note: Temperature information is not updated dynamically. You can update it by refreshing the browser window view or by clicking **Temperatures**.

To change temperature thresholds

1. Click **System**, then click **Temperatures**.
2. Click the component for which you want to change thresholds.
3. Change upper and lower thresholds.
4. Click **Apply**.

To set alert actions for temperatures

1. Click **Configure alert actions: Temperatures**.
2. Click the tab of the status type (OK or Critical) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.

4.   To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Users and groups

Use Users and groups to view users, groups, and their properties on a Linux system.

To view user and group information

- Click **System**, then click **Users and groups**.

Vital product data

Intel Server Manager displays information about firmware and hardware in an IPMI-compliant blade server under the heading Vital product data. The firmware data includes the following:

- Firmware type
- Build ID
- File name of the firmware
- Date the firmware was released
- Firmware revision number

In addition, details about the blade server hardware are given, including:

- Hardware type
- Machine type
- Serial number of the component
- Part number of the component
- Name of the manufacturer

To view vital product data for a blade server

1.   Click **System**, then click **Vital product data**.

Voltages

On motherboards that support voltage monitoring, Intel Server Manager monitors the power voltages on the computer's power supply lines. When the voltage on a given power supply line exceeds a threshold defined by the manufacturer, Intel Server Manager can notify you of a potential problem with the computer's power supply. The monitored voltages vary depending on the computer's motherboard. Also, the voltage thresholds that trigger an alert can vary across voltage lines, and can also be adjusted by the motherboard manufacturer.

Note—Voltage information will only appear if you have configured sensors.

To view voltage information

1.   Click **System**, then click **Voltages**.

2. Click the component for which you want more detailed information.

Notes

- Voltage information is not updated dynamically. You can update it by refreshing the browser window view or by clicking **Voltages**.

- You must have Macromedia* Flash installed to view the voltage status graphics. You can download the Flash player at *www.macromedia.com*.

To change voltage thresholds

1. Click **System**, then click **Voltages**.
2. Click the component for which you want to change thresholds.
3. Change upper and lower thresholds (values are in millivolts).
4. Click **Apply**.

To set alert actions for voltages

1. Click **Configure alert actions: Voltages**.
2. Click the tab of the status type (OK or Critical) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Using reports

Monitoring configuration changes

Configuration changes on a managed computer can generate alerts and are also logged. Computers running the administrator console can display configuration changes as pop-up alerts.

Note: Configuration change reports are not available for computers with the Intel Server Manager bridge agent installed (rather than the full server installation) or for out-of-band computers.

To view configuration changes

1. Click **Reports**, then click **Configuration changes**.
2. Click **Next** and **Previous** to scroll through the pages of the log.
3. To display changes for a range of dates, click **Filter by date range**, clear the **Show events for all dates** checkbox, enter a start date and an end date, then click **Filter**.

Viewing hardware events

Use Hardware events to view a list of events occurring on the hardware components of an IPMI system. This log captures system-generated hardware events, rather than the BIOS data captured in the *BIOS event log*. Log entries can be filtered by date range, generator, or sensor type.

- **Date**—The date and time the event occurred.
- **Generator**—The component that originated the event.
- **Sensor type**—The type of sensor on which the event occurred.
- **Details**—A description of what occurred on the sensor to produce the event.

To view the hardware events log

1. Click **Reports**, then click **Hardware events**.
2. Click the **Next** and **Previous** buttons to scroll through the pages of notifications in the log.
3. To filter by date range, clear the **Show events for all dates** checkbox, enter a start date, enter an end date, then click **Filter**.
4. To filter by generator or sensor type, select a generator type, select a sensor type, then click **Filter**.

Hardware events log backup

The Hardware events log displays information from the System Events Log (SEL) that is created and stored on the BMC. Because event data is not purged from the log, when the SEL reaches its storage limit, no new entries will be created as new system events are generated. For in-band

servers, you can configure Intel Server Manager to back up the SEL when it reaches a certain percentage of its capacity. The backup action performed depends on the status of the computer:

Computer status	Backup action
Unmanaged and in-band	Backup files are created in the local system temporary folder. Filenames are IPM#.tmp, where # is a number that increments with each new backup file. After creation, these files are not managed by Intel Server Manager, but may be manually viewed or deleted.
Unmanaged and out-of-band	The SEL cannot be backed up. When it becomes full, new events will not be added to it.
Managed and in-band	Backup information is sent to the administrator computer, where it is stored in the AutoSELBackup table in the database. If the administrator computer is not on when the server needs to back up, the server computer will hold the information until the administrator is powered on.
Managed and out-of-band, administrator powered on	The administrator computer retrieves backup information and stores it in the AutoSELBackup table in the database.
Managed and out-of-band, administrator powered off	The SEL cannot be backed up. When it becomes full, new events will not be added to it.

To configure hardware events log backup options

1. Click **Reports**, then click **Hardware events**.
2. Click **Configure the log file backup**.
3. Check **Turn on hardware event backup**.
4. Specify the frequency to check the log and the percentage at which it should be backed up.
5. Click **Apply**.

To back up or clear the hardware events log immediately

1. Click **Reports**, then click **Hardware events**.
2. Click **Configure the log file backup**.
3. To back up the log contents and then clear the log, click **Back up now**.
4. To clear the log without backing up its contents, click **Clear now**.

Notes:

- The backup process saves only information that is contained in the SEL. Anything cleared from the SEL before backup will not be saved.

- When an administrator begins managing a computer by adding it to the My computers list, any backup files that already exist in that computer's temporary folder will not be sent to the administrator for backup in the database. All new backups will be sent to the administrator.

- You can manually delete data from the SEL backup using a third-party SQL query analyzer.

- Be aware that while individual backup files may not be large, if you have turned on automatic hardware event backup the disk space required for storing backup files may be substantial over time. Some systems log many hardware events and may store backup files frequently. On an unmanaged server, If you do not regularly monitor the size of the temporary files directory it may eventually take up excessive amounts of disk space. On a managed server, the backup data saved to the administrator computer's database may likewise take up excessive space.

Viewing hardware event log archives

IPMI-enabled systems store a log of hardware events in the Server Event Log (SEL) on the server's BMC. When the log file is full, it can be archived so new events will continue to be stored in the SEL, which has limited storage capacity. (For information about viewing hardware events and archiving event logs, see *Viewing hardware events.*)

You can view the log files that have been archived for a server. Archives are listed by computer name and by the date and time of backup.

To view archived hardware event logs

1. Click **Reports**, then click **Hardware events archive**.

2. Find the computer name you want, then click the date/time entry in the **Archive time** column to view the archive.

3. Click **Next** and **Previous** to scroll through the pages of the log.

4. To filter by date range, clear the **Show events for all dates** checkbox, enter a start date, enter an end date, then click **Filter**.

5. To filter by generator or sensor type, select a generator type, select a sensor type, then click **Filter**.

Using system reports

Intel Server Manager can gather a substantial amount of information about the software and hardware components installed on the computers that you manage. The type of data that is available is described in *Viewing system data*. You can use this information to make decisions about performing specific tasks, such as a BIOS upgrade for the computers that need it.

The predefined reports listed below gather system data for the computers you select. These reports can help you with some of the more common tasks that you perform as an administrator:

- **BIOS**—Displays the computer name, BIOS manufacturer, BIOS version, and BIOS date.

- **Operating system**—Displays the computer name, the operating system and version of the operating system, including any service packs or updates.

- **Installed programs**—Provides a drop-down list of the applications that are installed on the computers you selected for the report. When you select an application from the list, the report updates to show which computers have the selected application installed.

