Dell OpenManage™ Server Administrator Version 5.1

User's Guide

Notes and Notices

NOTICE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

Information in this document is subject to change without notice.
© 2006 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *PowerEdge*, *PowerVault*, and *Dell OpenManage* are trademarks is a trademark of Dell Inc.; *Microsoft*, *Windows*, *MS-DOS*, *Active Directory*, and *Windows NT* are registered trademarks and *Windows Server* is a trademark of Microsoft Corporation; *Novell* and *ConsoleOne* are registered trademarks of Novell, Inc.; *SUSE* is a registered trademark of Novell, Inc. in the United States and other countries; *Intel* and *Pentium* are registered trademarks and *Intel386* is a trademark of Intel Corporation; *Red Hat* is a registered trademark of Red Hat, Inc.; *VESA* is a registered trademark of Video Electronics Standards Association; *UNIX* is a registered trademark of The Open Group in the United States and other countries; *OS/2* is a registered trademark of International Business Machines Corporation; *VMware* is a registered trademark and *ESX Server* is a trademark of VMware Inc.

Server Administrator includes software developed by the Apache Software Foundation (**www.apache.org**). Server Administrator utilizes the OverLIB JavaScript library. This library can be obtained from **www.bosrup.com**.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

May 2006

Contents

1 Introduction 9

Overview **9**

Integrated Features **9**

Installation 9

Server Administrator Home Page 10

Instrumentation Service 10

Remote Access Service 10

Storage Management Service 11

Diagnostic Service 11

Logs 12

Other Documents You Might Need **12**

Obtaining Technical Assistance **14**

2 What's New for Version 5.1 15

3 Setup and Administration 17

Security Management **17**

Role-Based Access Control 17

Authentication 18

Encryption 19

Assigning User Privileges **19**

Creating Server Administrator Users for Supported Windows Operating Systems 19

Creating Server Administrator Users for Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems 21

Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems **22**

Configuring the SNMP Agent **23**
Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems 23
Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux 26
Configuring the SNMP Agent on Systems Running Supported SUSE Linux Enterprise Server Operating Systems 29
X.509 Certificate Management Prerequisites **32**
Firewall Configuration on Systems Running Supported Red Hat Enterprise Linux Operating Systems **32**

4 Installing Server Administrator 35

Overview **35**
Dell Installation and Server Management CD 35
Unattended and Silent Installation 35
Upgrading Server Administrator 36
Before You Begin **37**
Installation Requirements **37**
Supported Operating Systems 37
System Requirements 38
Installation Procedures **40**
Installing Server Administrator with Citrix 40
Considerations Before Installing Storage Management Service 41
Filesystem Hierarchy Standard v2.3 Support 42

5 Using Server Administrator 43

Starting Your Server Administrator Session **43**
Logging In and Out **43**
Single Sign-On 44
Systems Running a Supported Microsoft Windows Server™ 2003 Operating System 45

The Server Administrator Home Page **46**
Global Navigation Bar 48
System Tree 48
Action Window 48

Using the Online Help **50**

Using the Preferences Home Page **50**

Using the Server Administrator Command Line Interface **51**

Secure Port Server and Security Setup **52**
Setting User and System Preferences 52
X.509 Certificate Management 53

Controlling Server Administrator **54**
Starting Server Administrator 54
Stopping Server Administrator 54
Restarting Server Administrator 55

6 Instrumentation Service 57

Overview **57**

Managing Your System **58**

Managing System Tree Objects **59**

Server Administrator Home Page System Tree Objects **59**
System 60

Managing Preferences: Home Page Configuration Options **77**
General Settings 78
Server Administrator 78

7 Remote Access Service 79

Overview **79**

Hardware Prerequisites **80**

Software Prerequisites **80**

Adding and Configuring DRAC Users **81**

Configuring an Existing DRAC User **82**

Configuring the DRAC Network Properties **84**

Configuring the DRAC Alert Properties **85**

Configuring the SNMP Alert Properties 85

Configuring DRAC III Dial-in (PPP) Users and Modem Settings **86**

Adding and Configuring a DRAC III Dial-In (PPP) User. 86

Adding and Configuring DRAC III Demand Dial-Out Entries 87

Configuring the DRAC III Modem Settings 87

Configuring the DRAC Remote Features Properties. **88**

Configuring DRAC Security **89**

Certificate Management 89

Configuring Remote Connect Authentication Options 91

Accessing and Using a Dell Remote Access Controller **92**

8 Working With the Baseboard Management Controller (BMC) 93

Overview **93**

Viewing Basic BMC Information **94**

Configuring BMC Users **94**

Setting BMC Platform Event Filter Alerts **95**

Setting Platform Event Alert Destinations 97

Configuring the BMC to use a Serial Over LAN (SOL) Connection **97**

Configuring the BMC to use a Serial Port Connection **98**

Configuring the BMC to use a LAN Connection **99**

9 Storage Management Service 101

Overview **101**

Software Prerequisites **102**

Hardware Prerequisites **102**

Storage Management Service **102**
Storage Management Service and Array Manager 103
Storage Management Tree Objects 103
Storage Management Tasks 104

Migrating from Array Manager to the Storage Management **110**

Storage Management Command Line Interface **110**

Displaying Online Help **110**

10 Server Administrator Logs 113

Overview **113**

Integrated Features **113**
Log Window Task Buttons 113

Server Administrator Logs **114**
Hardware Log 114
Alert Log 114
POST Log 115
Command Log 115

11 Troubleshooting 117

Setting Alert Actions for Systems Running Supported Red Hat® Enterprise Linux and SUSE® Linux Enterprise Server Operating Systems **117**

BMC Platform Events Filter Alert Messages **118**

Understanding Service Names **119**

Fixing a Faulty Server Administrator Installation on Supported Windows Operating Systems **119**

Glossary 121

Index 145

1

Introduction

Overview

Server Administrator provides a comprehensive, one-to-one systems management solution in two ways: from an integrated, Web browser-based Graphical User Interface (GUI) and from a command line interface (CLI) through the operating system. Server Administrator is designed for system administrators to both locally and remotely manage systems on a network. Server Administrator allows system administrators to focus on managing their entire network by providing comprehensive one-to-one systems management.

NOTE: For the purposes of Server Administrator, a system can be a stand-alone system, a system with attached network storage units in separate chassis, or a modular system consisting of one or more server modules in a chassis.

Server Administrator provides information about:

- Systems that are operating properly and systems that have problems
- Systems that require remote recovery operations

NOTE: For remote recovery, a Dell Remote Access Controller card must be installed.

Integrated Features

Server Administrator provides easy-to-use management and administration of local and remote systems through a comprehensive set of integrated management services. Server Administrator resides solely on the system being managed and is accessible both locally and remotely from the Server Administrator home page. Remotely monitored systems may be accessed by dial-in, LAN, or wireless connections. Server Administrator ensures the security of its management connections through role-based access control (RBAC), authentication, and industry-standard secure socket layer (SSL) encryption.

Installation

You can install Server Administrator by using several methods. The *Dell™ PowerEdge™ Installation and Server Management* CD provides a setup program to install, upgrade, and uninstall Server Administrator and other managed system software components on your managed system. The *Dell Systems Management Consoles* CD provides a setup program to install, upgrade, and uninstall management station software components on your management station. Additionally, you can install Server Administrator on multiple systems through an unattended installation across a network.

NOTE: If you have a modular system, you must install Server Administrator on each server module that is installed in the chassis.

NOTE: For more information on unattended installation/uninstallation refer to the *Dell OpenManage™ Installation and Security User's Guide*.

To update individual system components, use component-specific Dell Update Packages. Use the Dell *Server Update Utility* application CD to view the complete version report and to update an entire system. The Server Update Utility is a CD-ROM–based application for identifying and applying updates to your server. The Server Update Utility can be downloaded from **support.dell.com**.

See the *Server Update Utility User's Guide* for more information about obtaining and using the Server Update Utility (SUU) to update your Dell PowerEdge server or to view the updates available for any server listed in the Repository.

Server Administrator Home Page

The Server Administrator home page provides easy-to-set up and easy-to-use Web browser-based system management tasks from the managed system or from a remote host through a LAN, dial-up service, or wireless network. When the Server Administrator secure port server is installed and configured on the managed system, you can perform remote management functions from any system that has a supported Web browser and connection. Additionally, the Server Administrator home page provides extensive, context-sensitive online help.

Instrumentation Service

The Instrumentation Service provides rapid access to detailed fault and performance information gathered by industry-standard systems management agents and allows remote administration of monitored systems, including shutdown, startup, and security.

Remote Access Service

NOTE: The Remote Access Service is not available on modular systems. You must directly connect to the Dell Embedded Remote Access/Modular Chassis Controller (ERA/MC) on a modular system. See the *Dell Embedded Remote Access/MC User's Guide* for more information.

The Remote Access Service provides a complete, remote system management solution for systems equipped with a DRAC solution. The Remote Access Service provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Service also provides alert notification when a system is down and allows you to remotely restart a system. Additionally, the Remote Access Service logs the probable cause of system crashes and saves the most recent crash screen.

Storage Management Service

The Storage Management Service provides storage management information in an integrated graphical view.

The Storage Management Service of Server Administrator:

- Enables you to view the status of local and remote storage attached to a monitored system.
- Supports SCSI, SATA, ATA, and SAS. Does not support Fibre Channel.
- Allows you to perform controller and enclosure functions for all supported RAID and non-RAID controllers and enclosures from a single graphical or command line interface without the use of the controller BIOS utilities.
- Protects your data by configuring data redundancy, assigning hot spares, or rebuilding failed drives.
- Provides features for configuring storage.

On supported Windows operating systems, Storage Management is installed using the Typical Setup.

On systems running supported Red Hat® Enterprise Linux and SUSE® Linux Enterprise Server operating systems, you can either install the Storage Management Service through the Red Hat Package Manager (RPM) or use the `srvadmin-install.sh` script—a menu driven script that installs the appropriate RPMs based on the options you choose.

For more information on the Storage Management Service, see the Storage Management online help and the *Dell OpenManage Server Administrator Storage Management User's Guide*. For information on how to launch the online help, see "Displaying Online Help.

NOTICE: Dell OpenManage Array Manager is no longer supported. If you are upgrading a system (installed with Dell OpenManage version 4.3 or later) with Array Manager installed, Array Manager will be removed during the upgrade process. You can use Storage Management instead.

NOTE: Installing Storage Management replaces any previous installation of the Array Manager managed system (server software) and console (client software) that resides on the system. If only the Array Manager console is installed on the system, then installing the Storage Management does not replace the Array Manager console.

NOTE: Dell OpenManage Array Manager Console (for Management Station) is available under Windows, only if previous Dell OpenManage Management Station software (with Array Manager Console installed) is detected. It is only available for upgrade.

Diagnostic Service

NOTE: The Diagnostic Service is no longer available through Server Administrator.

To run diagnostics on your system, install Dell PowerEdge Diagnostics from your *Dell PowerEdge Service and Diagnostic Utilities* CD or download and install Dell PowerEdge Diagnostics from the Dell Support website at **support.dell.com**. Dell PowerEdge Diagnostics is a stand-alone application that can be run without installing Server Administrator. See the *Dell PowerEdge Diagnostics User's Guide* for more information.

Logs

Server Administrator displays logs of commands issued to or by the system, monitored hardware events, POST events, and system alerts. You can view logs on the home page, print or save them as reports, and send them by e-mail to a designated service contact.

Other Documents You Might Need

Besides this *User's Guide*, you can find the following guides either on the Dell Support website at **support.dell.com** or on the *Documentation* CD:

- The *Dell OpenManage Installation and Security User's Guide* provides complete information on installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator for each supported operating system.
- The *Dell OpenManage Software Quick Installation Guide* provides an overview of applications that you can install on your management station (console) and on your managed systems and procedures for installing your console and managed system applications on systems running supported operating systems.
- The *Dell OpenManage Server Administrator Compatibility Guide* provides compatibility information about Server Administrator installation and operation on various hardware platforms (or systems) running supported Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.
- The *Dell OpenManage Server Administrator SNMP Reference Guide* documents the Simple Network Management Protocol (SNMP) management information base (MIB). The SNMP MIB defines variables that extend the standard MIB to cover the capabilities of systems management agents.
- The *Dell OpenManage Server Administrator CIM Reference Guide* documents the Common Information Model (CIM) provider, an extension of the standard management object format (MOF) file. The CIM provider MOF documents supported classes of management objects.
- The *Dell OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed in your Server Administrator home page Alert log or on your operating system's event viewer. This guide explains the text, severity, and cause of each Instrumentation Service Alert message that Server Administrator issues.
- The *Dell OpenManage Server Administrator Command Line Interface User's Guide* documents the complete command line interface for Server Administrator, including an explanation of CLI commands to view system status, access logs, create reports, configure various component parameters, and set critical thresholds.
- The *Dell PowerEdge Diagnostics User's Guide* provides complete information on installing and using PowerEdge Diagnostics on your system.
- The *Dell OpenManage Baseboard Management Controller Utilities User Guide* provides additional information about using Server Administrator to configure and manage your system's BMC.

- The *Dell OpenManage Server Administrator Storage Management User's Guide* is a comprehensive reference guide for configuring and managing local and remote storage attached to a system.
- The *Dell Remote Access Controller Installation and Setup Guide* provides complete information about installing and configuring a DRAC III, DRAC III/XT, and an ERA/O controller, configuring an ERA controller, and using a RAC to remotely access an inoperable system.
- The *Dell Remote Access Controller Racadm User's Guide* provides information about using the racadm command-line utility.
- The *Dell Remote Access Controller 4 User's Guide* provides complete information about installing and configuring a DRAC 4 controller and using DRAC 4 to remotely access an inoperable system.
- The *Dell Remote Access Controller 5 User's Guide* provides complete information about installing and configuring a DRAC 5 controller and using DRAC 5 to remotely access an inoperable system.
- The *Dell Embedded Remote Access/MC Controller User's Guide* provides complete information about configuring and using an ERA/MC controller to remotely manage and monitor your modular system and its shared resources through a network.
- The *Dell PowerEdge 1950 Systems — Configuration Guide* provides an overview of setting up a PowerEdge 1950 system.
- The *Dell PowerEdge 1955 Systems — Configuration Guide* provides an overview of setting up a PowerEdge 1955 system.
- The *Dell PowerEdge 2900 Systems — Configuration Guide* provides an overview of setting up a PowerEdge 2900 system.
- The *Dell PowerEdge 2950 Systems — Configuration Guide* provides an overview of setting up a PowerEdge 2950 system.
- The *Dell OpenManage Remote Install User's Guide* provides information about unattended, simultaneous provisioning and configuration solutions over the network by leveraging image-based technology.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Server Update Utility User's Guide* provides information about obtaining and using the Server Update Utility (SUU) to update your Dell PowerEdge server or to view the updates available for any server listed in the Repository.

The *Dell Installation and Server Management* CD contains a readme file for Server Administrator and additional readme files for most applications found on the CD.

NOTE: For information on how to monitor and set alerts for Server Administrator processes, see the white paper titled *Monitoring the OpenManage Server Administrator Services* at **www.dell.com/openmanage**.

Obtaining Technical Assistance

If at any time you do not understand a procedure described in this guide or if your product does not perform as expected, help tools are available to assist you. For more information about these help tools, see "Getting Help" in your system's *Hardware Owner's Manual*.

Additionally, Dell Enterprise Training and Certification is available; see **www.dell.com/training** for more information. This service may not be offered in all locations.

2

What's New for Version 5.1

- Added support for SUSE® Linux Enterprise Server (Version 10), on Intel® Extended Memory 64 Technology (Intel EM64T) systems.

  Server Administrator is only supported on the host system (domain 0), Xen extensions are not supported.

  NOTE: Remote Access Service is not supported on SUSE Linux Enterprise Server (Version 10).
- Added support for Microsoft® Windows® Small Business Server 2003 R2 on Intel EM64T systems.
- Added support for Microsoft Multilingual Interface (MUI) on the Microsoft Windows Storage Server 2003 R2 operating system.

  The Server Administrator Graphical User Interface (GUI) is not automatically displayed in the language you select in MUI. To view the Server Administrator GUI in the language of your choice, change the default browser language in your browser settings. Server Administrator GUI is only available in English, French, German, Japanese, Spanish, and Simplified Chinese.
- Added support for the following Dell™ PowerEdge™ systems: 840 and 860.
- Added support for Microsoft Virtual Server on the service console.
- Added support for VMware® ESX Server™ 3.0 on the service console.

  NOTE: Dell OpenManage® installation with VMware ESX Server software requires special steps.

  See the *VMware Systems Compatibility Guide* located in the Resource Center at **www.dell.com/vmware** to determine the versions of ESX Server software compatible with this release of Dell OpenManage. Each ESX Server release from Dell has an associated Dell VMware ESX Server *Deployment Guide*, also posted at this Web location. Instructions for installing supported versions of Dell OpenManage available at the time of that ESX Server release are found in that ESX Server release's *Deployment Guide*.
- Added support for Health rollup for the Storage Management Service.
- The **FRU** tab has been renamed as **System Components (FRU).**
- The Diagnostic Service is no longer available through Server Administrator. To run diagnostics, install Dell PowerEdge Diagnostics from your *Dell PowerEdge Service and Diagnostic Utilities* CD or download and install Dell PowerEdge Diagnostics from the Dell Support website at **support.dell.com**. Dell PowerEdge Diagnostics is a stand-alone application that can be run without installing Server Administrator. See the *Dell PowerEdge Diagnostics User's Guide* for more information.

3

Setup and Administration

Security Management

Server Administrator provides security through role-based access control (RBAC), authentication, and encryption for both the Web-based and command line interfaces.

Role-Based Access Control

RBAC manages security by determining the operations that can be executed by persons in particular roles. Each user is assigned one or more roles, and each role is assigned one or more user privileges that are permitted to users in that role. With RBAC, security administration corresponds closely to an organization's structure.

User Privileges

Server Administrator grants different access rights based on the user's assigned group privileges. The three user levels are: User, Power User, and Administrator.

Users can view most information.

Power Users can set warning threshold values and configure which alert actions are to be taken when a warning or failure event occurs.

Administrators can configure and perform shutdown actions, configure Auto Recovery actions in case a system has a non-responsive operating system, and clear hardware, event, and command logs. *Administrators* can also configure the system to send e-mails.

Server Administrator grants read-only access to users logged in with *User* privileges, read and write access to users logged in with *Power User* privileges, and read, write, and admin access to users logged in with *Administrator* privileges. See Table 3-1.

Table 3-1. User Privileges

User Privileges	Access Type		
	Admin	Write	Read
User			X
Power User		X	X
Admin	X	X	X

Read access allows viewing of data reported by Server Administrator. Read access does not allow changing or setting values on the managed system.

Write access allows values to be changed or set on the managed system.

Admin access also allows shutdown of the managed system.

Privilege Levels to Access Server Administrator Services

Table 3-2 summarizes which user levels have privileges to access and manage Server Administrator services.

Table 3-2. Server Administrator User Privilege Levels

Service	User Privilege Level Required	
	View	Manage
Instrumentation	U, P, A	P, A
Remote Access	U, P, A	A
Storage Management	U, P, A	A

Table 3-3 defines the user privilege level abbreviations used in Table 3-2.

Table 3-3. Legend for Server Administrator User Privilege Levels

U	User
P	Power User
A	Administrator
NA	Not Applicable

Authentication

The Server Administrator authentication scheme ensures that the correct access types are assigned to the correct user privileges. Additionally, when the command line interface (CLI) is invoked, the Server Administrator authentication scheme validates the context within which the current process is running. This authentication scheme ensures that all Server Administrator functions, whether accessed through the Server Administrator home page or CLI, are properly authenticated.

Microsoft Windows Authentication

For supported Microsoft® Windows® operating systems, Server Administrator authentication uses Integrated Windows Authentication (formerly called NTLM) to authenticate. This authentication system allows Server Administrator security to be incorporated in an overall security scheme for your network.

Red Hat® Enterprise Linux and SUSE® Linux Enterprise Server Authentication

For supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator authentication is based on the Pluggable Authentication Modules (PAM) library. This documented library of functions allows an administrator to determine how individual applications authenticate users.