In addition to generating the predefined reports described above, you can:

- *Export all system data* for a single computer or for selected computers.

- View system data about hardware and software components on the computers you manage.

To run system reports

1. From the My computers page, select the computers you want to manage.

2. Click on the toolbar.

3. Select a report type, type a report name, then click **Run**.

   The report is saved in /usr/Intel/ism/wwwroot/ism/reports folder.

To view system reports

1. Click **Reports,** then click **System reports**.

2. Click the name of the report you want to view.

Why do I see an error message in a report?

If Intel Server Manager can't connect to a computer or if you do not have rights to view inventory information, you may see these error messages in the body of the report:

Error message	Explanation
Failed: This client computer could not complete the operation.	Intel Server Manager could not connect to the computer. The computer may be turned off, or network problems may be preventing a connection. See *System requirements* for the ports that must be open for Intel Server Manager to function correctly.
Failed: You do not have sufficient rights to perform this operation.	You can't view inventory information on computers unless you can log on with administrator privileges.

Exporting system data

Using Intel Server Manager, you can export information about hardware and software components on the computers you manage. The type of data that is available is described in *Viewing system data*.

Note: If the export fails, it could be that the necessary ports are not open. In order for Intel Server Manager to function properly and completely, ports 623, 6780, 9593, 9594, and 9595 must be open. If any of these ports are not open you may have a conflict with the use of a firewall or a router. Refer to your firewall or router documentation to resolve port conflicts.

Exporting from the administrator console

From the administrator console, you can export data from selected computers to a file in .XML format. This system inventory export contains all of the information available in the Intel Server Manager system inventory as configured by the original equipment manufacturer of the computer. Therefore, the contents can vary from computer to computer.

Because Intel Server Manager gathers all of a computer's system information during an export, a single export process can sometimes take up to a minute or more. Performing a system inventory export for several computers takes considerably longer. The operation takes place in the background, however, so you can continue to work in Intel Server Manager while it gathers and exports the data.

To export data from one or more computers

1. From the My computers page, select the computer(s) for which you want to export data.
2. Click on the toolbar.
3. Type an export name and click **Run**.

Exporting from the server console

As administrator, you can log on to an individual computer and run an export for just that computer from the server console. Intel Server Manager end-users have the same options.

Because Intel Server Manager gathers all of a computer's system information during an export, the export process can sometimes take up to a minute or more.

To export data

1. Log on to the computer for which you want to export data.
2. Click **Reports,** then click **Run export**.
3. Type a name for the export, then click **Run**.

The .XML output is saved in the /usr/Intel/ism/wwwroot/ism/exports folder.

To view exported data

1. Click **Reports,** then click **System exports**.
2. Click the name of the export you want to view.

Viewing the administrator and system logs

When an event occurs on a Intel Server Manager computer, Intel Server Manager records the event details in a log. The administrator installation of Intel Server Manager has an administrator log that records event details for other Intel Server Manager computers on the network. This log includes the date and time the event occurred, the computer name, a brief description of the event, and an icon indicating the event severity.

You can filter log files to view only certain categories of events or view events that occurred within a date range. This may be useful if the log file is large and contains many entries. About 50 categories of log entries are available, including configuration changes, processor missing, and disk space.

Notes

- Date/time information is listed as UTC/Greenwich Mean Time.

- The log continues to store events until it reaches maximum size (500K). When the log reaches its maximum size, the older entries are removed and stored in a compressed file (in the /var directory) and the log is cleared to allow new entries to be added.

To view the Administrator log

1. From the administrator console, click **Reports**, then click **Administrator log.**

2. Use the View drop-down list in the log file toolbar to view all events or to select a particular type of event to view.

3. To filter by date range, click **Filter by date range**, clear the **Show events for all dates** checkbox, enter a start date, enter an end date, then click **Filter**.

4. Click **Next** and **Previous** to scroll through the pages in the log.

Configuring and viewing alerts

Using alerts

When a problem or other event occurs on a computer (for example, the computer is running low on disk space), Intel Server Manager can send an alert. You can customize these alerts by choosing the severity level or threshold that will trigger the alert. Alerts are sent to the administrator console and can be configured to perform specific actions or notify the local machine.

- *How do I see alerts?*
- *What kinds of computer problems can generate alerts?*
- *Configuring severity levels for events*
- *What is the difference between a global alert and an individual alert?*
- *Example: Configuring an individual alert for a disk space problem*
- *Example: Configuring global alert actions for all computers*

How do I see alerts?

Intel Server Manager can notify you of problems or other computer events by:

- Adding information to the *log*.
- *E-mailing* a notice.
- *Shutting down or rebooting* a computer.
- Sending an *SNMP trap* to an SNMP management console on the network.
- Displaying a pop-up alert in the terminal window. Note that when using the agent on a Linux platform while running Gnome or KE, a terminal must be open to receive alerts.

What kinds of computer problems can generate alerts?

Intel Server Manager monitors computers differently depending on the hardware and chipset that is installed. For example, chassis intrusion detection might not be available for all computers. Some of the events that Intel Server Manager can monitor are listed below:

- Applications or packages are added or removed on a computer.
- Hardware components (such as NICs, modems, drives, and memory) are added or removed on a computer.
- Errors in ECC memory have been detected.
- A system has been powered on, powered off, or rebooted remotely.
- Thresholds for system performance (such as virtual memory, drive space, voltages, temperatures, etc.) have been exceeded.
- The computer's case has been opened.

Configuring severity levels for events

Computer problems or events have some or all of the severity levels shown below. You can choose the severity level or threshold that will trigger the alert.

- **Informational**—Is available to support configuration changes, *BSA* events, discovery information, or computer events that manufacturers may include with their systems.

- **OK**—Notifies you when a problem has been resolved and returned to an acceptable level.

- **Warning**—Provides some advance warning of a problem before it reaches a critical point.

- **Critical**—Probably needs your immediate attention.

Depending on the nature of the event or computer problem, some severity levels don't apply and aren't included. For example, with the Installed applications event, applications have either been added or removed, so the alert can be Informational only. Other events, such as Disk space and Virtual memory, include three severity levels (OK, Warning, and Critical).

What is the difference between a global alert and an individual alert?

Users can configure some alerts and thresholds specifically for their computer. For example, from the client or server console, you can set customized warning and critical thresholds for disk space. These thresholds will trigger events that are sent to the administrator.

As an administrator you can configure global alert actions for events that take place on any computer on the network. The global alert actions you configure from the Intel Server Manager administrator console are independent from any alert actions configured locally on your managed computers. From the administrator console, you can also configure alert actions for individual computers by logging on to a computer from the My computers page.

Example: Configuring an individual alert for a local drive space

1. From the console of the managed computer, click **Management**, then click **Alerts**.
2. Click **Drive Space**.
3. Click the types of alerts you want to send and click **Apply**.
4. To set options for an alert (if applicable), click **Apply** to save your settings, then click **Set preferences**.

Example: Configuring global alert actions for all computers

1. From the administrator console, click **Management**, then click **Alerts**.
2. Click **Drive Space**.
3. Click the tab of the status type (Critical, Warning, or OK) you want to set alerts for.
4. Click the types of alerts you want to send and click **Apply**.
5. To set options for an alert (if applicable), click **Apply** to save your settings, then click **Set preferences**.

Using SNMP

When an event occurs on a managed computer, Intel Server Manager can send an *SNMP trap* to an *SNMP management console.* Configuring a managed computer to send an SNMP trap requires several steps, depending on the computer's operating system. In general, you need to:

- Install SNMP.

- Specify a destination for the SNMP traps. This destination can be either an *IP address* or a computer name.

Intel Server Manager can send SNMP traps to a management console using two different routes:

- **From the managed computers directly to a management console.** This method is more reliable than having an administrator forward the events, because if the administrator computer responsible for sending the SNMP traps goes off the network, none of the SNMP traps will be sent.

- **From the managed computers to an administrator computer. The administrator then sends the SNMP trap to a management console.** This method, although less reliable than the first, is much easier to implement. Instead of installing and configuring the SNMP software on each computer on your network, the administrator computer can receive SNMP traps and then send them to a management console on behalf of all computers it manages.

SNMP is required on a computer to install the Intel Server Manager administrator console. The SNMP service must be running to receive alerts from IPMI-enabled systems. See your Linux documentation or your Linux vendor's Web site support for specific installation information. See *SNMP* for information on configuring SNMP.

IPMI configuration

Use the IPMI configuration page to customize settings for communicating with IPMI-enabled systems. The features described below are available for in-band servers; if a server is out of band, only the power configuration and BMC user settings are available.

NOTE: It is strongly recommended that you do not change IPMI settings unless you are familiar with the *IPMI specification* and understand the related technologies involved in these settings. Improper use of these configuration options may prevent Intel Server Manager from successfully communicating with IPMI-enabled computers.

The following configuration options are available:

- *Restore default BMC settings*

- *LAN and serial configuration*

- *Watchdog timer settings*

- *Power configuration settings*

- *BMC username/password settings*

Restoring default BMC settings

If you have customized the BMC settings for a computer, you can restore them to the settings that Intel Server Manager uses when the product is installed, which include the following:

- IP synchronization is re-enabled

- LAN and serial channel configuration is reset to automatic settings:

    - All LAN and serial channels are enabled with an administrative privilege limit and no session limit

    - Per-message authentication is enabled, with MD5, MD2, straight password, and RMCP+ (IPMI 2.0 only) authentication methods

- Power configuration is restored to the recommended setting (restore computer to the state it was in when power was lost)

- The PEF (Platform Event Filtering) table is restored to Intel Server Manager defaults, which includes the Event destination in the LAN Configuration

Notes:

- BMC user name settings are not reset when BMC settings are restored.

- When a server is out of band, the Restore recommended settings option is not available.

To restore default BMC settings

1. Click the computer you want to manage on the **My computers** list.

2. Log on to the computer.

3. Click **Management**, then click **IPMI configuration**.

4. Click **IPMI configuration**, then click **Restore recommended settings**.

Changing LAN and serial configurations

IPMI messages can be carried directly from the BMC over LAN and serial interfaces in addition to the computer's System Interface. Enabling LAN or serial communication allows the Intel Server Manager administrator console to receive IPMI-specific alerts even if the computer is powered down. The administrator console maintains this communication as long as the computer has a physical network connection with a valid network address, and as long as the computer's main power remains connected.

To change LAN and serial configuration settings

1. Click the computer you want to manage on the **My computers** list.

2. Log on to the computer.

3. Click **Management**, then click **IPMI configuration**.

4. Click **LAN and serial configuration**.

5. Select an access method for LAN and for serial access.

6. Click **Apply**.

Notes:

- If you select custom configuration, click the **Customize** option to specify configuration details.

- For serial modem operation, you may need to configure the server board's BIOS and jumper settings. See the documentation that same the particular server for details

Changing watchdog timer settings

IPMI provides an interface for the BMC watchdog timer. This timer can be set to expire periodically, and is configured to initiate certain actions if it expires (such as power cycling). Intel Server Manager is configured to reset the timer periodically so it does not expire; if the computer becomes unavailable (for example, it is powered down or hangs), the timer is not reset and it then expires, which initiates the action.

You can specify how much time to allow before the timer expires and select an action to perform if it does expire.

To change watchdog timer settings

1. Click the computer you want to manage on the **My computers** list.
2. Log on to the computer.
3. Click **Management**, then click **IPMI configuration**.
4. Click **Watchdog timer settings**.
5. Check **Turn on the watchdog timer** to enable the timer.
6. Specify the frequency of checking the timer (number of minutes or seconds).
7. Select an action to initiate when the watchdog timer expires.
8. Click **Apply**.

Changing power configuration settings

When power is lost on an IPMI-enabled computer, you can specify what action should be taken when power is restored. It is recommended to restore the computer to whatever state it was in at the time power was lost, but you can also choose to keep it powered off or always power up the computer.

To change power configuration settings

1. Click the computer you want to manage on the **My computers** list.
2. Log on to the computer.
3. Click **Management**, then click **IPMI configuration**.
4. Click **Power configuration**.
5. Select an option for when power is restored.
6. Click **Apply**.

Changing BMC user settings

Intel Server Manager authenticates to a BMC with a user name/password combination that is unique to the BMC (separate from any other Intel Server Manager user names). Intel Server Manager reserves the first user name so it can always communicate with the BMC. If the BMC allows other user names to be defined, you can define user names with passwords for BMC authentication.

To change BMC user settings

1. Click the computer you want to manage on the **My computers** list.
2. Log on to the computer.
3. Click **Management**, then click **IPMI configuration**.
4. Click **BMC user settings**.
5. To add or change a username, click **Edit**.
6. To clear the data for a user name, click **Clear**.

Monitoring computer health

Monitoring health

Intel Server Manager monitors important computer functions and resources so it can alert you to problems as soon as it becomes aware of them. Depending on the computer's hardware, resources and functions, Intel Server Manager can monitor any of the following:

- **Drive space**—Monitors how much drive space remains on each logical drive. *Thresholds* are configurable for each logical drive.

- **Fan speeds**—Monitors the speed for cooling fans installed in the computer. (Fan speed monitoring can occur only if you have configured sensors.)

- **Performance**—Monitors performance data of counters you specify (for components such as drives, memory, network traffic, and so forth).

- **Services—**Monitors the system services you have selected.

- **Temperatures**—Monitors the temperature of vital components in your system. (Temperature monitoring can occur only if you have configured sensors.)

- **Virtual memory**—Monitors how much virtual memory remains available to the computer. Thresholds are configurable.

- **Voltages**—Monitors the power voltages on the computer's power supply lines. (Voltage monitoring can occur only if you have configured sensors.)

When a problem occurs in one of the areas listed above, the computer's health status changes from Normal to either Warning or Critical, depending on the event and its severity. (The status icon for the computer will include a Warning ⚠️ or Critical 🛑 icon.) You can observe a computer's health change using one of the following Intel Server Manager tools:

- **My computers list**—The *My computers list* displays an icon and the Status column indicates the health for each computer in the list.

- **Summary**—The computer summary page displays a description of the problem.

- **System**—Under the System link in the left pane, click the item generating the health status change (such as Drives or Memory). The page for the item includes a description of the problem and steps you can take to resolve the problem.

- **Alerts**—ISM includes five different *alert actions* you can select to notify you of health changes.

You can select the health contributors that determine the computer's health status. By default all health contributors are selected. If you deselect an item it no longer contributes to the overall health, but you will still receive alerts for that item. For example, if you decide that Performance counters do not need to be included in overall health warnings for a server, you can deselect Performance. You will, however, receive any alerts you have selected for Performance counters.

For an out-of-band IPMI server, a limited number of health contributors can be monitored through the server's BMC. These are indicated with "(IPMI)" in the list of health contributors. These are not configurable, so they are monitored when the server is out of band whether or not you have deselected them on the list of health contributors.

When you receive health status notifications for a blade server or chassis management module (MM), you can view the details in the management module's web interface provided by the

manufacturer. On the summary page for the server or MM, click the health status notification to open the manufacturer's user interface.