Encryption

Server Administrator is accessed over a secure HTTPS connection using secure socket layer (SSL) technology to ensure and protect the identity of the system being managed. Java Secure Socket Extension (JSSE) is used by supported Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems to protect the user credentials and other sensitive data that is transmitted over the socket connection when a user accesses the Server Administrator home page.

Assigning User Privileges

You must properly assign user privileges to all Server Administrator users before installing Server Administrator in order to ensure critical system component security.

The following procedures provide step-by-step instructions for creating Server Administrator users and assigning user privileges for each supported operating system:

- "Creating Server Administrator Users for Supported Windows Operating Systems"
- "Creating Server Administrator Users for Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems"

NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Server Administrator on a system running Windows Server™ 2003 due to operating system constraints.

NOTICE: You should disable guest accounts for supported Microsoft Windows operating systems in order to protect access to your critical system components. See "Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems" for more information.

Creating Server Administrator Users for Supported Windows Operating Systems

NOTE: You must be logged in with Admin privileges to perform these procedures.

Creating Users and Assigning User Privileges for Supported Windows Server 2003 Operating Systems

NOTE: For questions about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.

1. Click the **Start** button, right-click **My Computer,** and point to **Manage**.
2. In the console tree, expand **Local Users and Groups**, and then click **Users**.
3. Click **Action**, and then click **New User**.

4 Type the appropriate information in the dialog box, select or deselect the appropriate check boxes, and then click **Create**.

NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Server Administrator on a system running Windows Server 2003 due to operating system constraints.

5 In the console tree, under **Local Users and Groups**, click **Groups**.

6 Click the group to which you want to add the new user: **Users**, **Power Users**, or **Administrators**.

7 Click **Action**, and then click **Properties**.

8 Click **Add**.

9 Type the user name that you are adding and click **Check Names** to validate.

10 Click **OK**.

New users can log into Server Administrator with the user privileges for their assigned group.

Creating Users and Assigning User Privileges for Supported Windows 2000 Operating Systems

NOTE: For questions about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.

1 Right-click **My Computer** and point to **Manage**.

2 In the console tree, expand **Local Users and Groups**, and then click **Users**.

3 Click **Action**, and then click **New User**.

4 Type the appropriate information in the dialog box, select or deselect the appropriate check boxes, and then click **Create**.

NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Server Administrator on a system running Windows Server 2003 due to operating system constraints.

5 In the console tree, under **Local Users and Groups**, click **Groups**.

6 Click the group to which you want to add the new user: **Users**, **Power Users**, or **Administrators**.

7 Click **Action**, and then click **Properties**.

8 Click **Add**.

9 Click the name of the user you want to add, and then click **Add**.

10 Click **Check Names** to validate the user name that you are adding.

11 Click **OK**.

New users can log into Server Administrator with the user privileges for their assigned group.

Adding Users to a Domain

NOTE: For information about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.

NOTE: You must have Microsoft® Active Directory® installed on your system to perform the following procedures.

1. Click the **Start** button, and then point to **Control Panel**→ **Administrative Tools**→ **Active Directory Users and Computers**.
2. In the console tree, right-click **Users** or right-click the container in which you want to add the new user, and then point to **New**→ **User**.
3. Type the appropriate user name information in the dialog box, and then click **Next**.

   NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into Server Administrator on a system running Windows Server 2003 due to operating system constraints.
4. Click **Next**, and then click **Finish**.
5. Double-click the icon representing the user you just created.
6. Click the **Member of** tab.
7. Click **Add**.
8. Select the appropriate group and click **Add**.
9. Click **OK**, and then click **OK** again.

   New users can log into Server Administrator with the user privileges for their assigned group and domain.

NOTICE: With Active Directory, when adding Universal Groups from separate domains, you must create an Association Object with Universal Scope. The Default Association objects created by the Dell Schema Extender Utility are Domain Local Groups and do not work with Universal Groups from other domains.

Creating Server Administrator Users for Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

Admin access privileges are assigned to the user logged in as `root`. To create users with User and Power User privileges, perform the following steps.

NOTE: You must be logged in as `root` to perform these procedures.

NOTE: You must have the **useradd** utility installed on your system to perform these procedures.

Creating Users

NOTE: For information about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.

Creating Users With User Privileges

1. Run the following command from the command line:

   `useradd -d <home-directory> -g <group> <username>`

   where `<group>` is *not* `root`.

   NOTE: If `<group>` does not exist, you must create it by using the **groupadd** command.

2. Type `passwd <username>` and press <Enter>.
3. When prompted, enter a password for the new user.

   NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components.

   The new user can now log into Server Administrator with User group privileges.

Creating Users With Power User Privileges

1. Run the following command from the command line:

   `useradd -d <home-directory> -g root <username>`

   NOTE: You must set `root` as the primary group.

2. Type `passwd <username>` and press <Enter>.
3. When prompted, enter a password for the new user.

   NOTICE: You must assign a password to every user account that can access Server Administrator to protect access to your critical system components.

   The new user can now log into Server Administrator with Power User group privileges.

Disabling Guest and Anonymous Accounts in Supported Windows Operating Systems

NOTE: You must be logged in with Admin privileges to perform this procedure.

1. If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer,** and point to **Manage**. If your system is running Windows 2000, right-click **My Computer** and point to **Manage**.
2. In the console tree, expand **Local Users and Groups** and click **Users**.
3. Click the **Guest** or **IUSR_*system name*** user account.
4. Click **Action** and point to **Properties**.
5. Select **Account is disabled** and click **OK**.

   A red circle with an X appears over the user name. The account is disabled.

Configuring the SNMP Agent

Server Administrator supports the Simple Network Management Protocol (SNMP)—a systems management standard—on all supported operating systems. The SNMP support may or may not be installed depending on your operating system and how the operating system was installed. In most cases, SNMP is installed as part of your operating system installation. An installed supported systems management protocol standard, such as SNMP, is required before installing Server Administrator. See "Installation Requirements" for more information.

You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as the Dell OpenManage™ IT Assistant, perform the procedures described in the following sections.

NOTE: For IT Assistant to retrieve management information from a system running Server Administrator, the community name used by IT Assistant must match a community name on the system running Server Administrator. For IT Assistant to modify information or perform actions on a system running Server Administrator, the community name used by IT Assistant must match a community name that allows Set operations on the system running Server Administrator. For IT Assistant to receive traps (asynchronous event notifications) from a system running Server Administrator, the system running Server Administrator must be configured to send traps to the system running IT Assistant.

The following procedures provide step-by-step instructions for configuring the SNMP agent for each supported operating system:

- Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems
- Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux
- Configuring the SNMP Agent on Systems Running Supported SUSE Linux Enterprise Server Operating Systems

Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems

Server Administrator uses the SNMP services provided by the Windows SNMP agent. You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as IT Assistant, perform the procedures described in the following sections.

NOTE: See your operating system documentation for additional details on SNMP configuration.

Enabling SNMP Access By Remote Hosts

Windows Server 2003, by default, does not accept SNMP packets from remote hosts. For systems running Windows Server 2003, you must configure the SNMP service to accept SNMP packets from remote hosts if you plan to manage the system by using SNMP management applications from remote hosts.

To enable a system running the Windows Server 2003 operating system to receive SNMP packets from a remote host, perform the following steps:

1. Click the **Start** button, right-click **My Computer**, and point to **Manage**.

   The **Computer Management** window appears.

2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon and click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and then click **Properties**.

   The **SNMP Service Properties** window appears.

5. Click the **Security** tab.
6. Select **Accept SNMP packets from any host**, or add the remote host to the **Accept SNMP packets from these hosts** list.

Changing the SNMP Community Name

Configuring the SNMP community names determines which systems are able to manage your system through SNMP. The SNMP community name used by management applications must match an SNMP community name configured on the Server Administrator system so that the management applications can retrieve management information from Server Administrator.

1. If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer,** and point to **Manage**. If your system is running Windows 2000, right-click **My Computer** and point to **Manage**.

   The **Computer Management** window appears.

2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon and click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and then click **Properties**.

   The **SNMP Service Properties** window appears.

5 Click the **Security** tab to add or edit a community name.

   a To add a community name, click **Add** under the **Accepted Community Names** list.

   The **SNMP Service Configuration** window appears.

   b Type the community name of a system that is able to manage your system (the default is public) in the **Community Name** text box and click **Add**.

   The **SNMP Service Properties** window appears.

   c To change a community name, select a community name in the **Accepted Community Names** list and click **Edit**.

   The **SNMP Service Configuration** window appears.

   d Make all necessary edits to the community name of the system that is able to manage your system in the **Community Name** text box, and then click **OK**.

   The **SNMP Service Properties** window appears**.**

6 Click **OK** to save the changes.

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the Server Administrator system to change Server Administrator attributes using IT Assistant.

1 If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer,** and point to **Manage**. If your system is running Windows 2000, right-click **My Computer** and point to **Manage**.

   The **Computer Management** window appears.

2 Expand the **Computer Management** icon in the window, if necessary.

3 Expand the **Services and Applications** icon, and then click **Services**.

4 Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and click **Properties.**

   The **SNMP Service Properties** window appears.

5 Click the **Security** tab to change the access rights for a community.

6 Select a community name in the **Accepted Community Names** list, and then click **Edit**.

   The **SNMP Service Configuration** window appears.

7 Set the **Community Rights** to **READ WRITE** or **READ CREATE**, and click **OK**.

   The **SNMP Service Properties** window appears.

8 Click **OK** to save the changes.

Configuring Your System to Send SNMP Traps to a Management Station

Server Administrator generates SNMP traps in response to changes in the status of sensors and other monitored parameters. You must configure one or more trap destinations on the Server Administrator system for SNMP traps to be sent to a management station.

1. If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer,** and point to **Manage**. If your system is running Windows 2000, right-click **My Computer** and point to **Manage**.

   The **Computer Management** window appears.

2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon and click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and click **Properties**.

   The **SNMP Service Properties** window appears.

5. Click the **Traps** tab to add a community for traps or to add a trap destination for a trap community.
   a. To add a community for traps, type the community name in the **Community Name** box and click **Add to list**, which is located next to the **Community Name** box.
   b. To add a trap destination for a trap community, select the community name from the **Community Name** drop-down box and click **Add** under the **Trap Destinations** box.
   c. The **SNMP Service Configuration** window appears.

      Type in the trap destination and click **Add**.

      The **SNMP Service Properties** window appears.
6. Click **OK** to save the changes.

Configuring the SNMP Agent on Systems Running Supported Red Hat Enterprise Linux

Server Administrator uses the SNMP services provided by the ucd-snmp or net-snmp SNMP agent. You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as IT Assistant, perform the procedures described in the following sections.

NOTE: See your operating system documentation for additional details on SNMP configuration.

SNMP Agent Access Control Configuration

The management information base (MIB) branch implemented by Server Administrator is identified by the 1.3.6.1.4.1.674 OID. Management applications must have access to this branch of the MIB tree to manage systems running Server Administrator.

For Red Hat Enterprise Linux operating systems, the default SNMP agent configuration gives read-only access for the "public" community only to the MIB-II "system" branch (identified by the 1.3.6.1.2.1.1 OID) of the MIB tree. This configuration does not allow management applications to retrieve or change Server Administrator or other systems management information outside of the MIB-II "system" branch.

Server Administrator SNMP Agent Install Actions

If Server Administrator detects the default SNMP configuration during installation, it attempts to modify the SNMP agent configuration to give read-only access to the entire MIB tree for the "public" community. Server Administrator modifies the **/etc/snmp/snmpd.conf** SNMP agent configuration file in two ways.

The first change is to create a view to the entire MIB tree by adding the following line if it does not exist:

```
view all included .1
```

The second change is to modify the default "access" line to give read-only access to the entire MIB tree for the "public" community. Server Administrator looks for the following line:

```
access notConfigGroup "" any noauth exact systemview none none
```

If Server Administrator finds the line above, it modifies the line so that it reads:

```
access notConfigGroup "" any noauth exact all none none
```

These changes to the default SNMP agent configuration give read-only access to the entire MIB tree for the "public" community.

NOTE: To ensure that Server Administrator is able to modify the SNMP agent configuration to provide proper access to systems management data, it is recommended that any other SNMP agent configuration changes be made after installing Server Administrator.

Server Administrator SNMP communicates with the SNMP agent using the SNMP Multiplexing (SMUX) protocol. When Server Administrator SNMP connects to the SNMP agent, it sends an object identifier to the SNMP agent to identify itself as a SMUX peer. Because that object identifier must be configured with the SNMP agent, Server Administrator adds the following line to the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, during installation if it does not exist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Changing the SNMP Community Name

Configuring the SNMP community names determines which systems are able to manage your system through SNMP. The SNMP community name used by management applications must match an SNMP community name configured on the Server Administrator system so that the management applications can retrieve management information from Server Administrator.

To change the SNMP community name used for retrieving management information from a system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   com2sec publicsec default public
   ```

   or

   ```
   com2sec notConfigUser default public
   ```

2. Edit this line, replacing `public` with the new SNMP community name. When edited, the new line should read:

   ```
   com2sec publicsec default community_name
   ```

   or

   ```
   com2sec notConfigUser default community_name
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   service snmpd restart
   ```

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the system running Server Administrator in order to change Server Administrator attributes using IT Assistant.

To enable SNMP Set operations on the system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   access publicgroup "" any noauth exact all none none
   ```

   or

   ```
   access notConfigGroup "" any noauth exact all none none
   ```

2. Edit this line, replacing the first `none` with `all`. When edited, the new line should read:

   ```
   access publicgroup "" any noauth exact all all none
   ```

   or

   ```
   access notConfigGroup "" any noauth exact all all none
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   service snmpd restart
   ```

Configuring Your System to Send Traps to a Management Station

Server Administrator generates SNMP traps in response to changes in the status of sensors and other monitored parameters. One or more trap destinations must be configured on the system running Server Administrator for SNMP traps to be sent to a management station.

To configure your system running Server Administrator to send traps to a management station, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Add the following line to the file:

   ```
   trapsink IP_address community_name
   ```

   where *IP_address* is the IP address of the management station and *community_name* is the SNMP community name

2. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   service snmpd restart
   ```

Configuring the SNMP Agent on Systems Running Supported SUSE Linux Enterprise Server Operating Systems

Server Administrator uses the SNMP services provided by the ucd-snmp or net-snmp agent. You can configure the SNMP agent to enable SNMP access from remote hosts, change the community name, enable Set operations, and send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as IT Assistant, perform the procedures described in the following sections.

NOTE: On SUSE Linux Enterprise Server (Version 9), the SNMP agent configuration file is located at **/etc/snmpd.conf**. On SUSE Linux Enterprise Server (Version 10), the SNMP agent configuration file is located at **/etc/snmp/snmpd.conf**.

NOTE: See your operating system documentation for additional details about SNMP configuration.

Sever Administrator SNMP Install Actions

Server Administrator SNMP communicates with the SNMP agent using the SNMP Multiplexing (SMUX) protocol. When Server Administrator SNMP connects to the SNMP agent, it sends an object identifier to the SNMP agent to identify itself as a SMUX peer. This object identifier must be configured with the SNMP agent, therefore, Server Administrator adds the following line to the SNMP agent configuration file (**/etc/snmpd.conf** or **/etc/snmp/snmpd.conf**) during installation if it does not exist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Enabling SNMP Access From Remote Hosts

The default SNMP agent configuration on SUSE Linux Enterprise Server operating systems gives read-only access to the entire MIB tree for the "public" community from the local host only. This configuration does not allow SNMP management applications such as IT Assistant running on other hosts to discover and manage Server Administrator systems properly. If Server Administrator detects this configuration during

installation, it logs a message to the operating system log file, **/var/log/messages**, to indicate that SNMP access is restricted to the local host. You must configure the SNMP agent to enable SNMP access from remote hosts if you plan to manage the system by using SNMP management applications from remote hosts.

NOTE: For security reasons, it is advisable to restrict SNMP access to specific remote hosts if possible.

To enable SNMP access from a specific remote host to a system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmpd.conf** or **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit or copy this line, replacing 127.0.0.1 with the remote host IP address. When edited, the new line should read:

   ```
   rocommunity public IP_address
   ```

   NOTE: You can enable SNMP access from multiple specific remote hosts by adding a `rocommunity` directive for each remote host.

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

To enable SNMP access from all remote hosts to a system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmpd.conf** or **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit this line by deleting 127.0.0.1. When edited, the new line should read:

   ```
   rocommunity public
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

Changing the SNMP Community Name

Configuring the SNMP community name determines which management stations are able to manage your system through SNMP. The SNMP community name used by management applications must match the SNMP community name configured on the Server Administrator system, so the management applications can retrieve the management information from Server Administrator.

To change the default SNMP community name used for retrieving management information from a system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmpd.conf** or **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit this line by replacing `public` with the new SNMP community name. When edited, the new line should read:

   ```
   rocommunity community_name 127.0.0.1
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the system running Server Administrator in order to change Server Administrator attributes using IT Assistant. To enable remote shutdown of a system from IT Assistant, SNMP Set operations must be enabled.

NOTE: Rebooting of your system for change management functionality does not require SNMP Set operations.

To enable SNMP Set operations on a system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmpd.conf** or **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Find the line that reads:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edit this line by replacing `rocommunity` with `rwcommunity`. When edited, the new line should read:

   ```
   rwcommunity public 127.0.0.1
   ```

3. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

Configuring Your System to Send Traps to a Management Station

Server Administrator generates SNMP traps in response to changes in the status of sensors and other monitored parameters. One or more trap destinations must be configured on the system running Server Administrator for SNMP traps to be sent to a management station.

To configure your system running Server Administrator to send traps to a management station, edit the SNMP agent configuration file, **/etc/snmpd.conf** or **/etc/snmp/snmpd.conf**, and perform the following steps:

1. Add the following line to the file:

   ```
   trapsink IP_address community_name
   ```

   where `IP_address` is the IP address of the management station and `community_name` is the SNMP community name.

2. To enable SNMP configuration changes, restart the SNMP agent by typing:

   ```
   /etc/init.d/snmpd restart
   ```

X.509 Certificate Management Prerequisites

Web certificates are necessary to ensure the identity of a remote system and to ensure that information exchanged with the remote system cannot be viewed or changed by others.

This section explains the administrative prerequisites for ensuring your ability to generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from Certification Authority (CA) on each supported operating system.

The X.509 certificate management is provided through the Server Administrator home page for all supported operating systems.

Firewall Configuration on Systems Running Supported Red Hat Enterprise Linux Operating Systems

If you enable firewall security when installing Red Hat Enterprise Linux, the SNMP port on all external network interfaces is closed by default. To enable SNMP management applications such as IT Assistant to discover and retrieve information from Server Administrator, the SNMP port on at least one external network interface must be open. If Server Administrator detects that the SNMP port is not open in the firewall for any external network interface, Server Administrator displays a warning message and logs a message to the system log.

You can open the SNMP port by disabling the firewall, opening an entire external network interface in the firewall, or opening the SNMP port for at least one external network interface in the firewall. You can perform this action before or after Server Administrator is started.

To open the SNMP port using one of the previously described methods, perform the following steps:

1. At the Red Hat Enterprise Linux command prompt, type `setup` and press <Enter> to start the Text Mode Setup Utility.

   NOTE: This command is available only if you have performed a default installation of the operating system.

   The **Choose a Tool** menu appears.

2. Select **Firewall Configuration** using the down arrow and press <Enter>.

   The **Firewall Configuration** screen appears.

3 Press <Tab> to select **Security Level** and then press the spacebar to select the security level you want to set. The selected Security Level is indicated by an asterisk.

NOTE: Press <F1> for more information about the firewall security levels. The default SNMP port number is 161. If you are using the X Window System graphical user interface, pressing <F1> may not provide information about firewall security levels on newer versions of Red Hat Enterprise Linux.

a To disable the firewall, select **No firewall** or **Disabled** and go to step 7.

b To open an entire network interface or the SNMP port, select **High, Medium,** or **Enabled** and continue with step 4.

4 Press <Tab> to go to **Customize** and press <Enter>.

The **Firewall Configuration - Customize** screen appears.

5 Select whether to open an entire network interface or just the SNMP port on all network interfaces.

a To open an entire network interface, press <Tab> to go to one of the Trusted Devices and press the spacebar. An asterisk in the box to the left of the device name indicates that the entire interface will be opened.

b To open the SNMP port on all network interfaces, press <Tab> to go to **Other ports** and type `snmp:udp`.

6 Press <Tab> to select **OK** and press <Enter>.

The **Firewall Configuration** screen appears.

7 Press <Tab> to select **OK** and press <Enter>.

The **Choose a Tool** menu appears.

8 Press <Tab> to select **Quit** and press <Enter>.

4

Installing Server Administrator

Overview

You can install Server Administrator using several methods. The *Dell™ Installation and Server Management* CD provides a setup program to install, upgrade, and uninstall Server Administrator and other managed system software components on your managed system. The *Dell Systems Management Consoles* CD provides a setup program to install, upgrade, and uninstall management station software components on your management station. Additionally, you can install Server Administrator on multiple systems through an unattended installation across a network. Dell OpenManage™ products are installed using the install process native to the operating system. Follow the configuration wizard to set up Server Administrator. For details, see the *Dell OpenManage Installation and Security User's Guide*.

Dell Installation and Server Management CD

The *Dell Installation and Server Management* CD provides a setup program to install, upgrade, and uninstall Server Administrator and other managed system software components on your managed system. Additionally, you can install Server Administrator on multiple systems through an unattended installation across a network.

Using the setup program on the *Dell Installation and Server Management* CD, you can install and upgrade Server Administrator on systems running all supported operating systems. On systems running supported Microsoft® Windows®, Red Hat® Enterprise Linux, and SUSE® Linux Enterprise Server operating systems, you can uninstall Server Administrator with the *Dell Installation and Server Management* CD or through the operating system. See the *Dell OpenManage Installation and Security User's Guide* for more details.

NOTE: On installing or uninstalling Server Administrator on Dell PowerEdge 4600, you must reboot the system for the changes to take effect.

Unattended and Silent Installation

You can use the *Dell Installation and Server Management* CD to perform an unattended installation and uninstallation of Server Administrator on systems running supported Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems. Additionally, you can install and uninstall Server Administrator from the command line on systems running supported Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.

Upgrading Server Administrator

Dell OpenManage software allows you to upgrade from versions 4.3 or later to version 5.1. Before the upgrade, you must uninstall the earlier version of Server Administrator and then install the latest version using the *Dell Installation and Server Management* CD.

NOTE: Service Pack upgrade is not supported in Dell OpenManage 5.1.

NOTE: If you have a version of Dell OpenManage earlier than 4.3, upgrade to version 4.3 and then install Dell OpenManage 5.1. For more information see the *Dell OpenManage Installation and Security User's Guide*.

To upgrade from 4.*x* (where *x* is >=3) to Dell OpenManage 5.1 use **setup.exe** or type:

```
msiexec /i SysMgmt.msi /qn
```

(for fresh installs or major upgrades. For example, upgrading from Dell OpenManage version 4.3 to version 5.1.)

For minor upgrades, for example, upgrading from Dell OpenManage version 4.3 to version 4.4, type

```
msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus /qn
```

Upgrading the MSI Engine

Dell OpenManage software allows you to upgrade the MSI engine while doing interactive installs. For silent installs, you have to add appropriate command to the install scripts.

Use the following command in your deployment script to upgrade the MSI engine (if required) and to install/upgrade the systems management software.

NOTE: Dell OpenManage systems management and Management Station installers require MSI 3.1 or later. Update the MSI engine if you are using a system running Windows Server™ 2003 (without a Service Pack), Windows 2000 Server, or Windows XP operating system. If you are using a system running Windows Server 2003 SP1 or Windows Server 2003 x64 operating system, you do not have to update the MSI engine.

```
:retry
start /wait msiexec /i SysMgmt.msi /qn
if %errorlevel% == 1613 (
REM UPGRADE THE WINDOWS INSTALLER ENGINE
start /wait WindowsInstaller-KB893803-v2-x86.exe /quiet /norestart
goto retry
)
if %errorlevel% == 1638 (
REM THIS IS A MINOR UPGRADE
start /wait msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus/qn
)
```

See the *Dell OpenManage Installation and Security User's Guide* for information on installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator in each supported operating system.

Before You Begin

- Read and follow the applicable instructions in "Setup and Administration."
- Read the installation requirements to ensure that your system meets or exceeds the minimum requirements.
- Read the *Dell OpenManage Installation and Security User's Guide* for step-by-step instructions on installing, upgrading, and uninstalling Server Administrator for each supported operating system.
- Read the *Server Administrator Compatibility Guide*. This document contains compatibility information about Server Administrator installation and operation on various hardware platforms (or systems) running supported Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.
- Read the Dell OpenManage Install readme file on the *Dell Installation and Server Management* CD. The file contains the latest information about new features, in addition to information about known issues.
- Read the Server Administrator readme file on the *Dell Installation and Server Management* CD. The file contains the latest information about software, firmware, and driver versions, in addition to information about known issues.
- Read the installation instructions for your operating system.

Installation Requirements

The following sections describe the Server Administrator general requirements. Operating system–specific installation prerequisites are listed as part of the installation procedures.

Supported Operating Systems

Server Administrator supports each of the following operating systems:

- Microsoft Windows 2000 Server family (Intel x86) (includes Windows 2000 Server SP4 and greater, and Windows 2000 Advanced Server SP4 and greater)
- Microsoft Windows Server™ 2003 family (Intel x86) (includes SP1 with Web, Standard, and Enterprise editions) and Microsoft Windows Small Business Server [SBS] 2003 SP1
- Microsoft Windows Server 2003 family (Intel EM64T) (includes SP1 with Standard, and Enterprise editions), Microsoft Windows SBS 2003 SP1, and Microsoft Windows SBS 2003 R2
- Microsoft Windows Server 2003 family (with R2) (includes Standard and Enterprise editions)
- Microsoft Windows Server 2003 (Intel EM64T) R2 (includes Standard and Enterprise editions)
- Microsoft Windows Storage Server 2003 R2 (includes Express, Standard, Workgroup, and Enterprise editions)

- Red Hat Enterprise Linux AS, ES, and WS, (Version 3) (Intel x86) Update 6
- Red Hat Enterprise Linux AS, ES, and WS, (Version 3) (Intel EM64T) Update 6
- Red Hat Enterprise Linux AS, ES, and WS, (Version 4) (Intel x86)
- Red Hat Enterprise Linux AS, ES, and WS, (Version 4) (Intel EM64T)

  NOTE: Support for updated kernels released by Red Hat and for later versions of Red Hat Enterprise Linux may require the use of Dynamic Kernel Support (see the *Installation and Security User's Guide* for an explanation of this feature).
- SUSE Linux Enterprise Server (Version 9) (SP3 for Intel EM64T)
- SUSE Linux Enterprise Server (Version 10) (Intel EM64T)

NOTE: See the Server Administrator readme file on the *Dell Installation and Server Management* CD or the *Compatibility Guide* on the *Product Documentation* CD for the latest detailed list of the Server Administrator Services that are supported on each supported operating system.

System Requirements

Server Administrator must be installed on each system to be managed. You can then manage each system running Server Administrator locally or remotely through a supported Web browser.

The Prerequisite Checker (**setup.exe**) on the *Dell Installation and Server Management* CD will automatically analyze your system to determine if the system requirements have been met. For more information, see "Prerequisite Checker for Windows."

Managed System Requirements

- One of the "Supported Operating Systems."
- A minimum of 128 MB of RAM.
- A minimum of 256 MB of free hard-drive space.
- Administrator rights.
- A TCP/IP connection on the monitored system and the remote system to facilitate remote system management.
- One of the "Supported Web Browsers."
- One of the supported systems management protocol standards.
- A mouse, keyboard, and monitor to manage a system locally. The monitor requires a minimum screen resolution of 800 x 600. The recommended screen resolution setting is 1024 x 768.

- The Server Administrator Remote Access Service requires a Dell Remote Access Controller (DRAC) to be installed on the system to be managed. See "Remote Access Service" and the "Other Documents You Might Need" for appropriate Dell Remote Access Controller User's Guides for complete software and hardware requirements.

  NOTE: The DRAC software is installed as part of the **Typical Setup** and **Custom Setup** installation options when installing managed system software from the *Dell Installation and Server Management* CD, provided that the managed system meets all of the DRAC installation prerequisites. See "Remote Access Service" and the "Other Documents You Might Need" for appropriate Dell Remote Access Controller User's Guides for complete software and hardware requirements.

- The Storage Management Service is installed by default on systems running supported Windows operating systems, by using **Typical Setup**.

  NOTE: On Red Hat Enterprise Linux and SUSE Linux Enterprise Server systems, you can either install the Storage Management Service through the Red Hat Package Manager (RPM) or use the `srvadmin-install.sh` script—a menu driven script that installs the appropriate RPMs based on the options you choose

Remote Management System Requirements

- One of the "Supported Web Browsers" to manage a system remotely from the Server Administrator home page.
- A TCP/IP connection on the managed system and the remote system to facilitate remote system management.
- A minimum screen resolution of 800 x 600. The recommended screen resolution setting is 1024 x 768.

Supported Web Browsers

A supported Web browser is required to manage a system locally from the Server Administrator home page. Supported browsers are:

- Internet Explorer 6.0 SP2
- Mozilla Firefox 1.5 (SUSE Linux Enterprise Server and Red Hat Enterprise Linux)
- Mozilla 1.7.11 (SUSE Linux Enterprise Server and Red Hat Enterprise Linux)

Supported Systems Management Protocol Standards

A supported systems management protocol standard must be installed on the managed system before installing Server Administrator. On supported Microsoft Windows operating systems, Server Administrator supports these two systems management standards: Common Information Model/Windows Management Instrumentation (CIM/WMI) and Simple Network Management Protocol (SNMP). On supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator supports the SNMP systems management standard.

NOTE: For information about installing a supported systems management protocol standard on your managed system, see your operating system documentation.

Table 4-1 shows the availability of the systems management standards for each supported operating system.

Table 4-1. Availability of Systems Management Protocol by Operating Systems

Operating System	SNMP	CIM/WMI
Supported Microsoft Windows operating systems	Available from the operating system installation media.	Always installed.
Supported Red Hat Enterprise Linux operating systems	You must install the SNMP package provided with the operating system.	Unavailable.
SUSE® Linux Enterprise Server operating systems	You must install the SNMP package provided with the operating system.	Unavailable.

Prerequisite Checker for Windows

The **setup.exe** prerequisite checker program, located in the Windows directory on the *Dell Installation and Server Management* CD, provides the capability of examining the prerequisite status for software components without launching the actual installation. This program displays a status window that provides information about the system hardware that some software components may require for operation.

The Prerequisite Check can be executed silently using **runprereqcheck.exe /s**.

Installation Procedures

See the *Dell OpenManage Installation and Security User's Guide* for information on installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator on each supported operating system.

Installing Server Administrator with Citrix

If you want to install Server Administrator with Citrix, you must perform the installation in the following order:

1. Install the operating system using the *Dell Installation and Server Management CD*.

   NOTE: Do not install Server Administrator or other system management software, until you have installed the Citrix software.

2. Install the Citrix software. See your Citrix documentation for complete information about installing and configuring the Citrix software.
3. Install Server Administrator using the *Dell Installation and Server Management CD*.

All applications (including Server Administrator) work properly if installed **after** installing Citrix. Citrix remaps all your hard drive letters when installed.

For example, if you install Server Administrator on drive C: and then install Citrix, it will change your drive letter C: to M:. This results in Server Administrator not working properly if you install Citrix after installing Server Administrator. You can repair Server Administrator by typing:
`msiexec.exe /fa SysMgmt.msi`

Considerations Before Installing Storage Management Service

Storage Management is integrated with Server Administrator. The Dell OpenManage Storage Management is a replacement for Array Manager.

If you install the Storage Management Service 2.0, any previous installation of Storage Management Service will be uninstalled.

PERC Console and FAST Compatibility Issues When Installing the Storage Management Service

Installing Storage Management on a system that has FAST or the PERC Console installed is an unsupported configuration. In particular, you may find that the Storage Management Service or the FAST features are disabled at run time when using the Storage Management Service on a system that also has FAST installed. Therefore, it is recommended that you uninstall FAST and the PERC Console before installing the Storage Management Service.

Dell OpenManage Storage Management replaces all storage management features provided by FAST and the PERC Console. In addition, the Storage Management Service has features not provided by FAST and the PERC Console.

Compatibility With Linux Utilities When Installing the Storage Management Service

It is recommended that you do not install the Storage Management Service on a Linux system that has RAID storage management utilities provided by Dell or other vendors. You should uninstall these utilities before installing the Storage Management Service. The Storage Management Service replaces the storage management features provided by these utilities. Examples of the Linux utilities provided by Dell or other vendors include:

- LinFlash
- DellMgr
- DellMON
- LINLib
- MegaMgr
- MegaMON

Prerequisite Drivers and Firmware on Linux and the Storage Management Service

On Linux, the Storage Management installation is unable to detect whether the drivers and firmware on the system are at the required level for installing and using Storage Management. When installing on Linux, you will be able to complete the installation regardless of whether the driver and firmware versions meet the required level. However, if the driver and firmware versions do not meet the required

level, you may not have access to all functions provided by the Storage Management. At the Storage Management Service runtime, check your application log files for notifications on outdated firmware versions. See the Storage Management readme (readme_sm.txt) for a complete listing of supported controller firmware and driver versions.

Filesystem Hierarchy Standard v2.3 Support

File Hierarchy System (FHS) is a component of the larger Linux Standards Base definition. In this release, Server Administrator supports the relocation of files.

A typical install places all files in: **/opt/dell/srvadmin**

The corresponding directories that are affected:

- Shareable (static) files in: **/opt/dell/srvadmin**
- Host specific files (user modifiable): **/etc/opt/dell/srvadmin** and **/etc/opt//srvadmin**
- Dynamic (log) files: **/var/tmp/dell/srvadmin**, **/var/tmp//srvadmin**, and **/var/log/dell/srvadmin** **/var/log//srvadmin**

For more information, see the *Dell OpenManage Installation and Security User's Guide*.

5

Using Server Administrator

Starting Your Server Administrator Session

To start a Server Administrator session in a local system, click the **Dell OpenManage™ Server Administrator** icon on your desktop.

To start a Server Administrator session on a remote system, open your Web browser and type one of the following in the address field and press <Enter>:

`https://hostname:1311`

where `hostname` is the assigned name for the managed node system and `1311` is the default port number

or

`https://IP address:1311`

where `IP address` is the IP address for the managed system and `1311` is the default port number

The Server Administrator **Log in** window appears.

NOTE: Type `https://` (and not `http://`) in the address field to receive a valid response in your browser.

NOTE: The default port for Dell OpenManage Server Administrator is 1311. You can change the port, if necessary. See "Secure Port Server and Security Setup" for instructions on setting up your system preferences.

Logging In and Out

To log into Server Administrator, type your preassigned **Username** and **Password** in the appropriate fields on the Systems Management **Log in** window. See "Single Sign-On" for information on how you can bypass the login page and access the Server Administrator Web application by clicking on the **Dell OpenManage Server Administrator** icon on your desktop.

NOTE: You must have preassigned user rights to log into Server Administrator. See "Setup and Administration" for instructions on setting up new users.

If you are accessing Server Administrator from a defined domain, you will also need to specify the correct **Domain** name.

NOTE: The **Application** drop-down menu will appear as a non-selectable field for systems that can only access one Dell OpenManage Server Administrator component. The drop-down menu is only functional when two or more Dell OpenManage Server Administrator components are available on the managed system.

Select the **Active Directory Login** check box to log in using Microsoft® Active Directory.

To end your Server Administrator session, click **Log Out** on the "global navigation bar." The **Log Out** button is located in the upper-right corner of each Server Administrator home page.

Single Sign-On

The Single Sign-On option in Microsoft Windows® enables all logged-in users to bypass the login page and access the Server Administrator Web application by clicking the **Dell OpenManage Server Administrator** icon on your desktop.

NOTE: See the Knowledge Base article at **support.microsoft.com/default.aspx?scid=kb;en-us;Q258063** for more information.

For local machine access, you must have an account on the machine with the appropriate privileges (User, Power User, or Administrator). Other users are authenticated against the Microsoft Active Directory.

To launch Server Administrator using Single Sign-On authentication against Microsoft Active Directory, the following parameters must also be passed in:

```
authType=ntlm&application=[plugin name]
```

Where *plugin name* = *omsa*, *ita*, etc.

For example:

```
https://localhost:1311/?authType=ntlm&application=omsa
```

To launch Server Administrator using Single Sign-On authentication against the local machine user accounts, the following parameters must also be passed in:

```
authType=ntlm&application=[plugin name]&locallogin=true
```

Where *plugin name* = *omsa*, *ita*, etc.

For example:

```
https://localhost:1311/?authType=ntlm&application=omsa&locallogin=true
```

Server Administrator has also been extended to allow other products (such as Dell OpenManage IT Assistant) to directly access Server Administrator Web pages without going through the login page (if you are currently logged in and have the appropriate privileges).

Systems Running a Supported Microsoft Windows Server™ 2003 Operating System

You must configure the security settings for your browser to log into Server Administrator from a remote management system that is running a supported Microsoft Windows Server 2003 operating system.

The security settings for your browser might prevent the execution of client-side scripts that are used by Server Administrator. To enable the use of client-side scripting, perform the following steps on the remote management system.

NOTE: If you have not configured your browser to enable the use of client-side scripting, you might receive a blank screen when logging into Server Administrator. In this case, an error message will appear instructing you to configure your browser settings.

Internet Explorer

1. Start your browser.
2. Click **Tools**→ **Internet Options**→ **Security**.
3. Click the **Trusted Sites** icon.
4. Click **Sites**.
5. Copy the Web address used to access the remote managed system from the browser's address bar and paste it onto the **Add this Web Site to the Zone** field.
6. Click **Custom Level**.

   For Windows 2000:

   - Under **Miscellaneous**, select the **Allow Meta Refresh** radio button.
   - Under **Active Scripting**, select the **Enable** radio button.

   For Windows 2003:

   - Under **Miscellaneous**, select the **Allow Meta Refresh** radio button.
   - Under **Active Scripting**, select the **Enable** radio button.
   - Under **Active Scripting**, select the **Allow scripting of Internet Explorer web browser controls** radio button.
7. Click **OK** to save the new settings.
8. Close the browser.
9. Log into Server Administrator.

To allow Single Sign-On for Server Administrator without prompts for user credentials, perform the following steps:

1. Start your browser.
2. Click **Tools**→ **Internet Options**→ **Security**.
3. Click the **Trusted Sites** icon.
4. Click **Sites**.

5 Copy the Web address used to access the remote managed system from the browser's address bar and paste it onto the **Add this Web Site to the Zone** field.

6 Click **Custom Level**.

7 Under **User Authentication**, select the **Automatic Logon with current username and password** radio button.

8 Click **OK** to save the new settings.

9 Close the browser.

10 Log into Server Administrator.

Mozilla

1 Start your browser.

2 Click **Edit→ Preferences**.

3 Click **Advanced→ Scripts and Plugins.**

4 Ensure that the **Navigator** check box is selected under **Enable JavaScript for**.

5 Click **OK** to save the new settings.

6 Close the browser.

7 Log into Server Administrator.

The Server Administrator Home Page

NOTE: Do not use your Web browser toolbar buttons (such as **Back** and **Refresh**) while using Server Administrator. Use only the Server Administrator navigation tools.

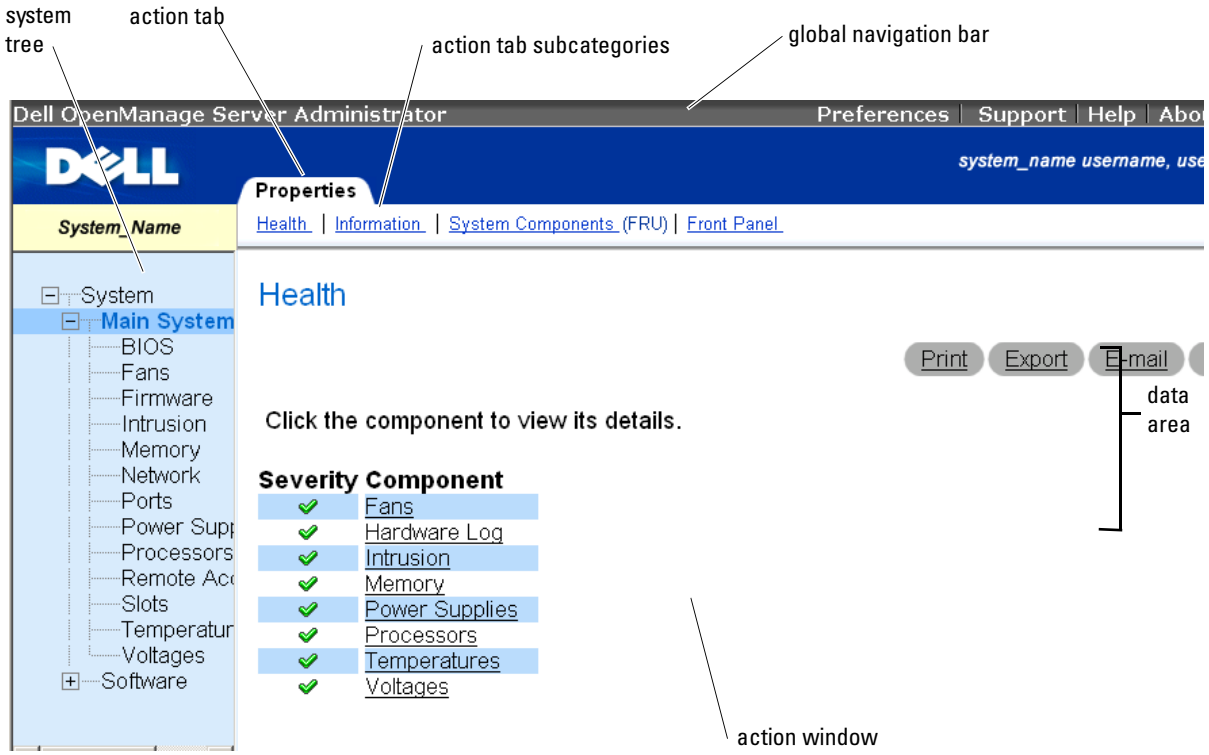
With only a few exceptions, the Server Administrator home page has three main areas:

- The global navigation bar provides links to general services.
- The system tree displays all visible system objects based on the user's access privileges.
- The action window displays the available management actions for the selected system tree object based on the user's access privileges. The action window contains three functional areas:
  - The action tabs display the primary actions or categories of actions that are available for the selected object based on the user's access privileges.
  - The action tabs are divided into subcategories of all available secondary options for the action tabs based on the user's access privileges.
  - The data area displays information for the selected system tree object, action tab, and subcategory based on the user's access privileges.

Additionally, when logged into the Server Administrator home page, the system model, the assigned name of the system, and the current user's user name and user privileges are displayed in the top-right corner of the window.

Figure 5-1 shows a sample Server Administrator home page layout for a user logged in with administrator privileges.

Figure 5-1. Sample Server Administrator Home Page



Clicking an object in the system tree opens a corresponding action window for that object. You can navigate in the action window by clicking action tabs to select major categories and clicking the action tab subcategories to access more detailed information or more focused actions. The information displayed in the data area of the action window can range from system logs to status indicators to system probe gauges. Underlined items in the data area of the action window indicate a further level of functionality. Clicking an underlined item creates a new data area in the action window that contains a greater level of detail. For example, clicking **Main System Chassis** under the **Health** subcategory of the **Properties** action tab lists the health status of all the components contained in the Main System Chassis object that are monitored for health status.

NOTE: Many of the system tree objects, system components, action tabs, or data area features are not available to users logged in with only User privileges. Admin or Power User privileges are required to view many of the system tree objects, system components, action tabs, and data area features that are configurable. Additionally, only users logged in with Admin privileges have access to the shutdown functionality included under the **Shutdown** tab.

Global Navigation Bar

The global navigation bar and its links are available to all user levels regardless of where you are in the program.

- Clicking **Preferences** opens the **Preferences** home page. See "Using the Preferences Home Page."
- Clicking **Support** connects you to the Dell™ Support website.
- Clicking **Help** opens the context-sensitive online help window. See "Using the Online Help."
- Clicking **About** displays Server Administrator version and copyright information.
- Clicking **Log Out** ends your current Server Administrator program session.

System Tree

The system tree appears on the left side of the Server Administrator home page and lists the components of your system that are viewable. The system components are categorized by component type. When you expand the main object known as **System**, the major categories of system components that may appear are **Main System Chassis**, **Software**, and **Storage**.

To expand a branch of the tree, click the plus sign () to the left of an object, or double-click the object. A minus sign () indicates an expanded entry that cannot be expanded further.

Action Window

When you click an item on the system tree, details about the component or object appear in the data area of the action window. Clicking an action tab displays all available user options as a list of subcategories.

Clicking an object on the system tree opens that component's action window, displaying the available action tabs. The data area defaults to a preselected subcategory of the first action tab for the selected object. The preselected subcategory is usually the first option. For example, clicking the **Main System Chassis** object opens an action window in which the **Properties** action tab and **Health** subcategory is displayed in the window's data area.

Data Area

The data area is located below the action tabs on the right side of the home page. The data area is where you perform tasks or view details about system components. The content of the window depends on the system tree object and action tab that are currently selected. For example, when you select **BIOS** from the system tree, the **Properties** tab is selected by default and the version information for the system BIOS appears in the data area. The data area of the action window contains many common features, including status indicators, task buttons, underlined items, and gauge indicators.

System Component Status Indicators

The icons that appear next to component names show the status of that component (as of the latest page refresh).

Table 5-1. System Component Status Indicators

	A green check mark indicates that a component is healthy (normal).
	A yellow triangle containing an exclamation point indicates that a component has a warning (noncritical) condition. A warning condition occurs when a probe or other monitoring tool detects a reading for a component that falls within certain minimum and maximum values. A warning condition requires prompt attention.
	A red X indicates that a component has a critical (failure) condition. A critical condition occurs when a probe or other monitoring tool detects a reading for a component that falls within certain minimum and maximum values. A critical condition requires immediate attention.
	A blank space indicates that a component's health status is unknown.

Task Buttons

Most windows opened from the Server Administrator home page contain at least four task buttons: **Print**, **Export**, **Email**, and **Refresh**. Other task buttons are included on specific Server Administrator windows. Log windows, for example, also contain **Save As** and **Clear Log** task buttons. For specific information about individual task buttons, click **Help** on any Server Administrator home page window to view detailed information about the specific window you are viewing.

- Clicking **Print** prints a copy of the open window to your default printer.
- Clicking **Export** generates a text file that lists the values for each data field on the open window. The export file is saved to a location you specify. See "Setting User and System Preferences" for instructions on customizing the delimiter separating the data field values.
- Clicking **Email** creates an e-mail message addressed to your designated e-mail recipient. See "Setting User and System Preferences" for instructions on setting up your e-mail server and default e-mail recipient.
- Clicking **Refresh** reloads the system component status information in the action window data area.
- Clicking **Save As** saves an HTML file of the action window in a **.zip** file.
- Clicking **Clear Log** erases all events from the log displayed in the action window data area.

NOTE: The **Export**, **Email**, **Save As**, and **Clear Log** buttons are only visible for users logged in with Power User or Admin privileges.

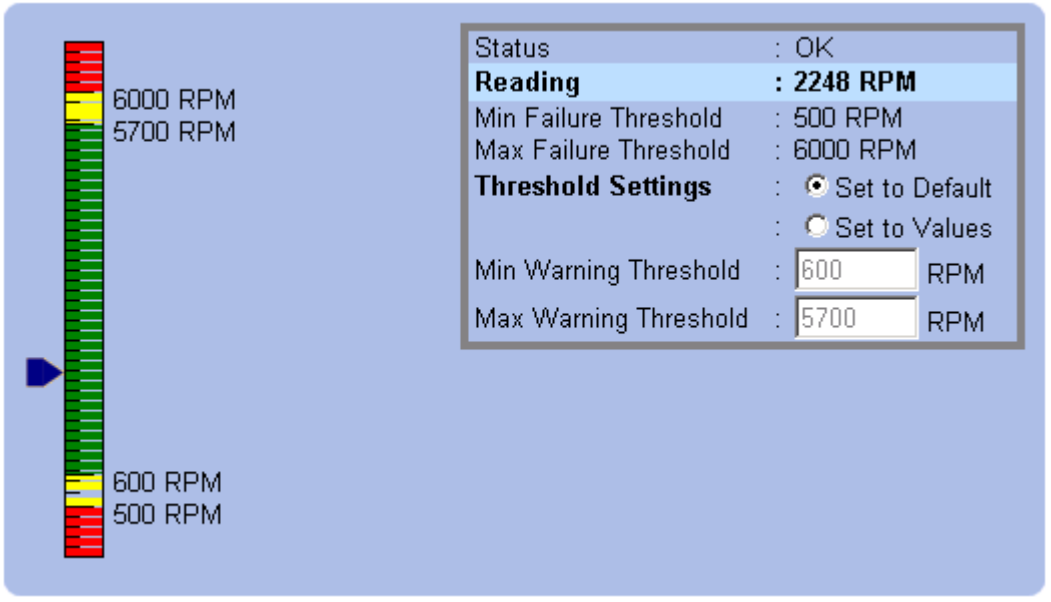
Underlined Items

Clicking an underlined item in the action window data area displays additional details about that item.

Gauge Indicators

Temperature probes, fan probes, and voltage probes are each represented by a gauge indicator. For example, Figure 5-2 shows readings from a system's CPU fan probe.

Figure 5-2. Gauge Indicator



Using the Online Help

Context-sensitive online help is available for every window of the Server Administrator home page. Clicking **Help** on the global navigation bar opens an independent help window that contains detailed information about the specific window you are viewing. The online help is designed to help guide you through the specific actions required to perform all aspects of the Server Administrator services. Online help is available for all windows you can view, based on the software and hardware groups that Server Administrator discovers on your system and your user privilege level.

Using the Preferences Home Page

The Preferences home page defaults to the **Access Configuration** window under the **Preferences** tab.

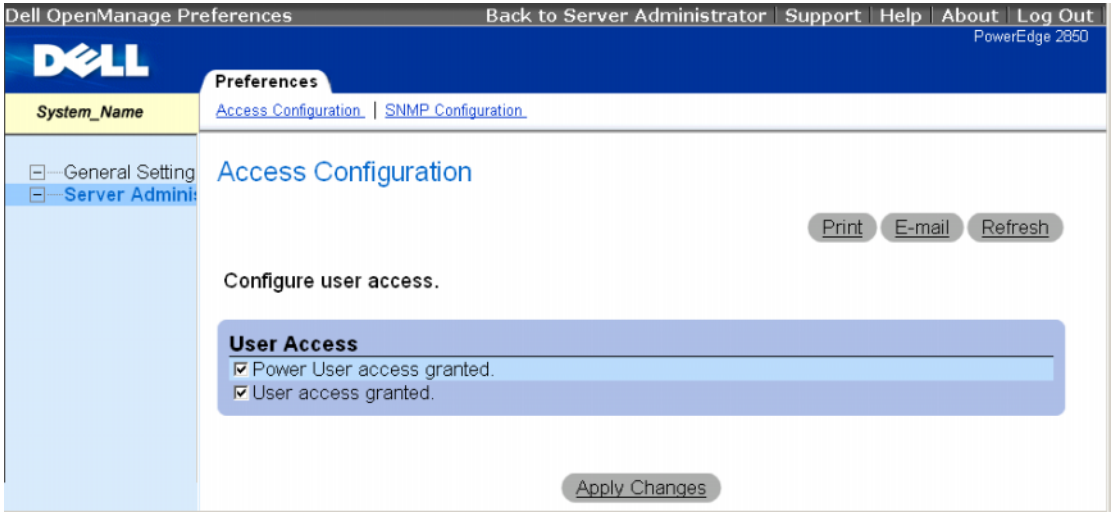
From the Preferences home page you can restrict access to users with User and Power User privileges, set the Simple Network Management Protocol (SNMP) password, and configure user settings and secure port system settings.

Like the Server Administrator home page, the Preferences home page has three main areas:

- The global navigation bar provides links to general services.
  - Clicking **Back to Server Administrator** returns you to the Server Administrator home page.
- The left pane of the Preferences home page (where the system tree is displayed on the Server Administrator home page) displays the preference categories for the managed system.
- The action window displays the available settings and preferences for the managed system.

Figure 5-3 shows a sample Preferences home page layout.

Figure 5-3. Sample Preferences Home Page



Using the Server Administrator Command Line Interface

The Server Administrator command line interface (CLI) allows users to perform essential systems management tasks from the operating system command prompt of a monitored system.

In many cases, the CLI allows a user with a very well-defined task in mind to rapidly retrieve information about the system. Using CLI commands, for example, administrators can write batch programs or scripts to execute at specific times. When these programs execute, they can capture reports on components of interest, such as fan RPMs. With additional scripting, the CLI can be used to capture data during periods of high system usage to compare with the same measurements at times of low system usage. Command results can be routed to a file for later analysis. The reports can help administrators to gain information that can be used to adjust usage patterns, to justify purchasing new system resources, or to focus on the health of a problem component.

For complete instructions on the functionality and use of the CLI, see the *Server Administrator Command Line Interface User's Guide*.

Secure Port Server and Security Setup

This section contains the following topics:

- Setting User and System Preferences
- X.509 Certificate Management

Setting User and System Preferences

You set user and secure port system preferences from the **Preferences** home page.

NOTE: You must be logged in with Admin privileges to set or reset user or system preferences.

Perform the following steps to set up your user preferences:

1. Click **Preferences** on the global navigation bar.

   The **Preferences** home page appears.

2. Click **General Settings**.

3. To add a preselected e-mail recipient, type the e-mail address of your designated service contact in the **Mail To:** field, and click **Apply Changes**.

   NOTE: Clicking **Email** in any window sends an e-mail message with an attached HTML file of the window to the designated e-mail address.

4. To change the home page appearance, select an alternative value in the **skin** or **scheme** fields and click **Apply Changes**.

Perform the following steps to set up your secure port system preferences:

1. Click **Preferences** on the global navigation bar.

   The **Preferences** home page appears.

2. Click **General Settings**, and the **Web Server** tab.

3. In the **Server Preferences** window, set options as necessary.

   - The **Session Timeout** feature can set a limit on the amount of time that a Server Administrator session can remain active. Select the **Enable** radio button to allow Server Administrator to time out if there is no user interaction for a specified number of minutes. Users whose session times out must log in again to continue. Select the **Disable** radio button to disable the Server Administrator session timeout feature.
   - The **HTTPS Port** field specifies the secure port for Server Administrator. The default secure port for Server Administrator is 1311.

   NOTE: Changing the port number to an invalid or in-use port number might prevent other applications or browsers from accessing Server Administrator on the managed system. See the *The Dell OpenManage Installation and Security User's Guide* for the list of default ports.

- The **IP Address to Bind to** field specifies the IP address(es) for the managed system that Server Administrator binds to when starting a session. Select the **All** radio button to bind to all IP addresses applicable for your system. Select the **Specific** radio button to bind to a specific IP address.

NOTE: Changing the **IP Address to Bind to** value to a value other than **All** may prevent other applications or browsers from accessing Server Administrator on the managed system.

- The **SMTP Server name** and **DNS Suffix for SMTP Server** fields specify your company or organization's Simple Mail Transfer Protocol (SMTP) and domain name server (DNS) suffix. To enable Server Administrator to send e-mails, you must type the IP address and DNS suffix for the SMTP Server for your company or organization in the appropriate fields.

NOTE: For security reasons, your company or organization might not allow e-mails to be sent through the SMTP server to outside accounts.

- The **Command Log Size** field specifies the largest file size in MB for the command log file.
- The **Support Link** field specifies the URL for the business entity that provides support for your managed system.
- The **Custom Delimiter** field specifies the character used to separate the data fields in the files created using the **Export** button. The **;** character is the default delimiter. Other options are **!**, **@**, **#**, **$**, **%**, **^** , *****, **~**, **?**, **:**, **|**, and **,**.

4 When you finish setting options in the **Server Preferences** window, click **Apply Changes**.

X.509 Certificate Management

Web certificates are necessary to ensure the identity of a remote system and ensure that information exchanged with the remote system cannot be viewed or changed by others. To ensure system security, it is strongly recommended that you either generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from a Certification Authority (CA).

NOTE: You must be logged in with Admin privileges to perform certificate management.

To manage X.509 certificates through the Preferences home page, click **General Settings**, click the **Web Server** tab, and click **X.509 Certificate**.

Use the X.509 certificate tool to either generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from a CA. Authorized CAs include Verisign, Entrust, and Thawte.

Controlling Server Administrator

Server Administrator automatically starts each time you reboot the managed system. To manually start, stop, or restart Server Administrator, use the following instructions.

NOTE: To control Server Administrator, you must be logged in with administrator privileges (logged in as `root` for supported Red Hat® Enterprise Linux or SUSE® Linux Enterprise Server operating systems).

Starting Server Administrator

Supported Microsoft Windows Operating Systems

To start Server Administrator on systems running a supported Microsoft Windows operating system, perform the following steps:

1. Click the **Start** button and point to **Settings**→ **Control Panel**→ **Administrative Tools**→ **Services**.

   The **Services** window appears.
2. Right-click the **Secure Port Server** icon.
3. Click **Start**.

Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

To start Server Administrator on systems running a supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system, run the following command from the command line:

```
dsm_om_connsvc start
```

Stopping Server Administrator

Supported Microsoft Windows Operating Systems

To stop Server Administrator, perform the following steps:

1. Click the **Start** button and point to **Settings**→ **Control Panel**→ **Administrative Tools**→ **Services**.

   The **Services** window appears.
2. Right-click the **Secure Port Server** icon.
3. Click **Stop**.

Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

To stop Server Administrator on systems running a supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system, run the following command from the command line:

```
dsm_om_connsvc stop
```

Restarting Server Administrator

Supported Microsoft Windows Operating Systems

To restart Server Administrator, perform the following steps:

1. Click the **Start** button and point to **Settings**→ **Control Panel**→ **Administrative Tools**→ **Services**.
   The **Services** window appears.
2. Right-click the **Secure Port Server** icon.
3. Click **Restart**.

Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server Operating Systems

To restart Server Administrator on systems running a supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system, run the following command from the command line:

```
dsm_om_connsvc restart
```

6

Instrumentation Service

Overview

The Server Administrator Instrumentation Service monitors the health of a system and provides rapid access to detailed fault and performance information gathered by industry standard systems management agents. The reporting and viewing features allow retrieval of overall health status for each chassis that comprises your system. At the subsystem level, you can view information about the voltages, temperatures, current, fan rpm, and memory function at key points in the system.
A detailed account of every relevant cost of ownership (COO) detail about your system can be seen in the summary view. Version information for BIOS, firmware, operating system, and all installed systems management software is easy to retrieve.

Additionally, system administrators can use the Instrumentation Service to perform the following essential tasks:

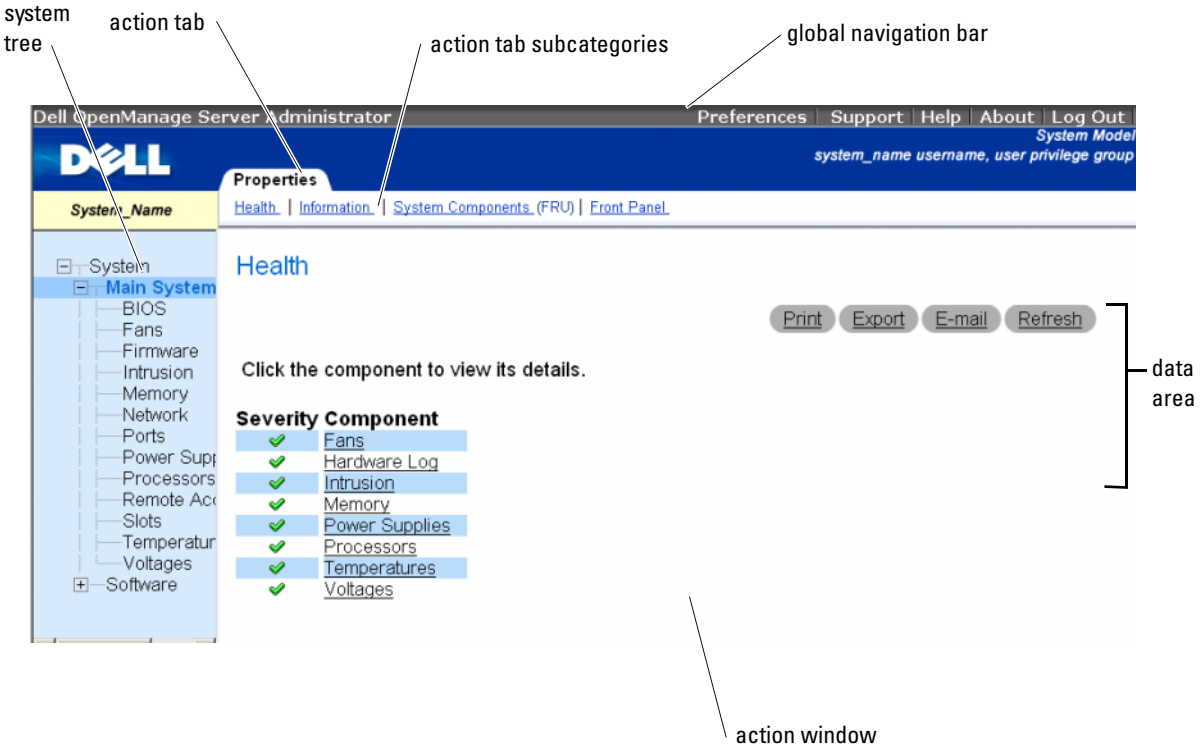
- Specify minimum and maximum values for certain critical components. The values, called thresholds, determine the range in which a warning event for that component occurs (minimum and maximum failure values are specified by the system manufacturer).
- Specify how the system responds when a warning or failure event occurs. Users can configure the actions that a system takes in response to notifications of warning and failure events. Alternatively, users who have around-the-clock monitoring can specify that no action is to be taken and rely on human judgment to select the best action in response to an event.
- Populate all of the user-specifiable values for the system, such as the name of the system, the phone number of the system's primary user, the depreciation method, whether the system is leased or owned, and so on.

NOTE: For both managed systems and network management stations running Microsoft® Windows Server™ 2003, you must configure the Simple Network Management Protocol (SNMP) service to accept SNMP packets. See "Configuring the SNMP Agent for Systems Running Supported Windows Operating Systems" for details.

Managing Your System

The Server Administrator home page defaults to the **System** object of the system tree view. The default for the **System** object opens the **Health** components under the **Properties** tab.

Figure 6-1. Sample Server Administrator Home Page



NOTE: Context-sensitive online help is available for every window of the Server Administrator home page. Clicking **Help** on the global navigation bar opens an independent help window that contains detailed information about the specific window you are viewing. The online help is designed to guide you through the specific actions required to perform all aspects of the Server Administrator services. Online help is available for all windows you can view, based on the software and hardware groups that Server Administrator discovers on your system and your user privilege level.

NOTE: Many of the system tree objects, system components, action tabs, action tab subcategories, or data area features are not available to a user logged in with User privileges. Admin or Power User privileges are required to view many of the system tree objects, system components, action tabs, and data area features that are configurable. Additionally, only users logged in with Admin privileges have access to critical system features such as the shutdown functionality included under the **Shutdown** tab.

The Preferences home page defaults to the **Access Configuration** window under the **Preferences** tab.

From the **Preferences** home page, you can restrict access to users with User and Power User privileges, set the SNMP password, and configure user settings and secure port server settings.

Managing System Tree Objects

The Server Administrator system tree displays all visible system objects based on the software and hardware groups that Server Administrator discovers on the managed system and on the user's access privileges. The system components are categorized by component type. When you expand the main object—**System**—the major categories of system components that may appear are "**Main System Chassis**," "**Software**," and "**Storage**."

If Storage Management Service is installed, depending on the controller and storage attached to the system, the Storage tree object will expand to display the following objects:

- Controller
- Battery
- Connector
- Enclosure or Backplane
- Physical Disks
- EMMs
- Fans
- Power Supplies
- Temperatures
- Virtual Disks
- Firmware/Driver Versions

Server Administrator Home Page System Tree Objects

NOTE: Many of the system tree objects, system components, action tabs, action tab subcategories, or data area features are not available to a user logged in with User privileges. Admin or Power User privileges are required to view many of the system tree objects, system components, action tabs, and data area features that are configurable. Additionally, only users logged in with Admin privileges have access to critical system features such as the shutdown functionality included under the **Shutdown** tab

System

The **System** object contains three main system component groups: "Main System Chassis," "Software," and "Storage." The Server Administrator home page defaults to the **System** object of the system tree view. Most administrative functions can be managed from the **System** object action window. The **System** object action window has the following tabs, depending on the user's group privileges: **Properties**, **Shutdown**, **Logs**, **Alert Management**, **Session Management**, and **Diagnostics**.

NOTE: Update functionality is supported on releases prior to Server Administrator version 2.0. The Dell Server Update Utility and Dell Update Packages can be downloaded from the Dell Support website at **support.dell.com**. These are supported on Microsoft Windows®, Red Hat® Enterprise Linux, and SUSE® Linux Enterprise Server operating systems.

NOTE: The Dell Server Update Utility or Dell Update Packages must be launched from the system you want to update.

Properties

Subtabs: Health | Summary | Asset Information | Auto Recovery

Under the **Properties** tab, you can:

- View the current health alert status for hardware and software components in the **Main System Chassis** object, the attached storage components.
- View detailed summary information for all components in the system being monitored.
- View and configure asset information for the system being monitored.
- View and set the Automatic System Recovery (watchdog timer) actions for the system being monitored.

  NOTE: Automatic System Recovery actions may not execute exactly per the time-out period (n seconds) when the watchdog identifies a system that has stopped responding. The action execution time ranges from *n-h+1* to *n+1* seconds, where *n* is the time-out period and *h* is the heart beat interval. The value of the heart beat interval is 7 seconds when *n* <= 30 and 15 seconds when *n* > 30.

  NOTE: The functionality of the watchdog timer feature cannot be guaranteed when an uncorrectable memory event occurs in the system DRAM Bank_1. If an uncorrectable memory event occurs in this location, the BIOS code resident in this space may become corrupted. Because the watchdog feature uses a call to BIOS to effect the shutdown or reboot behavior, the feature may not work properly. If this occurs, you must manually reboot the system.

Shutdown

Subtabs: Remote Shutdown | Thermal Shutdown | Web Server Shutdown

Under the **Shutdown** tab, you can:

- Configure the operating system shutdown and remote shutdown options.
- Set the thermal shutdown severity level to shut down your system in the event that a temperature sensor returns a warning or failure value.

  NOTE: A thermal shutdown occurs only when the temperature reported by the sensor goes above the temperature threshold. A thermal shutdown does not occur when the temperature reported by the sensor goes below the temperature threshold.

- Shut down the Server Administrator secure port server (Web server).

  NOTE: Server Administrator is still available using the Command Line Interface (CLI) when the secure port server is shut down. The CLI functions do not require the secure port server to be running.

  NOTE: The secure port server starts automatically after a reboot, so you must shut down the secure port server every time a system starts up.

Logs

Subtabs: Hardware | Alert | POST | Command

- Under the **Logs** tab, you can:
- View the Embedded System Management (ESM) log or the System Event Log (SEL) for a list of all events related to your system's hardware components. The status indicator icon next to the log name will change from a green check mark () to a yellow triangle containing an exclamation point () when the log file reaches 80 percent capacity. On Dell™ PowerEdge™ *x8xx* and *x9xx*, the status indicator icon next to the log name will change to a red X () when the log file reaches 100 percent capacity.

  NOTE: It is recommended that you clear the hardware log when it reaches 80 percent capacity. If the log is allowed to reach 100 percent capacity, the latest events are discarded from the log.

- View the Alert log for a list of all events generated by the Server Administrator Instrumentation Service in response to changes in the status of sensors and other monitored parameters.

  NOTE: See the *Server Administrator Messages Reference Guide* for a complete explanation of each alert event ID's corresponding description, severity level, and cause.

- View the POST log for a list of the POST codes and their corresponding descriptions recorded during system start-up.
- View the Command log for a list of each command executed from either the **Server Administrator** home page or from its command line interface.

NOTE: See "Server Administrator Logs" for complete instructions on viewing, printing, saving, and e-mailing logs.

Alert Management

Subtabs: Alert Actions | Platform Events | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a system component sensor returns a warning or failure value.
- View current Platform Event Filter settings and set the Platform Event Filtering actions to be performed in the event that a system component sensor returns a warning or failure value. You can also use the **Configure Destination** option to select a destination where an alert for a platform event is to be sent.
- View current SNMP trap alert thresholds and set the alert threshold levels for instrumented system components. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

NOTE: Alert actions for all potential system component sensors are listed on the **Alert Actions** window, even if they are not present on your system. Setting alert actions for system component sensors that are not present on your system has no effect.

Session Management

Subtabs: Session

Under the **Session Management** tab, you can:

- View session information for current users that have logged into Server Administrator.
- Terminate user sessions.

NOTE: Only users with administrative privileges can view the Session Management page and terminate session(s) of logged-in users.

Diagnostics

Diagnostics is no longer available through Server Administrator. To run diagnostics on your system, install Dell PowerEdge Diagnostics from your *Dell PowerEdge Service and Diagnostic Utilities* CD or download and install Dell PowerEdge Diagnostics from the Dell Support website at **support.dell.com**. Dell PowerEdge Diagnostics is a stand-alone application that can be run without installing Server Administrator. See the *Dell PowerEdge Diagnostics User's Guide* for more information.

Main System Chassis

Clicking the **Main System Chassis** object allows you to manage your system's essential hardware and software components. The system may contain one main system chassis or several chassis. The main system chassis contains the essential components of a system. The **Main System Chassis** object action window has the following tab: **Properties**.

Properties

Subtabs: Health | Information | System Components (FRU)| Front Panel

Under the **Properties** tab, you can:

- View the health or status of hardware components and sensors. Each listed component has a "System Component Status Indicators" icon next to its name. A green check mark ( ) indicates that a component is healthy (normal). A yellow triangle containing an exclamation point ( ) indicates that a component has a warning (noncritical) condition and requires prompt attention. A red X ( ) indicates a component has a critical (failure) condition and requires immediate attention. A blank space ( ) indicates that a component's health status is unknown. The available monitored components include:
  - AC Switch
  - Batteries (Available only on PowerEdge 1950, 1955, 2900, and 2950 systems)
  - BIOS
  - Currents
  - Fans
  - Firmware
  - Hardware Log
  - Intrusion
  - Memory
  - Network
  - Ports
  - Power Supplies
  - Processors
  - Remote Access
  - Slots
  - Temperatures
  - Voltages

  NOTE: AC Switch and Currents are viewed in limited systems only.
- View information about the main system chassis attributes.
- View detailed information about the field-replaceable units (FRUs) installed in your system (under the **System Components (FRU)** subtab.) Note that only the FRUs that have electronic Piece Part IDentifiers (PPID) are listed.
- Enable or disable the managed system's front panel buttons, namely Power button and Non-Masking Interrupt (NMI) button (if present on the system).

AC Switch

Clicking the **AC Switch** object allows you to display key features of your system's AC failover switch. The **AC Switch** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view AC switch redundancy information and view information about the AC power lines.

Batteries

Clicking the **Batteries** object allows you to view information about your system's installed batteries. Batteries maintain the time and date when your system is turned off. The battery saves the system's BIOS setup configuration, which allows the system to reboot efficiently. The **Batteries** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Information

Under the **Properties** tab, you can view the current readings and status of your system's batteries.

Alert Management

Under the **Alert Management** tab, you can configure the alerts that you want to take effect in case of a battery warning or critical/failure event.

BIOS

Clicking the **BIOS** object allows you to manage key features of your system's BIOS. Your system's BIOS contains programs stored on a flash memory chip set that control communications between the microprocessor and peripheral devices, such as the keyboard and the video adapter, and other miscellaneous functions, such as system messages. The **BIOS** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Setup**.

Properties

Subtab: Information

Under the **Properties** tab, you can view BIOS information.

Setup

Subtab: BIOS

Under the **Setup** tab, you can set the state for each BIOS setup object.

NOTE: Setting the boot sequence to **Device List** on the **Setup** tab results in the following boot sequence: diskette, IDE CD drive, hard drive, option ROMs (if the devices are available).

You can modify the state of many BIOS setup features including but not limited to the Serial Port, Dual Network Interface Controller cards, Boot Sequence, User Accessible USB Ports, CPU Virtualization Technology, CPU HyperThreading, AC Power Recovery Mode, Embedded SATA Controller, Console Redirection, and Console Redirection Failsafe Baud Rate.

Depending upon your specific system configuration, additional setup items may be displayed. However, some BIOS setup options may be shown on the F2 BIOS Setup screen that are not accessible in Server Administrator.

NOTICE: The NIC configuration information within the Server Administrator **BIOS** setup may be inaccurate for embedded NICs. Using the **BIOS** setup screen to enable or disable NICs might produce unexpected results. It is recommended that you perform all configurations for embedded NICs through the actual **System Setup** screen that is available by pressing <F2> while a system is booting.

NOTE: The BIOS Setup tab for your system only displays the BIOS features that are supported on your system.

Currents

Clicking the **Currents** object allows you to manage current levels in your system. Server Administrator monitors currents across critical components in various chassis locations in the monitored system. The **Current** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Current Probes

Under the **Properties** tab, you can:

- View the current readings and status for your system's current probes.
- Configure current probe warning threshold values.
- Set alert actions in the event that a current probe returns a warning or failure value.

NOTE: When assigning probe threshold values, Server Administrator sometimes rounds the minimum or maximum values you enter to the closest assignable value.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a current sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for current sensors. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Fans

Clicking the **Fans** object allows you to manage your system fans. Server Administrator monitors the status of each system fan by measuring fan rpms. Fan probes report rpms to the Server Administrator Instrumentation Service. When you select **Fans** from the device tree, details appear in the data area in the right-hand pane of the Server Administrator home page. The **Fans** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtabs: Fan Probes | Fan Control

Under the **Properties** tab, you can:

- View the current readings for your system's fan probes and configure minimum and maximum values for fan probe warning threshold.

  NOTE: Some fan probe fields differ according to the type of firmware your system has: BMC or ESM. Some threshold values are not editable on BMC-based systems.

- Select fan control options.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a fan returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for fans. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Firmware

Clicking the **Firmware** object allows you to manage your system firmware. Firmware consists of programs or data that have been written to ROM. Firmware can boot and operate a device. Each controller contains firmware that helps provide the controller's functionality. The **Firmware** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view your system's firmware information.

Intrusion

Clicking the **Intrusion** object allows you to manage your system's chassis intrusion status. Server Administrator monitors chassis intrusion status as a security measure to prevent unauthorized access to your system's critical components. Chassis intrusion indicates that someone is opening or has opened the cover to the system's chassis. The **Intrusion** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Intrusion

Under the **Properties** tab, you can view the chassis intrusion status.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that the intrusion sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for the intrusion sensor. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Memory

Clicking the **Memory** object allows you to manage your system's memory devices. Server Administrator monitors the memory device status for each memory module present in the monitored system. Memory device prefailure sensors monitor memory modules by counting the number of ECC memory corrections. Server Administrator also monitors memory redundancy information if your system supports this feature. The **Memory** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Memory

Under the **Properties** tab, you can view memory attributes, memory device details, and memory device status.

NOTE: If a system with spare bank memory enabled enters a redundancy lost state, it may not be apparent which memory module is the cause. If you cannot determine which DIMM to replace, see the *switch to spare memory bank detected* log entry in the ESM system log to find which memory module failed.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a memory module returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for memory modules. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Network

Clicking the **Network** object allows you to manage your system's NICs. Server Administrator monitors the status of each NIC present in your system to ensure continuous remote connection. The **Network** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about the NICs installed in your system.

Ports

Clicking the **Ports** object allows you to manage your system's external ports. Server Administrator monitors the status of each external port present in your system. The **Ports** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about your system's external ports.

Power Supplies

Clicking the **Power Supplies** object allows you to manage your power supplies. Server Administrator monitors power supply status, including redundancy, to ensure that each power supply present in your system is functioning properly. The **Power Supplies** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Elements

Under the **Properties** tab, you can:

- View information about your power supply redundancy attributes.
- Check the status of individual power supply elements.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a power supply returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for power supplies. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Processors

Clicking the **Processors** object allows you to manage your system's microprocessor(s). A processor is the primary computational chip inside a system that controls the interpretation and execution of arithmetic and logic functions. The **Processors** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about your system's microprocessor(s) and access detailed cache information.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a processor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for processors. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Remote Access

Clicking the **Remote Access** object allows you to manage the Baseboard Management Controller (BMC) features and Remote Access Controller features. If you have a Dell Remote Access Controller (DRAC) card installed, DRAC manages the remote access capabilities of the system. When DRAC is not available, BMC is configured for remote access.

Selecting BMC allows you to manage the BMC features such as, general information on the BMC. You can also manage the configuration of the BMC on a local area network (LAN), serial port for the BMC, terminal mode settings for the serial port, BMC on a serial over LAN connection, and BMC users.

NOTE: If an application other than Server Administrator is used to configure the BMC while Server Administrator is running, the BMC configuration data displayed by Server Administrator may become asynchronous with the BMC. It is recommended that Server Administrator be used to configure the BMC while Server Administrator is running.

Selecting DRAC allows you to access your system's remote system management capabilities. The Server Administrator DRAC provides remote access to inoperable systems, alert notification when a system is down, and the ability to restart a system.

The **Remote Access** object action window can have the following tabs, depending on the user's group privileges: **Properties**, **Configuration**, and **Users**.

Properties

Subtab: Information

Under the **Properties** tab, you can view general BMC or DRAC information. Click **Reset to Defaults** to reset all the attributes to their system default values.

Configuration

Subtabs: LAN | Serial Port | Serial Over LAN

Under the **Configuration** tab when BMC is configured, you can configure the BMC on a LAN, serial port for BMC, and BMC on a serial over LAN connection.

Under the **Configuration** tab when DRAC is configured, you can:

- Configure network properties
- Configure SNMP traps
- Configure demand dial-out entries
- Configure dial-in users
- Configure remote properties such as remote boot parameters
- Configure modem properties

Users

Subtab: Remote Access Users

Under the **Users** tab, you can modify the remote access user configuration. You can add, configure, and view information about Remote Access Service users.

Slots

Clicking the **Slots** object allows you to manage the connectors or sockets on your system board that accept printed circuit boards, such as expansion cards. The **Slots** object action window has the **Properties** tab.

Properties

Subtab: Information

Under the **Properties** tab, you can view information about each slot and installed adapter.

Temperatures

Clicking the **Temperatures** object allows you to manage your system temperature in order to prevent thermal damage to your internal components. Server Administrator monitors the temperature in a variety of locations in your system's chassis to ensure that temperatures inside the chassis do not become too high. The **Temperatures** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Temperature Probes

Under the **Properties** tab, you can view the current readings and status for your system's temperature probes and configure minimum and maximum values for temperature probe warning threshold.

NOTE: Some temperature probe fields differ according to the type of firmware your system has: BMC or ESM. Some threshold values are not editable on BMC-based systems. When assigning probe threshold values, Server Administrator sometimes rounds the minimum or maximum values you enter to the closest assignable value.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a temperature probe returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for temperature probes. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