To select health contributors

1. Click **Management**, then click **Health**.

2. On the Health page, select the items you want contributing to overall system health, then click **Apply**.

Selecting performance counters

The Intel Server Manager Performance counters page lets you select performance items that you want to monitor. You can monitor specific hardware components, such as drives, processors, and memory, or you can monitor OS components, such as processes or bytes/sec transferred by the system's Web server. When you select a performance counter you also specify the frequency for polling the item, as well as specify the performance thresholds and number of violations that are allowed before an alert is generated.

When a performance counter has been selected you can then *monitor performance* on the Performance page by viewing a graph with real time or historical data.

You can also set alert actions to trigger notification when a performance counter crosses an upper or lower threshold a predetermined number of times.

To select a performance counter to monitor

1. Click **Management**, then click **Performance counters**.

2. Click **Select performance counters to monitor**.

3. From the Objects column, select the object you want to monitor.

4. From the Instances column, select the instance of the object you want to monitor, if applicable.

5. From the Counters column, select the specific counter you want to monitor.

6. Specify polling interval and days to keep history.

7. In the **Alert after counter is out of range** drop-down list, specify the number of times the counter will be allowed to cross the thresholds before an alert is generated.

8. Specify upper and/or lower thresholds.

9. Click **Apply**.

Notes

- Performance log files can quickly grow in size; polling a single counter at a two second interval adds 2.5MB of information to the performance log daily.

- Changing the **Alert after counter is out of range** number lets you choose to focus on an issue when it is a persistent problem or when it is an isolated event. For example, if you are monitoring the bytes sent from a Web server, Intel Server Manager can alert you when the bytes/sec consistently runs high. Or, you can specify a low number such as 1 or 2 to get alerted whenever your anonymous FTP connections exceeds a certain number of users.

To set a performance alert action

1. Click **Management**, then click **Alerts**.

2. Click **Performance**.

3. Click the tab of the status type (OK or Warning) you want to set alerts for.

4. Click the types of alerts you want to send and click **Apply**.

5. To set options for an alert (if applicable), click **Apply** to save your settings, then click **Set preferences**.

Note—You must select a counter or counters to monitor before alerting can take place.

(This page intentionally left blank.)

Preferences

Alerts preferences

Use Alerts preferences for the following:

- *Configuring e-mail and pager alerts*
- *Configuring power cycle alerts*

Configuring e-mail and pager alerts

Use the E-mail alerts page to configure how you want Intel Server Manager to format and send alert-action e-mail messages. If you don't have access to an SMTP Internet mail server, this alert action won't work.

For information on configuring which events and severity levels trigger e-mail notices, see *Using alerts*.

Notes:

- In the event of a failed connection to the SMTP Internet mail server, Intel Server Manager will make continued attempts according to the delivery options you've specified. When Intel Server Manager successfully passes an e-mail notice to the SMTP server, it no longer has control of delivery for that notice.
- Intel Server Manager does not set e-mail alerts on SMTP servers that require authentication.

You can change these Intel Server Manager e-mail settings:

- **Outgoing mail server (SMTP)**—The SMTP Internet mail server that the alert action will send the message through.
- **To**—The e-mail address that will receive the alerts. Use a comma-separated list of e-mail addresses to notify multiple e-mail accounts. You can also send the message to a pager address such as 5551234567@ mobile.att.net.
- **From**—The e-mail address that will appear in the message's From field. This must be a valid e-mail address.
- **Subject**—The message's subject text. Extended characters are not allowed in the subject field and will be replaced by a "?" character. If the alert description (%D) or severity (%S) is included in the subject line, it will always display in English.
- **Body**—The message's body text
- **Parameter language**—The language of the parameters.
- **Delivery attempts**—How often Intel Server Manager should retry failed connections to the SMTP mail server you specified.
- **Minutes between attempts**—How long Intel Server Manager should wait to retry failed connections to the SMTP mail server you specified.

The subject and body can contain dynamic parameters that get replaced when the e-mail message is sent. You can use up to 10 of these parameters in your message:

- %% = %

- %D = Description
- %N = Computer name
- %S = Severity
- %T = Time (UTC)

To set e-mail and pager alerts preferences

1. Click **Preferences**, then click **Alerts**.
2. Click **Preferences: E-mail alerts**, then check **Send e-mail alerts.**
3. Configure the e-mail options.
4. Click **Apply**.

Configuring power cycle alerts

Use the Power cycle alerts page to cause server or client computers to shutdown or reboot when certain configured events occur.

To configure which events and which severity levels trigger power cycle alerts, see *Using alerts*.

Note—Power cycles may cause data loss on unattended machines.

To set power cycle alerts

1. Click **Preferences**, then click **Alerts**.
2. Click **Preferences: Power cycle alerts**, then check **Allow power cycle alerts**.
3. Configure power cycle options.
4. When finished, click **Apply**.

Use the options below to configure power cycle alerts.

- **When an event is received: Shut down/reboot**—The type of power cycle (shutdown or reboot) to occur when a configured event is received.
- **Seconds before the power cycle is initiated**—The amount of time between when an event is received and when the power cycle take place. A warning appears on the managed computer's screen showing the number of seconds until shutdown or reboot; this allows time to save data and close applications. If this option is set to 0 no warning is given.
- **Allow a hard power cycle if graceful power cycle fails**—This option causes a hard power cycle in the event that a Intel Server Manager attempt to gracefully shut down or reboot a managed computer fails. This option is only available for IPMI systems and blade servers in a managed chassis management module.

Computer lists preferences

You can use Computer lists preferences to:

- *Change the display order of the columns in the My computers list*
- *Add columns with custom attributes to the My computers list*

You can select which attributes are shown in the columns of the My computers list. The first (leftmost) column always shows the computer name, but the other columns can be arranged as you like. You can also define custom attributes for the computers you manage. For example, you might add a Location column and manually assign a physical location (1st floor, 2nd floor, etc.) to each managed computer.

To change the column order

1. Click **Preferences**, then click **Computer lists**.

2. Click **Preferences: Computer list**.

3. Click the drop-down list of the column you want to change (column 1 is the leftmost column in the My computers list), and select the field name you want to display in the column. For example, if you want to display "IP address" in column 2 after the computer name, click the drop-down list for column 2 and select "IP address."

4. Click **Apply** to save your changes, or click **Restore defaults** to return the columns to their original order.

To add a column with custom attributes

1. Click **Preferences**, then click **Computer lists**.

2. Click **Preferences: Computer list**.

3. Click one of the tabs labeled "(not defined)".

4. Type the heading for the attributes in the **Column Name** box.

5. For each attribute that can be assigned, type the attribute and click **Add to list**.

6. When all the attributes you want are listed, click **Apply**.

7. In the list of columns, click the drop-down list for the column (2-8) and select the attribute heading you created.

8. Click **Apply** to add the new column to the My computers list.

The custom attribute column is now available in the My computers list. To assign an attribute value to managed computers, select the computers and click on the toolbar. See "*Applying custom attributes*" for more information.

Discovery preferences

You can use Discovery preferences to change discovery and refresh preferences. Data about the computers you manage is updated periodically, by automatic discovery and by updating status information for managed computers. Use Discovery preferences to set the frequency at which these actions are automatically performed.

Intel Server Manager refreshes information about managed computers in two ways:

- The My computers list is updated

- All managed computers are queried to update their status

When the My computers list is updated, computer status from the last query is shown, and any alerts that have been sent from the managed computers are also shown. You may receive alert notification before the list status is updated.

You will likely refresh the list more frequently than you query computers. The query process can take substantial amounts of time if you are managing many computers, so you may choose to do this infrequently. But you can refresh the list frequently to show status updates more often. This lets you see alert information promptly even if Intel Server Manager has not run a query on all computers recently.

You can set the rate at which Intel Server Manager performs a discovery operation automatically. This discovery process runs in the background and is performed based on the addresses and methods you specify.

You can also choose whether to clear the Other computers list each time background discovery is executed. If you do not check this option, the list is updated but not completely rebuilt when background discovery occurs. If you check this option, the list is cleared and reconstructed each time discovery is executed.

To change the refresh rate for computer status

1. Click **Preferences**, then click **Discovery**.
2. Specify the time periods for refreshing the computer list and for updating managed computer information.
3. Click **Apply** to change the settings.

To immediately query all managed computers

1. Click **Preferences**, then click **Discovery**.
2. Click **Query now**.

To change frequency of automatic discovery

1. Click **Preferences**, then click **Discovery**.
2. Specify the number of hours for automatic discovery.
3. Click **Apply** to change the settings.

To initiate discovery of unmanaged computers

1. Click **Preferences**, then click **Discovery**.
2. Click **Discover now**.

This begins a background discovery process. While it is running you can continue to manage computers from the console.

To clear the Other computers list

- To clear the list immediately, click **Clear now** (or click on the Other computers toolbar).

- To clear the list each time automatic discovery occurs, check **Clear the Other computers list before re-discovery**, and then click **Apply**.

Changing computer management options

My computers preferences include options that let you change settings related to managing computers:

- **Enable management of out-of-band IPMI servers over LAN.** Enables the discovery of Baseboard Management Controllers that are listening for connections over the LAN, thus allowing you to manage them.

- **Enable serial management of out-of-band IPMI servers.** This option lets you manage out-of-band IPMI servers with a serial port connection. When this option is checked, clicking on the toolbar to add computers to your My computers list will display serial connection options. These allow you to define a particular serial connection for a computer with port, baud rate, flow type, and phone number information. The computer on that connection is then added to your list of managed computers. In addition, when you enable this option a group (Serial IPMI devices) is automatically added to your My computers list so you can view all serial devices in a single list.

- **Enable blade and chassis management.** This option enables Discovery to discover chassis and blade servers. If it is not selected, Discovery doesn't find them. You can still manage blade servers and chassis by clicking and entering the computer name or IP address of the individual blade server or chassis.

Hardware events preferences

Use Hardware events preferences to configure hardware events log backup options for out-of-band IPMI servers.

IPMI-enabled systems maintain a log of hardware events in the BMC's System Events Log (SEL). Because event data is not purged from the log, the SEL can reach its storage limit and stop logging new hardware events. To prevent this from happening, you can configure Intel Server Manager to back up the hardware events log in the SEL and clear the log when it reaches a certain percentage of its capacity. (For information on configuring SEL backup options, see *Viewing hardware events*.)

SEL backup options are not fully available for IPMI servers that are out of band. However, Intel Server Manager can retrieve the backup data for out-of-band servers. You can configure the settings for how frequently the SEL is checked and what percentage of the repository can be filled when a backup occurs.

To configure hardware events log backup options for out-of-band IPMI servers

1. Click **Preferences**, then click **Hardware events**.
2. To enable backup for out-of-band servers, check **Turn on hardware event backup**.
3. Specify the frequency to check the log and the percentage at which it should be backed up.
4. Click **Apply**.

Legacy support preferences

You can manage computers which have either a previous version of Intel Server Manager or a LANDesk Client Manager version from 6.3 - 8.0 installed on them. However, these "legacy" computers are not available to be managed until you enable this option in the Intel Server Manager administrator version. (This is because the passing of credentials is handled differently between different product versions, so a user name/password combination specifically defined for managing legacy computers is required.)

You can enable support of legacy computers using the Legacy support preferences page. When you enable it, you must set a password for the administrator user name.

After legacy support is enabled, computers with legacy versions are discovered and listed in the Other computers list. To add one of these computers to your My computers list, you must supply the same password credentials for the administrator user name that you used when you enabled legacy support.

After the administrator user name and password are set, you can change the password at any time on the Legacy support preferences page. (Note that you cannot disable Legacy support after you have enabled it.)

To enable legacy support

1. Click **Preferences**, then click **Legacy support**.
2. Check **Enable legacy support**.
3. Type the password that you will use for managing legacy computers, then retype it.
4. Click **Apply**.

To change the password for administration of legacy computers

1. Click **Preferences**, then click **Legacy support**.
2. Type the password that you will use for managing legacy computers, then retype it.
3. Click **Apply**.

Reference information

Troubleshooting

Installing Intel Server Manager on computers with a bridge agent

If you install Intel Server Manager on clients or servers that have a previously installed Intel Server Manager bridge agent, be aware that the Intel Server Manager agent removes the existing bridge agent during installation. Any custom BMC configurations that may have been defined on the computer are lost.

IPMI not detected on Linux server with OpenIPMI

If Intel Server Manager is installed on a Linux server that has the OpenIPMI device driver installed, the Intel Server Manager IPMI driver (LDIPMI) will not load and IPMI functionality for that server will not be detected. Intel Server Manager currently does not support OpenIPMI.

System information not available on Windows Server 2003 servers

When you use the Intel Server Manager administrator console to manage a server running Windows Server 2003, you may see a message that information is not available for some system inventory items (such as fans, voltages, storage devices, etc.). This can be due to problems in the WMI repository (also called the CIM repository) for that machine. In this case the problem cannot be resolved in Intel Server Manager because the ability to manage the machine depends on the presence of an existing CIMV2 schema in the repository. This can only be resolved by restoring the WMI repository (refer to Windows Server 2003 support documentation for details).

"Connection failed" error message

Problem: IPMI server on Other computers list cannot be managed

In rare cases an IPMI server may be displayed on the Other computers list but cannot be added to the My computers list. This occurs if the server was in band at the time it was last discovered but then changes to out-of-band status and is out of band when you attempt to add it to My computers.

If this happens you will receive a "Connection failed" error message when you try to manage the computer.

If this occurs, you need to discover the computer again. This will list the computer with "out of band" status on the Other computers list, and you can then add the computer to the My computers list and manage it as you would any other out-of-band computer.

1. Click to clear the Other computers list.

2. Click to discover computers.

3. If needed, refresh the Other computers list.

4. Select the computer and click to add it to My computers.

"The computer(s) could not be managed (general failure)" error message

General errors are generated by the manage/add computer system and are formatted as "The computer(s) could not be managed (general failure *%s*)" where *%s* is replaced with a number identifying the specific error.

Number	Meaning
0	A general catastrophic error occurred (possibly dealing with Windows Sockets).
1	An invalid network was found. The computer may have been attached to a network without a DNS.
2	Reserved for future use.
3	Invalid command line.
4	No computers selected to be managed.
5	Memory allocation error.

Port conflicts with routers or firewalls

If the computer you are trying to manage is on a different subnet than the administrator console, you may not be able to view all data. In order for Intel Server Manager to function properly and completely, ports 623, 6780, 9593, 9594, and 9595 must be open. If any of these ports are not open you may have a conflict with the use of a firewall or a router. Refer to your firewall or router documentation to resolve port conflicts.

Blade chassis cannot be managed due to failed DNS resolution

For Intel Server Manager to manage a blade chassis management module (MM), your network must have a properly configured method for DNS resolution and reverse DNS lookup must be available. In addition, there must be unrestricted SNMP access to the MM. If you are unable to manage a management module, review the following settings. After changing any of these settings, restart the MM to ensure that the new settings are in effect.