NOTE: Users can set minimum and maximum temperature probe threshold values for an external chassis to whole numbers only. If users attempt to set either the minimum or maximum temperature probe threshold value to a number that contains a decimal, only the whole number before the decimal place is saved as the threshold setting.

Voltages

Clicking the **Voltages** object allows you to manage voltage levels in your system. Server Administrator monitors voltages across critical components in various chassis locations in the monitored system. The **Voltages** object action window can have the following tabs, depending on the user's group privileges: **Properties** and **Alert Management**.

Properties

Subtab: Voltage Probes

Under the **Properties** tab, you can view the current readings and status for your system's voltage probes and configure minimum and maximum values for voltage probe warning threshold.

NOTE: Some voltage probe fields differ according to the type of firmware your system has: BMC or ESM. Some threshold values are not editable on BMC-based systems.

Alert Management

Subtabs: Alert Actions | SNMP Traps

Under the **Alert Management** tab, you can:

- View current alert actions settings and set the alert actions that you want to be performed in the event that a system voltage sensor returns a warning or failure value.
- View current SNMP trap alert thresholds and set the alert threshold levels for voltage sensors. The selected traps will be triggered if the system generates a corresponding event at the selected severity level.

Software

Clicking the **Software** object allows you to view detailed version information about the managed system's essential software components, such as the operating system and the systems management software. The **Software** object action window has the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Summary

Under the **Properties** tab, you can view a summary of the monitored system's operating system and system management software.

Operating System

Clicking the **Operating System** object allows you to view basic information about your operating system. The **Operating System** object action window has the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Information

Under the **Properties** tab, you can view basic information about your operating system.

Storage

Server Administrator provides the Storage Management Service:

The Storage Management Service provides features for configuring storage devices. In most cases, the Storage Management Service is installed using Typical Setup. The Storage Management Service is available on Microsoft Windows, Red Hat Enterprise Linux, and SUSE® Linux Enterprise Server operating systems.

When Storage Management Service is installed, clicking the **Storage** object allows you to view the status and settings for various attached array storage devices, volumes, system disks, and so on.

In Storage Management Service, the **Storage** object action window has the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Health

Under the **Properties** tab, you can view the health or status of attached storage components and sensors such as array subsystems, operating system disks, and volumes.

Volumes

Clicking the **Volumes** object allows you to view information about volumes on your system. A volume may be formatted and may have a file system and/or drive letter. The **Volumes** object action window can have the following tab, depending on the user's group privileges: **Properties**.

Properties

Subtab: Volumes

Under the **Properties** tab, you can view the current status of and detailed information about your volumes.

Storage Management Service

In the case of Storage Management Service, clicking the **Storage** object allows you to view the status and settings for the supported controllers attached to the system. The controller object expands to display the storage devices attached to the controller.

Depending on the controller and storage attached to the system, the expanded **Storage** object may display the following lower-level objects:

- Controller
- Battery
- Connector
- Enclosure or Backplane
- Physical Disks
- EMMs
- Fans
- Power Supplies
- Temperatures
- Virtual Disks
- Firmware/Driver Versions

The **Storage** object action window can have the following tabs, depending on the user's group privileges: **Properties**.

Properties

Subtab: Health

In the **Health** window of the **Properties** tab, you can view the current health or status of the attached storage components. This window displays the status of all lower-level objects.

A quick way to review the status of all storage components is to select the **Storage** object and view the **Health** window under the **Properties** tab. You can click the required storage components in the **Health** window to view detailed information on the health or status of the component.

Subtab: Information/Configuration

In the **Information/Configuration** window of the **Properties** tab, you can view the properties for the controllers attached to the system. You can also execute global tasks that apply to all controllers.

Controller

Clicking the **Controller** object allows you to view information about your controllers and the various components attached to the controller. The components attached to the controller can include battery, virtual disks, and so on. The **Controller** object action window can have the following tabs, depending on the user's group privileges: **Health** and **Information/Configuration**.

Health

Under the **Health** tab, you can view the current status of the battery, virtual disks, and other storage components attached to the controller. The status is visually indicated with the icons described in "Storage Component Severity."

Information/Configuration

Under the **Information/Configuration** tab, you can view the property information of the controller and the components attached to the controller. You can also execute controller tasks in this tab.

Connector

Clicking the **Connector** object allows you to view information about the connector and the enclosure or backplane attached to the connector. The **Connector** object action window can have the following tabs, depending on the user's group privileges: **Health** and **Configuration/Information**.

Health

Under the **Health** tab, you can view the current status of the connector and the enclosure or backplane attached to the connector. The status is visually indicated with the icons described in "Storage Component Severity."

Configuration/Information

Under the **Configuration/Information** tab, you can view the property information of the connector and the enclosure or backplane attached to the connector. You can also execute connector tasks in this tab.

Enclosure or Backplane

Clicking the **Enclosure or Backplane** object allows you to view information about the physical disks, temperature probes, and other components attached to the enclosure or backplane. The **Enclosure or Backplane** object action window can have the following tabs, depending on the user's group privileges: **Health** and **Configuration/Information**.

Health

Under the **Health** tab, you can view the current status of physical disks and other components attached to the enclosure or backplane. For example, the status of an enclosure's fans, power supplies, temperature probes, and so on is displayed in this tab. The status of physical disks attached to the backplane is also displayed here. The status is visually indicated with the icons described in "Storage Component Severity."

Configuration/Information

Under the **Configuration/Information** tab, you can view the property information of the physical disks, temperature probes, EMMs (Enclosure Management Modules) and other components attached to the enclosure or backplane. For enclosures, you can also execute enclosure tasks in this tab.

Physical Disks

Clicking the **Physical Disks** object allows you to view information about the physical disks attached to the enclosure or backplane. The **Physical Disks** object action window can have the following tab, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the physical disks attached to the enclosure or backplane. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, capacity, used and available disk space, and other information. You can also execute physical disk tasks in this tab.

EMMs

Clicking the **EMMs** object allows you to view information about the Enclosure Management Modules (EMMs). The **EMMs** object action window can have the following tab, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the EMMs. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, part number, firmware version, and SCSI rate.

Fans

Clicking the **Fans** object allows you to view information about the enclosure fans. The **Fans** object action window can have the following tab, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the fans. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes fan name, state, part number, and speed.

Power Supplies

Clicking the **Power Supplies** object allows you to view information about the enclosure power supplies. The **Power Supplies** object action window can have the following tab, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the enclosure power supplies. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, and part number.

Temperatures

Clicking the **Temperatures** object allows you to view information about the enclosure temperature probes. The **Temperatures** object action window can have the following tab, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the current status and property information of the enclosure temperature probes. The status is visually indicated with the icons described in "Storage Component Severity."

Property information includes name, state, and reading (current temperature). The minimum and maximum values set for the temperature probes' **Warning** and **Failure** thresholds are also displayed under this tab.

Virtual Disks

Clicking the **Virtual Disks** object allows you to view information about the virtual disks configured on the controller. The **Virtual Disks** object action window can have the following tab, depending on the user's group privileges: **Configuration/Information**.

Configuration/Information

Under the **Configuration/Information** tab, you can view the property information of the virtual disks configured on the controller. Property information includes name, state, and layout (RAID level). The read, write, and cache policy and stripe size are also displayed. You can also execute virtual disk tasks in this tab.

Firmware/Driver Versions

Clicking the **Firmware/Driver Version** object allows you to view information about the version of the driver and firmware that are currently installed on the controller. The firmware and driver properties can vary depending on the model of the controller.

Firmware and driver properties may include:

- Firmware Version
- Minimum Required Firmware Version
- Driver Version
- Minimum Required Driver Version

Storage Component Severity

The status of a component is graded for degrees of severity. Each level of severity requires you to take different actions in response. For example, you must take immediate reparative action in response to a **Warning** or **Critical/Failure** status to avoid any data loss.

It may be useful to review the Alert Log for events indicating why a component has a **Warning** or **Critical** status. For additional troubleshooting information, see the Storage Management online help.

NOTE: The status displayed reflects the status at the time the browser first displayed the page. If you believe the status has changed and wish to update the displayed information, click the **Refresh** button in the upper-right corner of the action window. Some storage configuration changes can only be detected if you perform a controller **rescan**; click the **Information/Configuration** tab in the required controller and click **Rescan**.

Table 6-1 explains the various severity levels and the corresponding component status.

Table 6-1. Severity Levels and Component Status

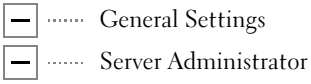
Severity Level	Component Status
	Normal/OK. The component is working as expected.
	Warning/Non-critical. A probe or other monitoring device has detected a reading for the component that is above or below the acceptable level. The component may still be functioning, but it could fail. The component may also be functioning in an impaired state. Data loss is possible.
	Critical/Failure/Error. The component has either failed or failure is imminent. The component requires immediate attention and may need to be replaced. Data loss may have occurred.

Managing Preferences: Home Page Configuration Options

The left pane of the **Preferences** home page (where the system tree is displayed on the **Server Administrator** home page) displays all available configuration options in the system tree window. The options displayed are based on the systems management software installed on the managed system.

See Figure 6-2 for available Preferences home page configuration options.

Figure 6-2. Preferences Home Page Configuration Options



General Settings

Clicking the **General Settings** object allows you to set user and secure port server (Web server) preferences for selected Server Administrator functions. The **General Settings** object action window has the following tabs, depending on the user's group privileges: **User** and **Web Server**.

User

Subtab: Properties

Under the **User** tab, you can set user preferences, such as the home page appearance and the default e-mail address for the **Email** button.

Web Server

Subtabs: Properties | X.509 Certificate

Under the **Web Server** tab, you can:

- Set secure port server preferences. See "Secure Port Server and Security Setup" for instructions on configuring your server preferences.
- Perform X.509 certificate management by generating a new X.509 certificate, reusing an existing X.509 certificate, or importing a root certificate or certificate chain from a Certification Authority (CA). For more information about certificate management, see "X.509 Certificate Management."

Server Administrator

Clicking the **Server Administrator** object allows you to enable or disable access to users with User or Power User privileges and to configure the SNMP root password. The **Server Administrator** object action window can have the following tab, depending on the user's group privileges: **Preferences**.

Preferences

Subtabs: Access Configuration | SNMP Configuration

Under the **Preferences** tab, you can:

- Enable or disable access to users with User or Power User privileges.
- Configure the SNMP root password.

NOTE: The default SNMP configuration user is `root` and the password is `calvin`.

7

Remote Access Service

Overview

The Server Administrator Remote Access Service provides a complete remote system management solution for SNMP- and CIM-instrumented systems equipped with a Dell™ Remote Access Card (DRAC) III, a DRAC III/XT, an Embedded Remote Access (ERA) controller, or an ERA Option (ERA/O) card. These hardware and software solutions are collectively known as Dell Remote Access Controllers (DRACs). DRAC 4 and DRAC 5 Remote Access Service also allow a basic management task to be performed from Dell OpenManage Server Administrator: you can connect to DRAC 4 or DRAC 5 from the Server Administrator graphical user interface depending on the DRAC card installed.

The DRAC 4 and DRAC 5 are systems management hardware and software solution designed to provide remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge™ systems.

By communicating with the system's baseboard management controller (BMC), the DRAC 4 and DRAC 5 can be configured to send you e-mail alerts for warnings or errors related to voltages, temperatures, and fan speeds. The DRAC 4 and DRAC 5 also log event data and the most recent crash screen (for systems running the Microsoft® Windows® operating system only) to help you diagnose the probable cause of a system crash.

Depending on your system, the DRAC 4 hardware is either a system card (DRAC 4/I) or a short PCI card (DRAC 4/P). The DRAC 4/I and DRAC 4/P are identical except for the hardware differences.

The DRAC 5 hardware is an embedded system card.

The DRAC 4 and DRAC 5 have their own microprocessor and memory, and are powered by the system in which they are installed. The DRAC 4 and DRAC 5 may be preinstalled on your system, or available separately in a kit.

NOTE: The information contained in this section pertains to the previous generation of DRACs. See the *Dell Remote Access Controller 4 User's Guide* for more information on using DRAC 4 or *Dell Remote Access Controller 5 User's Guide* for more information on using DRAC 5.

The Remote Access Service provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Service also provides alert notification when a system is down and allows you to remotely restart a system. Additionally, the Remote Access Service logs the probable cause of system crashes and saves the most recent crash screen.

You can log into the Remote Access Service through the Server Administrator home page or by directly accessing the controller's IP address using a supported browser.

See the *Server Administrator Command Line Interface User's Guide* and the *Dell Remote Access Controller Racadm User's Guide* for information about running the Remote Access Service from the command line.

When using the Remote Access Service, you can click **Help** on the global navigation bar for more detailed information about the specific window you are viewing. Remote Access Service help is available for all windows accessible to the user based on user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

NOTICE: Do not query or configure a DRAC 5 card using Server Administrator, remotely or locally, when the card is resetting or performing a firmware update. During reset, the DRAC 5 card goes offline for a short duration. Accessing the DRAC 5 card during reset may cause problems with the data displayed in the graphical user interface or Command Line Interface (CLI.)

NOTE: The Remote Access Service is not available on modular systems. You must directly connect to the DRAC on a modular system. See the *Dell Embedded Remote Access/MC Controller User's Guide* for more information.

NOTE: See the *Dell Remote Access Controller Installation and Setup Guide* for complete information about installing and configuring a DRAC III, a DRAC III/XT, ERA, or an ERA/O controller, and using a DRAC to remotely access an inoperable system. See the *Dell Embedded Remote Access/MC Controller User's Guide* for complete information about configuring and using an ERA/MC controller to remotely manage and monitor your modular system and its shared resources through a network.

Hardware Prerequisites

The managed system must have a DRAC installed to use the Remote Access Service.

For a list of specific hardware requirements for your DRAC, see the readme file for your remote access controller on the *Systems Management Consoles* CD and the *Dell Remote Access Controller Installation and Setup Guide* or the *Dell Embedded Remote Access/MC Controller User's Guide* on the documentation CD.

NOTE: The DRAC software is installed as part of the **Typical Setup** and **Custom Setup** installation options when installing managed system software from the *Dell Installation and Server Management* CD, provided that the managed system meets all of your DRAC's installation prerequisites. See the appropriate DRAC documentation for complete software and hardware requirements.

Software Prerequisites

The managed system must have the DRAC software installed. See the *Dell Remote Access Controller Installation and Setup Guide* or the *Dell Embedded Remote Access/MC Controller User's Guide* for a complete list of software installation prerequisites.

NOTE: The DRAC software is installed as part of the **Typical Setup** and **Custom Setup** installation options when installing managed system software from the *Dell Installation and Server Management* CD, provided that the managed system meets all of your DRAC's installation prerequisites. See the appropriate DRAC documentation for complete software and hardware requirements.

Adding and Configuring DRAC Users

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

The DRAC can store information for up to 16 users. The Remote Access Service provides security by requiring a user to provide a user name and password prior to establishing a remote connection. The Remote Access Service can also provide paging services to notify users if the system crashes, loses power, or experiences a defined list of other events. Paging services are only available for DRAC III cards.

NOTE: Some configuration capabilities are available only on systems with DRAC III, DRAC III/XT, ERA, and ERA/O, and not on systems with DRAC 4 or DRAC 5. To configure DRAC 4 or DRAC 5, use the **Launch Remote Connect Interface** option in the **RAC Properties** window. See the *Dell Remote Access Controller 4 User's Guide* for more information on using DRAC 4 or *Dell Remote Access Controller 5 User's Guide* for more information on using DRAC 5.

To create a DRAC user, perform the following steps:

1. Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access** object.
2. Click the **Users** tab.

   The **Remote Access Users** window appears.
3. Click **Add**.

   The **Add Remote Access User** window appears.
4. Type a user name in the **User Name** field.
5. Type a new password in the **New Password** field.
6. Type the new password again in the **Confirm Password** field.
7. Configure numeric paging (for DRAC III users only):
   a. Click the check box next to **Enable Numeric Paging** and enter a pager number in the **Pager Number** field.
   b. Enter the numeric message in the **Numeric Message** field that you want the DRAC to send when it receives certain events.
8. Configure e-mail paging:
   a. Click the check box next to **Enable Email Paging** and enter an e-mail address in the **Email Address** field.
   b. Enter the message in the **Message** field that you want the DRAC to send when it receives certain events.

9 Configure alphanumeric paging (for DRAC III users only):

a Click the check box next to **Enable Alpha-Numeric Paging** and enter a pager number in the **Pager Number** field.

b Select the alphanumeric protocol used by the pager's service provider, **7E0** or **8N1**.

c Select the pager's baud rate, **300** or **1200**.

d Enter the message in the **Custom Message** field that you want the DRAC to send when it receives certain events.

e Enter the pager's PIN in the **Pager ID** field, and then, if required, enter a pager password in the **Pager Password** field.

f Click **Apply Changes** at the bottom of the window.

10 Under **Severity Configuration**, specify the trap and the severity that the trap must have to trigger a paging action from the DRAC.

Traps enable you to configure the DRAC to respond to alert conditions from the system's ESM hardware or to other conditions such as operating system crashes or power failures.

The first (left-most) column of check boxes corresponds to the severity level **Informational**, the second column corresponds to the severity level **Warning**, and the third column corresponds to the severity level **Critical**. The last seven events can only report the severity level **Informational**.

11 Click **Apply Changes** and then click **OK** to save the alert, paging, and user configuration to the Server Administrator data repository.

Server Administrator returns to the **Users** tab. The user you just created and configured is displayed in the **User Name** list.

Configuring an Existing DRAC User

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

To configure a DRAC user, perform the following steps:

1 Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access** object.

2 Click the **Users** tab.

The **Remote Access Users** window appears.

3 Click the user name for the user you want to configure.

4 Change the password:

a Click the check box next to **Change Password** and type a new password in the **Password** field.

b Type the new password again in the **Confirm Password** field.

5 Configure numeric paging (for DRAC III users only):

   a Click the check box next to **Enable Numeric Paging** and enter a pager number in the **Pager Number** field.

   b Enter the numeric message in the **Numeric Message** field that you want the DRAC to send when it receives certain events.

6 Configure e-mail paging:

   a Click the check box next to **Enable Email Paging** and enter an e-mail address in the **Email Address** field.

   b Enter the message in the **Message** field that you want the DRAC to send when it receives certain events.

7 Configure alphanumeric paging (for DRAC III users only):

   a Click the check box next to **Enable Alpha-Numeric Paging** and enter a pager number in the **Pager Number** field.

   b Select the alphanumeric protocol used by the pager's service provider, **7E0** or **8N1**.

   c Select the pager's baud rate, **300** or **1200**.

   d Enter the message in the **Custom Message** field that you want the DRAC to send when it receives certain events.

   e Enter the pager's PIN in the **Pager ID** field, and then, if required, enter a pager password in the **Pager Password** field.

   f Click **Apply Changes** at the bottom of the window.

8 Under **Severity Configuration**, specify the trap and the severity that the trap must have to trigger a paging action from the DRAC.

   Traps enable you to configure the DRAC to respond to alert conditions from the system's ESM hardware or to other conditions such as operating system crashes or power failures.