- **The DNS protocol must be enabled on the MM.** On the web interface for the MM, make sure that DNS is enabled and that a valid DNS server IP address is referenced. On the MM's web interface, click **MM Control** | **Network Protocols** | **Domain Name System (DNS)** to make this change.

- **There must be one available SNMP community name on the MM.** Management modules are typically configured with one unassigned community name, but if you have changed this configuration Intel Server Manager may be unable to assign a community name for its own use. On the MM's web interface, click **MM Control** | **Network Protocols** | **Simple Network Management Protocol (SNMP)** to verify this setting.

- **SNMP access must be unrestricted across the network.** If the MM is behind a router, make sure there is no SNMP filter on the router. (See your router documentation for more information.)

SNMP

Intel Server Manager uses Simple Network Management Protocol (SNMP) to provide support for:

- *Alerting via SNMP*. Intel Server Manager can directly forward *SNMP traps*.

- An administrator performing SNMP gets on managed computers.

Traps are transmitted to a configured SNMP management application on an administrator computer via the SNMP service.

Installing SNMP

Intel Server Manager services

On Linux, Intel Server Manager runs the following services.

- **pds2—**Intel Ping Discovery Service. Enables Intel Server Manager to discover other Intel Server Manager computers on the network.

- **lsm—**Intel Intel Server Manager. Provides computer management and performance monitoring.

- **xinetd—**Extended Internet Services Daemon. Allows Intel Server Manager to execute a program when data is received on a specified port.

- **bcp—**Backend Communication Port. Allows Intel Server Manager to send events.

- **cba—**Web server.

- **watchdog—**IPMI watchdog.

- **ipsync—**Synchronizes IP numbers with the BMC.

- **lbridged**—ISM Linux Bridge Agent.

- **lsmipmisensord**—Provides Intel Server Manager with access to IPMI sensors or ASIC sensors.

- **ldipmidaemon—**Provides Intel Server Manager with access to in-band and out-of-band IPMI functionality.

Version information

Use Version information to view a list of files installed during the Intel Server Manager installation, and to view the availability of those files.

To view version information

1. In the top-right of the browser window, click **About**.
2. Click **Version Info**.
3. To exit, click **Back to about** or **Close** at the bottom of the screen.

Converting Celsius to Fahrenheit

Because temperature-monitoring computer hardware reports the temperature in degrees Celsius, users in the United States may want to convert the reported temperature to Fahrenheit. The table below lists the Fahrenheit equivalents to the Celsius values reported by Intel Server Manager. (The conversion formula is: **°F = 9/5(°C) + 32**)

°C	°F	°C	°F	°C	°F	°C	°F
0°	32.0°	26°	78.8°	51°	123.8°	76°	168.8°
1°	33.8°	27°	80.6°	52°	125.6°	77°	170.6°
2°	35.6°	28°	82.4°	53°	127.4°	78°	172.4°
3°	37.4°	29°	84.2°	54°	129.2°	79°	174.2°
4°	39.2°	30°	86.0°	55°	131.0°	80°	176.0°
5°	41.0°	31°	87.8°	56°	132.8°	81°	177.8°
6°	42.8°	32°	89.6°	57°	134.6°	82°	179.6°
7°	44.6°	33°	91.4°	58°	136.4°	83°	181.4°
8°	46.4°	34°	93.2°	59°	138.2°	84°	183.2°
9°	48.2°	35°	95.0°	60°	140°	85°	185.0°
10°	50.0°	36°	96.8°	61°	141.8°	86°	186.8°
11°	51.8°	37°	98.6°	62°	143.6°	87°	188.6°
12°	53.6°	38°	100.4°	63°	145.4°	88°	190.4°
13°	55.4°	39°	102.2°	64°	147.2°	89°	192.2°
14°	57.2°	40°	104.0°	65°	149.0°	90°	194.0°
15°	59.0°	41°	105.8°	66°	150.8°	91°	195.8°
16°	60.8°	42°	107.6°	67°	152.6°	92°	197.6°

17°	62.6°	43°	109.4°	68°	154.4°	93°	199.4°
18°	64.4°	44°	111.2°	69°	156.2°	94°	201.2°
19°	66.2°	45°	113.0°	70°	158.0°	95°	203.0°
20°	68.0°	46°	114.8°	71°	159.8°	96°	204.8°
21°	69.8°	47°	116.6°	72°	161.6°	97°	206.6°
22°	71.6°	48°	118.4°	73°	163.4°	98°	208.4°
23°	73.4°	49°	120.2°	74°	165.2°	99°	210.2°
24°	75.2°	50°	122.0°	75°	167.0°	100°	212.0°
25°	77.0°						

Glossary

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A

AGP

Advanced Graphics Port. A high-performance bus type that uses short expansion slots for AGP video cards. AGP buses are targeted at 3D graphics applications and based on a set of performance enhancements to *PCI*.

AMS

Alert Management System. A component of Intel management products that provides various alerting capabilities, such as paging, Internet mail, and broadcasts.

ASF

Alert Standard Format. A standard which defines alerting and remote control interfaces to proactively manage networked devices when their operating system is absent.

ASIC

Application-Specific Integrated Circuit. A customized microchip which is designed for a specific application.

B

BIOS

Basic Input/Output System. A set of software routines generally stored in a firmware chip located on the motherboard. The BIOS is responsible for your computer's input/output activities, such as interpreting keystrokes and mouse clicks, displaying images and characters on the screen, and sending data to the printer.

blade server

A server designed for use in a space-saving rack with multiple servers that share power management, cooling systems, and other management features for improved efficiency. Blade servers are typically stored in a blade *chassis* that contains one or more chassis *management modules.*

BMC

Baseboard Management Controller. A microchip that autonomously polls system health status. The BMC operates on standby power and can take several actions should any elements go out of range.

BSA

Bootstrap Agent. A set of modules installed onto computers that securely enable the bootstrapping (loading and executing) and configuration of other software packages from a remote console application.

C

cache

A block of fast memory that holds data or instructions the processor is most likely to use next. A primary cache is built into the microprocessor. A secondary cache is external to the microprocessor and uses its own memory chips. The write policy of a memory cache can be implemented in two ways: a *write-through cache* and a *write-back cache.*

chassis

The frame or structure of a computer. A blade chassis is the frame that holds multiple *blade servers* and typically includes a chassis *management module* (MM) that enables integrated management of multiple blade servers.

CIM

Common Information Model. An industry standard for managing a computer's components. CIM is also sponsored by the Desktop management Task Force (DMTF). Intel Server Manager uses CIM to gather information about a computer's components.

CMM

Chassis *management module.*

D

DHCP

Dynamic Host Configuration Protocol. A communication protocol for managing *IP address* assignments within a network. IP addresses for nodes on the network can be static (one address for one node) or can be assigned dynamically (for example, if there are more computers than available IP addresses).

DIMM

Dual In-line Memory Module. A small circuit board that contains memory chips on both sides of the module. Like the *SIMM*, the DIMM is easily inserted into a socket on the motherboard to

increase the amount of RAM available to the computer. The DIMM connector tabs use 168 pins with separate contacts on each side of the circuit board. The dual contacts allow twice as much data to pass in and out of the DIMM. (DIMM also refers to the socket type designed to receive the DIMM circuit board.)

discover

Searching specified networks for computers.

DMA

Direct Memory Access. The process of moving data from devices (such as a hard drive) directly into memory. This process frees up the processor substantially so it can focus on other tasks.

DMA channel

One of seven channels (numbered 0-6) used to move data from devices (such as a hard drive) directly into memory.

DNS server

Domain Name Service server. Maintains a dynamic database of computers on the Internet with a network address (usually an IP address) and a meaningful domain name, such as "www.Intel.com." When you type a domain name in a browser to find an Internet resource, a DNS server finds the associated IP address of that resource.

E

ECC

Error Correction Code. An advanced error detection protocol for system memory on a computer. This code can detect both single-bit and multi-bit errors and correct single-bit errors on the fly.

EDO

Extended Data Output. A type of memory chip technology that can increase the CPU's memory access time by 10 to 15 percent over a non-EDO chip. To achieve the performance increase, however, the computer must be designed to take advantage of the speed benefit EDO memory offers.

EISA

Enhanced Industry Standard Architecture. One of two immediate successors to the *ISA* bus standard. The EISA bus was developed by a consortium of IBM competitors to challenge IBM's *MCA* bus.

environment variables

Variables related to the user environment that are initialized on computer startup and used by the operating system and applications running on the environment.

expansion slots

Long, narrow sockets on a motherboard used to install custom expansion cards into a computer for extended functionality. For example, you can plug a network adapter into an expansion slot so the computer can connect to a network. Other examples of expansion cards include video cards, sound cards, and modems.

EXT2

A traditional Linux filesystem ideally suited for fairly small files on fairly small drives.

EXT3

A Linux filesystem that is a layer atop the traditional ext2 filesystem. It keeps a journal file of disk activity so that recovery from an improper shutdown is much quicker than that of ext2 alone. Because it is tied to ext2, it has some of the limitations of the older system and does not exploit all the potential of the pure journaling filesystems. However, ext3 partitions have the same file structure as ext2, so backing out to the old system (by choice or in the event the journal file were to become corrupted) is extremely simple.

F

FAT

File Allocation Table. A common file system supported by most operating systems. FAT is widely used and requires little overhead, but does not offer many of the features available in more advanced file systems, such as *NTFS* or FAT32.

FAT32

File Allocation Table 32-bit. FAT32 supports larger disk sizes (up to 2 terabytes) than the original FAT. It also uses a smaller cluster size, which reduces the amount of slack space (unused space) in each cluster.

file system

The portion of an operating system responsible for managing, saving, and retrieving files on a hard drive or other media. Common file systems include FAT, FAT32, NTFS, ext2, ext3, and ReiserFS.

FRU

Field Replaceable Unit. On an IPMI-enabled system, a module or component which is typically replaced in its entirety as part of a field service repair operation.

G

gigahertz (GHz)

One billion cycles per second. A microprocessor's speed (also known as its clock speed), is measured in gigahertz. Because each computer instruction requires a fixed number of cycles, the clock speed determines how many instructions the microprocessor can execute in one second. A microprocessor that runs at 10 GHz executes 10 billion cycles per second.

H

hexadecimal

A base-16 system of counting used to enumerate and provide addresses for many aspects of computer circuitry, such as memory, *IRQs*, and network adapter addresses. The hexadecimal digits are: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F. These digits represent the decimal numbers 0 through 15. After counting to the digit F in hexadecimal, you continue counting in double digits from 10 to 1F (16–31 in decimal), 20 to 2F (32–47 in decimal), and so forth.

HTTP server

Hypertext Transfer Protocol server. A server computer that stores files, such as HTML Web pages, and serves those files to HTTP client computers as they are requested.

I

I/O address

A hexadecimal address in base memory used for input and output.

in-band

When a network element (such as a firewall, router, server, and so forth) is being managed by a wide area or local area network management tool (such as SNMP), it is considered to be "in-band." See also *out-of-band.*

instrumentation

The executable code that provides CIM management functionality for a particular component. The instrumentation code is provided by the component manufacturer.

Interrupt Request (IRQ)

A prioritized signal line used by hardware devices to interrupt the processor and request processing attention. Each hardware device generally requires its own IRQ address--a number from 0 to 15 (0 to F in *hexadecimal*).

IP address

A number that identifies the location of a network and a local computer on a network. It is composed of four octets separated by decimals, such as 127.17.5.12. IP addresses are used exclusively with the *TCP/IP* network protocols.

IPMB

Intelligent Platform Management Bus. Name for the architecture, protocol, and implementation of a special bus that interconnects the baseboard and chassis electronics and provides a communications media for system platform management information.

IPMI

Intelligent Platform Management Interface. A specification developed to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that allow management of the hardware regardless of whether the machine is turned on or not, or what state the OS may be in.

ISA

Industry Standard Architecture. The original bus standard used in IBM and compatible computers. ISA was later superseded by more technologically advanced bus architectures, such as *EISA*, *MCA*, *PCI*, and *SCSI.*

J

JBOD

Just a Bunch Of Disks. Used to refer to hard disks that aren't configured according to RAID -- a subsystem of disk drives that improves performance and fault tolerance.

K

None

L

LIF socket

Low Insertion Force socket. An older socket type used on early motherboards for processors and other chips. Unlike its successor, the *ZIF socket*, you must use considerable force when inserting

a chip into a LIF socket, and a special tool or screwdriver is generally required to remove a chip from a LIF socket.

LPT1

First parallel printer port (Line Printer 1). Because parallel ports are typically used for connecting printers to a computer, the parallel port names LPT1 and LPT2 were named after the early "line printers" that connected to them (line printer 1, line printer 2, and so forth).

M

MAC address

Media Access Control address (also known as the hardware address or node address). A unique six-byte hexadecimal address (such as 00AA00C778F7) that is permanently coded into the network adapter and can be used to identify a specific computer on a network.

management module (MM)

A special-use, single-board computer with processor, bus, memory, and peripherals that facilitates the management of multiple blade servers housed in a blade chassis. An MM typically monitors IPMI components, provides power and temperature management, and allows for out-of-band management. In Intel Server Manager the MM is managed as a unique system and individual blade servers are also managed individually as well as being part of an MM group.

MCA

Microchannel Architecture. A bus architecture developed by IBM as a successor to the ISA bus.

megahertz (MHz)

One million cycles per second. A microprocessor's speed (also known as its clock speed), is measured in megahertz. Because each computer instruction requires a fixed number of cycles, the clock speed determines how many instructions the microprocessor can execute in one second. A microprocessor that runs at 450 MHz executes 450 million cycles per second.

MIB file

Management Information Base. A text file that describes a component. MIB files are generally organized in a hierarchy of components, groups, attributes, and attribute values.

MM

See *management module*.

MOF

Managed Object Format. The file format used by CIM to describe components. MOF files are text files generally organized in a hierarchy of classes, instances, properties, and values.

N

NDIS

Network Device Interface Specification. A standard that defines how the MAC sublayer (in the OSI model) communicates with the various protocol drivers. This interface is used to enable different protocols (such as TCP/IP, IPX*/SPX*, and NetBEUI) running in the same computer to communicate with the network adapter.

NTFS

New Technology File System. A proprietary, feature-rich file system developed by Microsoft and used in Windows NT*. Among other things, NTFS supports long filenames, file level security, and file compression.

O

out-of-band

When a network goes down or is severely disrupted, a network management tool (such as SNMP) is rendered useless and network elements (such as a firewall, router, server, and so forth) cannot be managed by the tool. These out-of-band network elements can be managed by IPMI. See also *in-band*.

P

packets

Discrete chunks of data, packaged with control and addressing information, that travel over a network cable between sending and receiving computers.

parallel port

A hardware port that is used to connect printers or other devices using parallel communication. Parallel ports and cables are generally used over short distances because "cross talk" (data from one wire bleeding over onto another) is a problem with parallel cables over long distances.

parity errors

Parity errors occur when a memory error-checking procedure finds that some data stored in memory has become flawed. Parity errors are generally caused by a physical problem in the memory chips and often signal that a memory chip is going bad.