   The first (left-most) column of check boxes corresponds to the severity level **Informational**, the second column corresponds to the severity level **Warning**, and the third column corresponds to the severity level **Critical**. The last seven events can only report the severity level **Informational**.

9 Click **Apply Changes** and then click **OK** to save the alert, paging, and user configuration to the Server Administrator data repository.

   Server Administrator returns you to the **Users** tab.

Configuring the DRAC Network Properties

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

Your DRAC contains an integrated 10BASE-T/100BASE-T Ethernet NIC and supports TCP/IP. The NIC has a default address of 192.168.20.1 and a default gateway of 192.168.20.1.

NOTE: If your DRAC is configured to the same IP address as another NIC on the same network, an IP address conflict occurs. The DRAC stops responding to network commands until the IP address is changed on the DRAC. The DRAC must be reset even if the IP address conflict is resolved by changing the IP address of the other NIC.

NOTE: Changing the IP address of the DRAC causes the DRAC to reset. If SNMP polls the DRAC before it initializes, a temperature warning is logged because the correct temperature is not transmitted until the DRAC is initialized.

To configure the network properties of your DRAC, perform the following steps:

1. Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access** object.
2. Click the **Configuration** tab.

   The **Configure Network Properties** window appears.
3. Click the check box next to **Enable NIC** (this option is selected by default).
4. To have the DHCP system assign the NIC information, click the check box next to **Use DHCP (For NIC IP Address)**. If you do not, clear (deselect) this check box and enter the DRAC's NIC information in the **Static IP Address**, **Static Subnet Mask**, and **Static Gateway Address** fields.
5. Enable dial-in networking (for DRAC III users only):
   a. Click the check box next to **Enable Dial-In** (this option is selected by default).
   b. To have the DHCP system assign the dial-in information, click the check box next to **Use DHCP (For Dial-In IP Address)**. If you do not, clear (deselect) this check box and enter the DRAC III modem's base IP Address in the **Base IP Address** field.
   c. Specify the **Dial-In Authentication** settings that dial-in connections require:
      - **Any** — Allows the connection to use any type of encryption, including no encryption
      - **Encrypted** — Requires the connection to use some type of encryption
      - **CHAP** — Requires the connection to use the CHAP
6. To enable SMTP server address control, click the check box next to **Enable SMTP**, and type the SMTP server address in the **SMTP (Email) Server Address** field.
7. Click **Apply Changes** and click **OK** to save your changes.

Configuring the DRAC Alert Properties

DRACs can be configured to respond to alert conditions from the system's ESM or to other conditions such as operating-system crashes or power failures.

DRACs offer the following types of alert actions:

- Alphanumeric paging (DRAC IIIs only) (See "Adding and Configuring DRAC Users" for information about configuring this type of alert action.)
- Numeric paging (DRAC IIIs only) (See "Adding and Configuring DRAC Users" for information about configuring this type of alert action.)
- E-mail (See "Adding and Configuring DRAC Users" for information about configuring this type of alert action.)
- SNMP traps (See the following subsection for information about configuring this type of alert action.)

Configuring the SNMP Alert Properties

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

To configure the Remote Access Service alert properties, perform the following steps:

1. Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access** object.
2. Click the **Configuration** tab.
3. Click **SNMP**.
4. Click **Add** or click the **Destination IP Address** to edit existing SNMP alert properties.
5. Click the check box next to **Enable SNMP Trap**, if a check isn't already in the check box.
6. Enter the SNMP community name to which the destination management station belongs in the **Community** field.
7. Enter a destination IP address of the management station to which you want the DRAC to send SNMP traps when an event occurs in the **IP Address** field.
8. Use the check boxes under **Severity Configuration** to specify the events and the severity level that those events must have to trigger an alert action from the DRAC.

   The first (left-most) column of check boxes corresponds to the severity level **Informational**, the second column corresponds to the severity level **Warning**, and the third column corresponds to the severity level **Critical**. The last seven events can only report the severity level **Informational**.
9. Click **Apply Changes** and then click **OK** to save your changes.

Configuring DRAC III Dial-in (PPP) Users and Modem Settings

Dial-in (PPP) users and modem features are currently only available for the DRAC III.

Adding and Configuring a DRAC III Dial-In (PPP) User

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

This subsection describes how to add and configure a dial-in (PPP) user. After dial-in users are authenticated, they must enter the DRAC user authentication at the remote access controller login screen to access the DRAC III.

NOTE: The Server Administrator managed-system PPP client uses the 192.168.234.235 network to talk with the installed DRAC III. It is possible that this network IP address could already be in use by other systems or applications. If this situation occurs, the PPP connection fails to operate. If this address is already in use, the user is required to change the managed-system PPP client IP address to a different number. To change the managed-system PPP server IP address to use another network so that conflicts do not occur, you must use the racadm utility. See the *Dell Remote Access Controller Racadm User's Guide* for information about using the racadm utility.

To add and configure dial-in users, perform the following steps:

1. On the Server Administrator home page, click the **Main System Chassis** object, and then click the **Remote Access** object.
2. Click the **Configuration** tab.
3. Click **Dial-In Users**.
4. Click **Add**.
5. Type a user name in the **User Name** field.
6. Type a new password in the **Password** field.
7. Type a callback number in the **Callback Number** field.

   This number is the one the Remote Access Service calls if **Callback Type** is set to **Preset**.
8. Select a setting from the **Callback Type** drop-down menu:
   - **None** — When called, the Remote Access Service does not disconnect and call back; the connection remains active.
   - **Preset —** When called, the Remote Access Service disconnects and calls the number specified in the **Callback Number** field; this setting activates the callback number control.
   - **User Specified** — When called, the Remote Access Service asks the user for the callback number. Then the Remote Access Service disconnects and calls the number the user specified.
9. Click **Apply Changes** and then click **OK** to save your changes.

Adding and Configuring DRAC III Demand Dial-Out Entries

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

If you set the dial-in (PPP) setting to **Preset**, the demand dial-out entry causes the Remote Access Service to disconnect and call the management station back at a preset number. Upon callback, you must provide your DRAC user authentication to access the Remote Access Service.

NOTE: The DRAC managed system software uses a PPP connection to talk to the installed DRAC. The IP address for this PPP connection is 192.168.234.235. It is possible that this network IP address could already be in use by other systems or applications. If this situation occurs, the PPP connection fails to operate. If this address is already in use, the user is required to change the managed-system PPP client IP address to a different number. To change the managed-system PPP server IP address to use another network so that conflicts do not occur, you must use the racadm utility. See the *Dell Remote Access Controller Racadm User's Guide* for information about using the racadm utility.

To add a demand dial-out entry, perform the following steps:

1. On the Server Administrator home page, click the **Main System Chassis** object, and then click the **Remote Access** object.
2. Click the **Configuration** tab.
3. Select **Demand Dial-Out**.
4. Click **Add**.
5. Enter the management station IP address that the Remote Access Service calls back when called by this user.
6. Enter the phone number used by the system's modem in the **Phone Number** field.
7. Enter the user name for the demand dial-out user in the **User Name** field.
8. Enter the password for the demand dial-out user in the **Password** field.
9. Select a setting from the **Authentication** drop-down menu:
   - **Any** — Allows the connection using any type of encryption, including no encryption
   - **Encrypted** — Requires the connection to use some type of encryption
   - **CHAP** — Requires the connection to use the CHAP
10. Click **Apply Changes** and click **OK** to save your changes.

Configuring the DRAC III Modem Settings

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

If your DRAC III kit includes the optional PCMCIA modem, you must configure the modem prior to use.

To configure the DRAC III modem, perform the following steps:

1. On the Server Administrator home page, click the **Main System Chassis** object, and then click the **Remote Access** object.
2. Click the **Configuration** tab.
3. Click **Modem**.

4 For **Dial Mode**, choose either **Pulse** or **Tone**.

5 From the **Country Code** drop-down menu, select the country where the DRAC III is located.

6 For **Initialization String**, enter the required initialization string for the DRAC III modem in the text field.

7 Select a **Baud Rate** setting from the drop-down menu (the default is **38400**).

8 Click **Apply Changes**, and then click **OK** to save your changes.

Configuring the DRAC Remote Features Properties

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

If the local boot image on the managed system has been corrupted, a DRAC has the ability to boot its host server using a diskette boot image that it downloads from a Trivial File Transfer Protocol (TFTP) server. This feature is called remote floppy boot. A DRAC can also update its firmware using a firmware image located on a TFTP server. This feature is called remote firmware update, and the process is similar to flashing a system BIOS.

To configure the remote floppy boot feature and the remote firmware update feature of your DRAC, perform the following steps:

1 Click the **Main System Chassis** object on the Server Administrator home page, and then click the **Remote Access** object.

2 Click the **Configuration** tab.

The **Configure Network Properties** window appears.

3 Click **Remote Features**.

The **Remote Properties** window appears.

4 Select the check box next to **Enable Remote Floppy Boot** to configure the remote boot parameters,

5 Configure the DRAC's remote boot parameters:

- **a** Click the check box next to **Enable Remote Floppy Boot**.
- **b** Type the TFTP server's IP address in the **Remote Floppy TFTP Address** field.
- **c** Type the boot image filename in the **Remote Floppy TFTP Path** field. The path must be relative to the root directory of the TFTP server.

6 Configure the DRAC's firmware update parameters:

- **a** Click the check box next to **Enable Remote Firmware Update**.
- **b** Type the TFTP server's IP address in the **Remote Firmware TFTP Address** field.
- **c** Type the firmware image filename in the **Remote Firmware Update Path** field. The path must be relative to the root directory of the TFTP server.

7 Click **Apply Changes** and click **OK** to save your changes.

Configuring DRAC Security

NOTE: You must have Admin privileges in Server Administrator to use the Remote Access Service.

NOTE: See the *Dell Remote Access Controller Installation and Setup Guide* for more information about DRAC security features.

To configure your DRAC security from the Server Administrator home page, click **System→ Main System Chassis→ Remote Access** and then click the **Security** tab. Under the **Security** tab, you can perform CSR certificate management and set DRAC user login authentication options.

NOTE: Some of the DRAC certificate management operations use the FTP protocol to communicate with the DRAC firmware. If a firewall software is installed on the system, these operations may fail.

Certificate Management

Use the **Certificate Management** window to generate a certificate signing request (CSR), upload a server certificate or certificate authority (CA) certificate to the DRAC firmware, or view an existing server certificate or CA certificate. From the **Certificate Management** window, the following options are available:

- Generating a CSR
- Uploading a Certificate
- Viewing a Certificate

A CSR is a digital request to a CA for a secure server certificate. Secure server certificates ensure the identity of a remote system and ensure that information exchanged with the remote system cannot be viewed or changed by others. To ensure the security for your DRAC, it is strongly recommended that you generate a CSR, submit the CSR to a CA, and upload the certificate returned from the CA.

A certificate authority is a business entity that is recognized in the IT industry for meeting high standards of reliable screening, identification, and other important security criteria. Examples of CAs include Thwate and VeriSign. Once the CA receives your CSR, they review and verify the information the CSR contains. If the applicant meets the CA's security standards, the CA issues a certificate to the applicant that uniquely identifies that applicant for transactions over networks and on the internet.

After the CA approves the CSR and sends you a certificate, you must upload the certificate to the DRAC firmware. The CSR information stored on the DRAC firmware must match the information contained in the certificate.

Generating a CSR

NOTICE: Each new CSR overwrites any previous CSR on the firmware. It is crucial that the CSR on the firmware matches the certificate returned from a CA.

1. From the **Certificate Management** window, select the **Generate a new CSR** option and click **Next**.

   The **Certificate Signing Request (CSR) Generation** window appears.

2. Type a value or choose a value from a drop-down menu for each listed attribute and click **Generate**.

   A message appears stating that the CSR was successfully generated and giving the path where it was saved.

3. You are now ready to send your CSR to a CA.

Uploading a Certificate

To upload your server certificate or CA certificate to the DRAC firmware, the certificate must reside on the DRAC's host server. You must designate the CSR type, the exact filename, and the absolute file path to the certificate on the server. Then, click **Upload**.

NOTE: Failure to enter the correct path for the location of the certificate on the host server does not result in a warning message.

1. From the **Certificate Management** window, select the **Upload certificate** option and click **Next**.

   The **Upload Certificate** window appears.

2. Select the certificate type from the drop-down menu.

   The selections are **Server Certificate** and **CA Certificate**.

3. Type the exact path and filename of the certificate to be uploaded.

   NOTE: When you have a fully qualified path or filename that contains spaces, you must place double quotation marks around the string. For example, if your file is contained in **c:\security files\certificates\sslcert.cer**, you must place the fully qualified path name and filename in double quotations because a space appears between "security" and "files." For example: `c:\security files\certificates\sslcert.cer`

4. Click **Upload**.

   A message appears stating that the certificate was successfully uploaded to the DRAC firmware.

5. Reset the DRAC to enable the new certificate.

NOTE: You must reset the DRAC after uploading the certificate to ensure that the new certificate is used.

Viewing a Certificate

The following information is included on both the **View Server Certificate** and **View CA Certificate** windows. See Table 7-1.

Table 7-1. Certificate Information

Attribute	Value
Type	Type of certificate, either a server certificate or a CA certificate
Serial	Certificate serial number
Key Size	Encryption key size
Valid From	Issuance date of the certificate
Valid To	Expiration date of the certificate
Subject	Certificate attributes entered by the subject
Issuer	Certificate attributes returned by the issuer

Configuring Remote Connect Authentication Options

Use the **Remote Connect Authentication Options** window to set DRAC user login authentication options. You can configure the DRAC to only allow login by users created through the Remote Access Service (RAC users), or to allow DRAC login by users created both through the Remote Access Service and through the local operating system.

1. Click **System→ Main System Chassis→ Remote Access** and then click the **Security** tab.

   The **Certificate Management** window appears.

2. Click **Authentication Options**.

   The **Remote Connect Authentication Options** window appears. There are two configuration options, each proceeded by a check box.

   The **RAC Authentication** check box is selected by default and cannot be deselected. This setting allows login to the DRAC by users created through the DRAC (DRAC users).

   Select the **Local Operating System Authentication** check box to also allow login to the DRAC by users created through the local operating system.

   NOTE: The **Local Operating System Authentication** check box is grayed out by default and cannot be checked or unchecked for DRAC firmware version 3.20 or later. Use Active Directory Authentication for DRAC firmware version 3.20 or later. See the *Using Microsoft Active Directory With Your Dell Remote Access Controller (DRAC III, DRAC III/XT, ERA, and ERA/O) User's Guide* for information on configuring Active Directory authentication.

3. Click **Apply Changes** and click **OK** to save your changes.

Accessing and Using a Dell Remote Access Controller

To link to the Remote Access Service DRAC **Log in** window from the Server Administrator home page, click the **Main System Chassis** object, click the **Remote Access Controller** object, click the **Remote Connect** tab, and then click **Remote Connect**. The DRAC **Log in** window appears.

After connecting to the DRAC you can monitor and manage your system, including accessing system and session information, managing the DRAC configurations, and performing remote access functions on the managed system. See the *Dell Remote Access Controller Installation and Setup Guide* for instructions on using a DRAC.

8

Working With the Baseboard Management Controller (BMC)

Overview

The Dell™ PowerEdge™ systems baseboard management controller (BMC) monitors the system for critical events by communicating with various sensors on the system board and sends alerts and log events when certain parameters exceed their preset thresholds. The BMC supports the industry-standard Intelligent Platform Management Interface (IPMI) specification, enabling you to configure, monitor, and recover systems remotely.

Server Administrator allows remote, in-band access to event logs, power control, and sensor status information and provides the ability to configure the BMC. You can manage the BMC through the Server Administrator graphical user interface by clicking the **Remote Access** object, which is a subcomponent of the **Main System Chassis** group. You can perform the following BMC–related tasks:

- View basic BMC information
- Configure BMC users
- Set BMC platform event filter alerts
- Configure the BMC on a serial over LAN connection
- Configure the BMC on a serial port connection
- Configure the BMC on a virtual LAN connection

However, in Dell PowerEdge *x8xx* and *x9xx* systems, BMC and RAC are combined into a single object known as Remote Access (**System→ Main System Chassis→ Remote Access**). You can view BMC or RAC information based on which hardware is providing the remote access capabilities for the system.

The reporting and configuration of BMC and DRAC can also be managed using the `omconfig chassis remoteaccess` CLI command.

In addition, you can use the Server Administrator Instrumentation Service to manage the Platform Event Filters (PEF) parameters and alert destinations.

NOTE: You can view BMC data on Dell PowerEdge *x8xx* and *x9xx* systems only. Other systems allow you to only install and uninstall BMC. Limited sensor data is available using BMC or ESM on Dell PowerEdge *x6xx* and *x7xx* systems.

See the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* for more information about the BMC.

Viewing Basic BMC Information

You can view the basic information about the BMC and also reset the BMC settings to their default values.

NOTE: You must be logged in with Admin privileges to reset the BMC settings.

1. Click the **System** object.
2. Click the **Main System Chassis** object.
3. Click the **Remote Access** object.

   The **Remote Access** page displays the following base information of the system's BMC:

   - BMC Name
   - IPMI Version
   - System GUID
   - Number of Possible Active Sessions
   - Number of Current Active Sessions
   - IPMI Over LAN Enabled
   - SOL Enabled
   - IP Address Source
   - IP Address
   - IP Subnet
   - IP Gateway
   - MAC Address

Configuring BMC Users

BMC users can be configured using the **Remote Access** page; this page is accessed by browsing through the following path.

1. Click the **System** object.
2. Click the **Main System Chassis** object.
3. Click the **Remote Access** object.
4. Click the **Users** tab.

   The **Remote Access Users** window displays information about users that can be configured as BMC users.

   NOTE: BMC Users are created independently of the users assigned or created through Server Administrator or the operating system.

5. Click **User ID** to configure a new or existing BMC user.

   The **Remote Access User Configuration** window allows you to configure a specific BMC user.

6 Specify the following general information:
   - Select **Enable User** to enable the user.
   - Enter the name for the user in the **User Name** field.
   - Select the **Change Password** check box.
   - Enter a new password in the **New Password** field.
   - Re-enter the new password in the **Confirm New Password** field.
7 Specify the following user privileges:
   - Select the maximum LAN user privilege level limit.
   - Select the maximum serial port user privilege granted.
   - On Dell PowerEdge *x9xx* systems, select Enable Serial Over LAN to enable Serial Over LAN.
8 Click **Apply Changes** to save changes.
9 Click **Back to Remote Access User Window** to go back to the **Remote Access Users** window.

NOTE: Six additional user entries are configurable when RAC is installed. This results in a total of 16 users. The same username and password rules apply to BMC and RAC users. When DRAC 5 is installed, all the 16 users entries are allocated to RAC.

Setting BMC Platform Event Filter Alerts

You can use the Server Administrator Instrumentation Service to configure the most relevant BMC features, such as Platform Event Filter (PEF) parameters and alert destinations.

1 Click the **System** object.
2 Click the **Alert Management** tab.
3 Click **Platform Events**.

   The **Platform Events** window allows you to take individual action on specific platform events. You can select those events for which you want to take shutdown actions and generate alerts for selected actions. You can also send alerts to specific IP address destinations of your choice.

   You can configure the following platform events.

   - Fan Probe Failure
   - Voltage Probe Failure
   - Discrete Voltage Probe Failure
   - Temperature Probe Warning
   - Temperature Probe Failure
   - Chassis Intrusion Detected
   - Redundancy Degraded
   - Redundancy Lost

- Processor Absent
- Processor Warning
- Processor Failure
- PS/VRM/DCtoDC Warning
- PS/VRM/DCtoDC Failure
- Hardware Log Failure
- Automatic System Recovery
- Battery Probe Warning
- Battery Probe Failure
- Power Supply Absent

NOTE: The **Enable Platform Event Filters Alerts** setting disables or enables platform event filter alert generation. It is independent of the individual platform event alert settings.

4 Choose the platform event for which you want to take shutdown actions or generate alerts for selected actions and click **Set Platform Events**.

The **Set Platform Events** window allows you to specify the actions to be taken if the system is to be shut down in response to a platform event.

5 Select one of the following actions:

- None
  Takes no action when the operating system is hung or has crashed.
- Reboot System
  Shuts down the operating system and initiates system startup, performing BIOS checks and reloading the operating system.
- Power Cycle System
  Turns the electrical power to the system off, pauses, turns the power on, and reboots the system. Power cycling is useful when you want to reinitialize system components such as hard drives.
- Power Off System
  Turns off the electrical power to the system.

NOTICE: If you select a Platform Event shutdown action other than none, your system will shut down forcefully when the specified event occurs. This shutdown is initiated by firmware and is done without first shutting down the operating system or any running applications.