PCI

Peripheral Component Interconnect. A bus architecture developed by Intel that has wide support as a successor to the original *ISA* bus.

PCMCIA

Personal Computer Memory Card International Association, also known as PC Card. An expansion card about the size of a credit card, originally developed for the portable computer market.

plug and play

A computer's ability to automatically detect and configure new hardware components when they are plugged in, without requiring you to first complete an installation procedure. With plug and play, you can use a new peripheral as soon as it is plugged in.

POST

Power-On Self-Test. A series of diagnostic tests run by a computer's BIOS when power is turned on. The POST determines whether system hardware is functioning properly; if any essential hardware is not functional, the boot process does not continue.

primary cache

Memory cache that is built into the microprocessor. The close proximity of a primary cache to the microprocessor's circuitry gives a primary cache more speed-up potential than a secondary cache.

primary gateway

In a TCP/IP network, the router that all network packets are sent to if their ultimate destination is not on the local network.

provider

The CIM instrumentation that collects and manages data from CIM components.

proxy server

A server that resides on the network between an application (such as a Web browser), and another server (such as an HTTP server). Proxy servers improve performance by caching and fulfilling requests for files that have been previously accessed by the proxy server. Proxy servers also provide security for the network by filtering requests made to the server.

Q

None

R

RAID

Redundant Array of Independent (or Inexpensive) Disks, a category of disk drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers.

Reiser filesystem

A Linux journaling filesystem, named after Hans Reiser,and is the best known of this quick new class of keeping track of the contents of hard drives. It is the filesystem recommended by the installation program of SuSE 7.1 and 7.2.

resolution

The number of tiny individual picture elements ("pixels") of a screen that combine to make up a screen display. A high resolution (1280 x 1024) uses many more pixels than a low resolution (640 x 480) and yields a sharper screen image. Higher resolutions are generally selected by users with larger monitors to achieve a more economical use of the large screen's viewing area.

S

SCSI

Small Computer Systems Interface. A bus type that allows up to seven SCSI devices to be chained together and share a common bus. Without processor intervention, SCSI devices can arbitrate which device in the chain has access to the bus at any given time. Two SCSI devices (such as a SCSI hard drive and a SCSI tape drive) can even relay data directly between each other without processor intervention.

SDR

Sensor Data Record. A data record that provides platform management sensor type, locations, event generation, and access information.

secondary cache

Memory cache that uses a cache controller and memory chips that are external to the microprocessor. Secondary cache does not offer the same degree of speed-up potential as primary cache. However, it can be considerably larger than a primary cache and therefore hold more instructions and data.

serial port

A hardware port that is used to connect serial devices (modem, mouse, and keyboard) to the computer. Serial ports convert the computer's parallel data into serial data that can be sent over a serial cable one bit (or voltage pulse) at a time. Serial ports and cables are used for long-distance communication to eliminate the "cross talk" (data from one wire bleeding over onto another) that can occur with parallel communication over long distances. Serial ports are also used to connect the mouse and keyboard to a computer. These devices don't send much data and therefore don't require the extra bandwidth of a parallel cable.

Service Provider

The software code that arbitrates access to DMI component instrumentation and manages the MIF database.

SIMM

Single In-line Memory Module. A small circuit board that contains usually eight or nine memory chips in a single bank. The SIMM is easily inserted into a socket on the motherboard to increase the amount of memory available to the computer.

Slot 1

The processor socket type used for some Intel® Pentium® processors. Slot 1 uses a 242-contact slot that accepts a processor packaged as a Single Edge Contact (SEC) cartridge. A motherboard has one or two Slot 1s. Slot 1 only supports communication between the L2 cache and processor at half the processor's clock speed.

Slot 2

The processor socket type used for the Intel® Pentium® II Xeon™ processors. Slot 2 uses a 330-contact slot that accepts a processor packaged as a Single Edge Contact (SEC) cartridge. The Slot 2 design allows the processor to communicate with the L2 cache at the processor's full clock speed.

slot type

The type of expansion slots available on the computer's motherboard, such as *ISA*, *EISA*, *MCA*, *PCI*, *SCSI*, or *AGP*. (Not to be confused with the processor's socket types: Slot 1 and Slot 2.)

S.M.A.R.T.

Self Monitoring Analysis and reporting Technology. A drive technology that monitors its own health and reports potential problems before they occur.

SNMP

Simple Network management Protocol. A network management protocol that is part of the standard TCP/IP protocol suite. Intel Server Manager can snap in to an SNMP management console, which can receive and manage SNMP traps to monitor network devices and notify of extraordinary events or problems that occur on the network.

SNMP management console

A computer on the network that has software installed to receive and manage SNMP traps. Some products commonly used for this purpose include Microsoft Systems management Server, HP OpenView Network Node Manager*, CA Unicenter Frameworks*, and IBM/Tivoli NetView*.

SNMP trap

A notification of some network event that SNMP sends to a specified destination, usually an SNMP management console.

SSL

Secure Sockets Layer. The most commonly used protocol for secure message transfer on the Internet. When establishing an HTTP connection that requires SSL security, the URL begins with "https" to indicate that the message is transmitted over the secure layer.

subnet mask

A 32-bit number composed of four octets separated by decimals, such as 255.255.255.0. The subnet mask is paired with an *IP address*, such as 127.17.5.12, to tell an IP router which octets in the IP address are the network ID and which octets are the node ID. A subnet mask of 255.255.255.0, for example, would indicate that the first three octets of an IP address (such as 127.17.5) are the network ID, and the last octet of the IP address (such as .12) is a node ID. (The valid numbers that can be used in a subnet mask are 255, 254, 252, 248, 240, 224, 192, 128, and 0.)

T

TCP/IP

Transmission Control Protocol/Internet Protocol. The basic protocol used for Internet (and network) communication.

threshold

A configurable value that, if passed, can trigger an alert action. You can set the thresholds for some system events, such as available disk space and memory.

U

UDP

User Datagram Protocol. A connectionless transport-layer protocol commonly used in the TCP/IP protocol family. Unlike TCP, when a UDP packet is sent over the network, UDP makes no effort to verify that the packet was successfully received on the other end.

UNC

Universal Naming Convention or Uniform Naming Convention. A format for specifying the location of resources (such as computers and printers) on a network. A UNC name uses this format:

\\computer name\shared resource pathname.

Example: \\My computer\My documents\file.txt

V

None

W

Wake on LAN technology

A standard method for remotely waking a personal computer from sleep mode or a power-off condition. Wake on LAN*technology is only supported on computers that contain a Wake on LAN network adapter, which enables a sleeping computer to monitor network traffic and respond to a Wake on LAN instruction.

write-back cache

A write-back cache writes data into the cache, then periodically checks for discrepancies between cache data and memory data. (Discrepancies can occur, for example, from a hard drive

transferring data directly into memory via *DMA*). Write-back cache is faster than write-through cache, but the overhead to monitor discrepancies between memory and cache makes write-back cache more expensive.

write-through cache

A write-through cache writes the same data into memory and cache in a single operation. A write-through cache is slower than a write-back cache, but potentially safer because it guarantees that cache data and corresponding memory data are always the same.

X

None

Y

None

Z

ZIF socket

Zero Insertion Force (ZIF) socket is a socket type used on motherboards for processors and other chips. Unlike the *LIF socket*, little pressure is needed to seat a chip into a ZIF socket, and a special tool or screwdriver is not required to remove a chip from a ZIF socket. The ZIF socket was designed to reduce the risk of accidentally bending a pin (or whole row of pins) on an expensive processor when seating the chip into a socket.

Copyright and trademark notice

Index