6 Select the **Generate Alert** check box for the alerts to be sent.

NOTE: To generate an alert, you must select both **Generate Alert** and the **Enable Platform Events Alerts** settings.

7 Click **Apply Changes**.

8 Click **Go Back to Platform Events Page** to go back to the **Platform Event Filters** window.

Setting Platform Event Alert Destinations

You can also use the **Platform Event Filters** window to select a destination where an alert for a platform event is to be sent. Depending on the number of destinations that are displayed, you can configure a separate IP address for each destination address. A platform event alert will be sent to each destination IP address that you configure.

1. Click **Configure Destinations** in the **Platform Event Filters** window.

   The **Configure Destinations** window displays a number of destinations.

2. Click the number of the destination you want to configure.

   NOTE: The number of destinations that you can configure on a given system may vary.

3. Select the **Enable Destination** check-box.
4. Click **Destination Number** to enter an individual IP address for that destination. This IP address is the IP address to which the platform event alert will be sent.
5. Enter a value in the **Community String** field to act as a password to authenticate messages sent between a management station and a managed system. The community string (also called the community name) is sent in every packet between the management station and a managed system.
6. Click **Apply Changes**.
7. Click **Go Back to Platform Events Page** to go back to the **Platform Event Filters** window.

Configuring the BMC to use a Serial Over LAN (SOL) Connection

You can configure the BMC for communication over a serial over LAN connection.

1. Click the **System** object.
2. Click the **Main System Chassis** object.
3. Click the **Remote Access** object.
4. Click the **Configuration** tab.
5. Click **Serial Over LAN**.

   The **Serial Over LAN Configuration** window appears.

6. Configure the following details:
   - Enable Serial Over LAN
   - Baud Rate
   - Minimum Privilege Required
7. Click **Apply Changes.**
8. Click **Advanced Settings** to further configure BMC.

9 In the **Serial Over LAN Configuration Advanced Settings window**, you may configure the following information:

- Character Accumulate Interval
- Character Send Threshold

10 Click **Apply Changes.**

11 Click **Go Back to Serial Over LAN Configuration** to return to the **Serial Over LAN Configuration** window.

Configuring the BMC to use a Serial Port Connection

You can configure the BMC for communication over a serial port connection.

1 Click the **System** object.

2 Click the **Main System Chassis** object.

3 Click the **Remote Access** object.

4 Click the **Configuration** tab.

5 Click **Serial Port**.

6 In the **Serial Port Configuration** window, specify the following details:

- Connection Mode Setting
- Baud Rate
- Flow Control
- Channel Privilege Level Limit

7 Click **Apply Changes.**

8 Click **Terminal Mode Settings**.

In the **Terminal Mode Settings** window, you can configure terminal mode settings for the serial port.

Terminal mode is used for Intelligent Platform Interface Management (IPMI) messaging over the serial port using printable ASCII characters. Terminal mode also supports a limited number of text commands to support legacy, text-based environments. This environment is designed so that a simple terminal or terminal emulator can be used.

9 Specify the following customizations to increase compatibility with existing terminals:

- Line Editing
- Delete Control
- Echo Control
- Handshaking Control
- New Line Sequence
- Input New Line Sequence

10 Click **Apply Changes**.

11 Click **Back To Serial Port Configuration Window** to go to back to the **Serial Port Configuration** window.

Configuring the BMC to use a LAN Connection

You can configure the BMC for communication over a LAN connection.

1 Click the **System** object.

2 Click the **Main System Chassis** object.

3 Click the **Remote Access** object.

4 Click the **Configuration** tab.

5 Click **LAN**.

The LAN Configuration page appears.

NOTE: BMC management traffic will not function properly if the LAN on motherboard (LOM) is teamed with any network adapter add-in-cards.

6 Specify the following NIC configuration details:

- Enable NIC (This option is available on Dell PowerEdge *x9xx* systems and when DRAC is installed. Select this option for NIC teaming. In Dell PowerEdge *x9xx* systems, you can team NICs for added redundancy.)
- NIC Selection
- MAC Address
- Enable IPMI Over LAN
- IP Address Source
- IP Address
- Subnet Mask
- Gateway Address
- Channel Privilege Level Limit
- Encryption Key (This option is available on Dell PowerEdge *x9xx* systems.)

7 Specify the following optional VLAN configuration details:

- Enable VLAN ID
- VLAN ID
- Priority

8 Click **Apply Changes.**

9

Storage Management Service

Overview

The Storage Management Service provides RAID and non-RAID storage management that is integrated with Server Administrator. On Microsoft® Windows®, Red Hat® Enterprise Linux, and SUSE® Linux Enterprise Server, the Storage Management Service is installed using Typical or Custom Setup. The Storage Management Service provides storage management information in an integrated graphical view.

The Storage Management Service:

- Allows you to perform controller and enclosure functions for all supported RAID and non-RAID controllers and enclosures from a single graphical or command line interface without the use of the controller BIOS utilities.
- Enables you to view the status of local and remote storage attached to a monitored system.
- Supports SCSI, SATA, ATA, and SAS; however, Fibre Channel is not supported.
- Protects your data by configuring data redundancy, assigning hot spares, or rebuilding failed drives.
- Provides a graphical interface that is wizard-driven with features for novice and advanced users and detailed online help.
- Provides a command line interface that is fully featured and scriptable.
- Provides detailed online help.

See the *Server Administrator Command Line Interface User's Guide* for information about running Storage Management from the command line.

NOTICE: The Storage Management Service (Storage Management) enables you to perform storage tasks that are data-destructive. Storage Management should be used by experienced storage administrators who are familiar with their storage environment.

NOTE: For complete documentation on the Storage Management, see the Storage Management online help and the *Dell OpenManage Server Administrator Storage Management User's Guide*.

NOTE: The Storage Management Service is available on systems running Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.

NOTE: It is recommended that you use Red Hat Enterprise Linux version 3 (Update 6) or Red Hat Enterprise Linux version 4 for Storage Management Service.

When using the Storage Management, you can click **Help** on the global navigation bar for more detailed information about the specific window you are viewing. Help is available for all windows accessible to the user based on user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

Software Prerequisites

See the Storage Management readme (**readme_sm.txt**) and the Server Administrator readme (**readme_sa.txt**) for the complete software and hardware requirements. These files are available on the *Systems Management Consoles* CD.

Hardware Prerequisites

Installing Storage Management on a system that does not have a supported controller, or a controller that is not attached to storage is an unsupported configuration. For a list of the supported controllers and for other information about the Storage Management Service hardware requirements, see the Server Administrator (**readme_sa.txt**), and Storage Management readme (**readme_sm.txt**) files on the *Systems Management Consoles* CD.

Storage Management Service

Installing the Storage Management replaces any previous installation of the Array Manager managed system (server software) and console (client software) that resides on the system. If only the Array Manager console is installed on the system, then installing the Storage Management does not replace the Array Manager console.

The Storage Management Service provides advanced features for configuring a system's locally attached RAID and non-RAID disk storage. Storage Management enables you to perform controller and enclosure functions for all supported RAID and non-RAID controllers and PowerVault™ 2xxS and PowerVault MD1000 enclosures from the Server Administrator graphical interface without requiring use of the controller BIOS utilities.

Using the Storage Management Service, you can protect your data by configuring data-redundancy, assigning hot spares, or rebuilding failed drives. You can also perform data-destructive tasks such as deleting virtual disks or resetting the controller configuration. All users of the Storage Management Service should be familiar with their storage environment and storage management.

In addition to the Server Administrator interface features, the Storage Management Service provides wizard-driven features for novice and advanced users and detailed online help.

The Storage Management command line interface (CLI) provides extended options for the Server Administrator **omreport** and **omconfig** commands. These options provide a command line interface that is fully featured and scriptable.

The Storage Management Service supports SCSI, SATA, ATA, and SAS; however, Fibre Channel is not supported.

This release of Storage Management does not support Windows volume and disk management. For additional information, see "Storage Management Service."

Storage Management Service and Array Manager

The Dell OpenManage Storage Management is a replacement for Array Manager. The Storage Management Service provides similar storage management and configuration features as Array Manager. There are differences in the operating system support and other features. Do read the details on "Migrating from Array Manager to the Storage Management" and see the *Storage Management User's Guide* for more details.

Storage Management Tree Objects

When installed, the Storage Management Service is accessible by selecting the **Storage** tree object on the Server Administrator graphical user interface. The **Storage** object expands to display tree objects for the supported controllers attached to the system. The controller object expands to display the storage attached to the controller.

Depending on the controllers and storage attached to the system, the expanded **Storage** object may display the following lower-level objects:

- Controller
- Battery
- Connector
- Enclosure or Backplane
- Physical Disks
- EMMs (Enclosure Management Modules)
- Fans
- Power Supplies
- Temperatures
- Firmware/Driver Versions
- Virtual Disks

Health Tab

The **Health** tab for each tree object displays status information for the selected object.

Information/Configuration Tab

The **Information/Configuration** tab displays the property information for the selected tree object. When using the Storage Management Service, the **Information/Configuration** tabs also have drop-down menus and buttons for executing storage tasks and launching wizards.

Storage Management Tasks

The Storage Management Service has drop-down menus and wizards for executing storage management and configuration tasks. This section discusses some of the common storage tasks and wizards provided by the Storage Management Service.

NOTE: For complete documentation of the Storage Management storage tasks and other features, see the Storage Management online help.

Create Virtual Disk Wizard

The Storage Management Service provides an Express and an Advanced Create Virtual Disk Wizard. The Express Wizard calculates an appropriate virtual disk configuration based on the available space and controller considerations. When using the Express Wizard, you select the RAID level and size for the virtual disk. The Express Wizard selects a recommended disk configuration for you that matches your RAID level and size selection. The Express Wizard requires minimal user input and is recommended for novice users.

The Create Virtual Disk Advanced Wizard allows you to specify the read, write, and cache policy for the virtual disk. You can also select the physical disks and the controller connector to be used. You need a good knowledge of RAID levels and hardware to use the Advanced Wizard. This wizard is recommended for advanced users.

To launch the Express and Advanced Create Virtual Disk Wizards:

1. Expand the **Storage** tree object to display the controller objects.
2. Expand a controller object.
3. Select the **Virtual Disks** object.
4. Click **Go To Create Virtual Disk Wizard.**
5. See the Storage Management online help for more information.

Reconfigure Virtual Disk Wizard

The Reconfigure Virtual Disk Wizard enables you to change the virtual disk configuration. Using this task, you can change the RAID level or increase the virtual disk size by adding physical disks.

To launch the Reconfigure Virtual Disk Wizard:

1. Expand the **Storage** tree object to display the controller objects.
2. Expand a controller object.
3. Select the **Virtual Disks** object.

4 Select **Reconfigure** from the **Available Tasks** drop-down menu.

5 Click **Execute.**

6 See the Storage Management online help for more information.

Maintain Integrity of Redundant Virtual Disks

If you have created a redundant virtual disk, the Check Consistency task verifies the accuracy of the redundant (parity) information. This task only applies to redundant virtual disks. When necessary, the Check Consistency task rebuilds the redundant data.

To launch the Check Consistency task:

1 Expand the **Storage** tree object to display the controller objects.

2 Expand a controller object.

3 Select the **Virtual Disks** object.

4 Select **Check Consistency** from the **Available Tasks** drop-down menu.

5 Click **Execute.**

6 See the Storage Management online help for more information.

Assign and Unassign Global Hot Spare

A global hot spare is an unused backup disk that is part of the array group. Hot spares remain in standby mode. When a physical disk that is used in a virtual disk fails, the assigned hot spare is activated to replace the failed physical disk without interrupting the system or requiring your intervention. When a hot spare is activated, it rebuilds the data for all redundant virtual disks that were using the failed physical disk.

You can change the hot spare assignment by unassigning a disk and choosing another disk as needed. You can also assign more than one physical disk as a global hot spare.

Global hot spares must be assigned and unassigned manually. They are not assigned to specific virtual disks. If you want to assign a hot spare to a virtual disk (it will replace any physical disk that fails in the virtual disk) then use the instructions to assign and unassign dedicated hot spare.

To assign a dedicated hot spare

1 Select the disk in the **Connector** (channel or port) table that you want to use as the dedicated hot spare. On some controllers, more than one disk can be selected. The disks you have selected as dedicated hot spares are displayed in the **Disks currently configured as dedicated hot spare** table.

2 Click **Apply Changes** when ready.

To unassign a dedicated hot spare

1. Click the disk in the **Disks currently configured as dedicated hot spare** table to unassign it. Clicking the disk removes the disk from the **Disks currently configured as dedicated hot spare** table and returns it to the Connector (channel or port) table.
2. Click **Apply Changes** when ready.

To locate this task in Storage Management

1. Expand the **Storage** tree object to display the controller objects.
2. Expand a controller object.
3. Select the **Virtual Disks** object.
4. Select **Assign/Unassign Dedicated Hot Spare** from the **Available Tasks** drop-down menu.
5. Click **Execute**.

See the Storage Management online help for more information.

Rebuild a Failed Physical Disk

If the failed physical disk is part of a redundant virtual disk, then the physical disk failure should not result in data loss if replaced immediately. The rebuild task is available when the **Physical Disks** object is selected. See the Storage Management online help for more information.

Global Tasks

The following global tasks are available when the Storage object is selected. See the Storage Management online help for more information.

- **Global Rescan.** A global rescan updates configuration changes (such as new or removed devices) for all controllers and their attached components.
- **Enable and Disable Smart Thermal Shutdown.** By default, the operating system and server shut down when the PV220S and PV221S enclosures reach a critical temperature of 0 or 50 degrees celsius. Using the Enable Smart Thermal Shutdown task, however, you can specify that only the enclosure and not the operating system and server be shut down when the enclosure reaches a critical temperature. To restore the system to its default setting use the Disable Smart Thermal Shutdown task.

Controller Tasks

The following controller tasks are available when the **Controller** object is selected. See the Storage Management online help for more information.

- **Rescan Controller.** A controller rescan updates configuration changes (such as new or removed devices) for all components attached to the controller.
- **Create Virtual Disk.** See "Create Virtual Disk Wizard."

- **Enable, Disable, Quiet, and Test Alarm.** These tasks enable you to manage the controller alarm. For example, you can set the alarm to sound in the event of a device failure or quiet the alarm once it is sounding.
- **Set Rebuild Rate.** The rebuild rate refers to how much of the system's resources are dedicated to rebuilding a failed physical disk. This task enables you to adjust this setting.
- **Reset Configuration.** This task erases all information on the controller, so that you can perform a fresh configuration. This operation destroys all virtual disks on the controller.
- **Export Log File.** This task exports the controller log to a text file.
- **Import Foreign Configuration.** This task imports virtual disks that reside on physical disks that have been moved from another controller.
- **Clear Foreign Configuration.** Use the clear foreign configuration task to clear or erase the virtual disk information from the newly attached physical disks.
- **Set Background Initialization Rate.** This task changes the amount of system resources dedicated to the background initialization task.
- **Set Check Consistency Rate.** This task changes the amount of system resources dedicated to the check consistency task.
- **Set Reconstruct Rate.** This task changes the amount of system resources dedicated to the reconstruct task.
- **Set Patrol Read Mode.** This feature identifies disk errors in order to avoid disk failures and data loss or corruption.
- **Start and Stop Patrol Read.** These tasks enable you start a Patrol Read task or stop a running task when the Patrol Read mode is set to manual.

Battery Tasks

The following battery tasks are available when the **Battery** object is selected. This task is only available for controllers that have batteries that require reconditioning. See the Storage Management online help for more information.

- **Recondition Battery.** This task fully discharges and recharges the controller battery.
- **Start Learn Cycle.** Use the Start Learn Cycle task to initiate the battery Learn cycle.
- **Battery Delay Learn Cycle.** Use this task to delay the start time of the Learn cycle for up to seven days.

Connector Tasks

The following connector tasks are available when the **Connector** object is selected. See the Storage Management online help for more information.

- **Rescan Connector.** This task rescans the controller connectors to verify the currently connected devices or to recognize new devices that have been added to the connectors. Performing a rescan on a connector is similar to performing a rescan on the controller.

Enclosure Tasks

The following enclosure tasks are available when the **Enclosure** object is selected. See the Storage Management online help for more information.

- **Enable and Disable Alarm.** Use these tasks to manage the enclosure alarm. When enabled, the alarm sounds when the enclosure encounters an error condition.
- **Set Asset Data.** Use this task to change the enclosure's asset tag and asset name.
- **Set Temperature Probe Values.** The temperature probes monitor the enclosure's temperature. Each temperature probe has a Warning and a Failure threshold. The Warning threshold indicates that the enclosure is approaching an unacceptably warm or cool temperature. Use this task to modify the Warning threshold.
- **Blink.** Use the Blink task to blink the light-emitting diodes (LEDs) on the enclosure. You may want to use this task to locate an enclosure. The LEDs on the enclosure may display different colors and blinking patterns.

Temperatures Tasks

The following temperature probe tasks are available when the **Temperatures** object is selected. See the Storage Management online help for more information.

- **Set Temperature Probe.** The temperature probes monitor the enclosure's temperature. Each temperature probe has a Warning and a Failure threshold. The Warning threshold indicates that the enclosure is approaching an unacceptably warm or cool temperature. Use this task to modify the Warning threshold.

Physical Disk Tasks

The following physical disk tasks are available when the **Physical Disks** object is selected. See the Storage Management online help for more information.

- **Blink and Unblink.** The Blink task allows you to find a disk within an enclosure by blinking one of the light-emitting diodes (LEDs) on the disk. The Unblink task cancels the Blink task.
- **Remove Dead Segments.** In certain circumstances, this task enables you to recover disk space that is currently unusable.
- **Assign and Unassign Global Hot Spare.** See "Assign and Unassign Global Hot Spare."
- **Prepare to Remove.** Use this task before removing a disk from an enclosure. It is recommended that you perform this task before removing a disk to prevent data loss.
- **Online and Offline.** Use the Offline task to deactivate a disk before removing it. Use the Online task to reactivate an offline disk.

- **Initialize.** On some controllers, the Initialize task prepares a physical disk for use as a member of a virtual disk.
- **Rebuild.** See "Rebuild a Failed Physical Disk."
- **Cancel Rebuild.** Use the Cancel Rebuild task to cancel a rebuild that is in progress.
- **Clear Physical Disk and Cancel Clear.** Use the clear physical disk task to erase data residing on an physical disk.

Virtual Disk Tasks

The following virtual disk tasks are available when the **Virtual Disks** object is selected. See the Storage Management online help for more information.

- **Reconfigure.** See "Reconfigure Virtual Disk Wizard."
- **Cancel Rebuild.** Use the Cancel Rebuild task to cancel a rebuild while it is in progress.
- **Cancel Reconfigure.** Use the Cancel Reconfigure task to cancel a virtual disk reconfiguration while it is in progress.
- **Format and Initialize; Slow and Fast Initialize.** Use the Format or Initialize; Slow and Fast Initialize task to erase files and remove the file systems on a virtual disk.
- **Cancel Background Initialization.** On some controllers, background initialization of redundant virtual disks begins automatically after the virtual disk is created. Use this task if you need to cancel the background initialization.
- **Restore Dead Segments.** Use the Restore Dead Segments task to recover data from a RAID-5 virtual disk that has been corrupted.
- **Delete.** Use this task to destroy all data on the virtual disk.
- **Assign and Unassign Dedicated Hot Spare.** See "Assign and Unassign Global Hot Spare."
- **Check Consistency, Cancel Check Consistency, Pause Check Consistency, and Resume Check Consistency.** See "Maintain Integrity of Redundant Virtual Disks."
- **Blink and Unblink.** The Blink and Unblink tasks blink or unblink the lights on the physical disks included in the virtual disk.
- **Rename.** Use this task to rename a virtual disk.
- **Change Policy.** Use this task to change a virtual disk's read, write, or cache policy.
- **Split Mirror.** Use this task to separate mirrored data originally configured as a RAID 1, RAID 1-concatenated, or RAID 10 virtual disk.
- **Unmirror.** Use this task to separate mirrored data and restore one half of the mirror to free space.

Additional Storage Management Features and Documentation

For complete documentation on the Storage Management Service, see the Storage Management online help and the *Dell OpenManage Server Administrator Storage Management User's Guide*. For information on how to launch the online help, see "Displaying Online Help."

Migrating from Array Manager to the Storage Management

If you replace an existing Array Manager installation with Storage Management, the following migration considerations apply:

- **Virtual Disk Preservation**. You can preserve the virtual disk names when migrating from Array Manager to Storage Management. To do so, however, you must not uninstall Array Manager prior to installing Storage Management. If Array Manager is uninstalled prior to installing Storage Management, then Storage Management will rename the virtual disks created with Array Manager. Whether or not Array Manager is uninstalled, Storage Management will be able to identify and manage the virtual disks created with Array Manager.
- **SNMP Traps**. The architecture for handling the SNMP traps and the Management Information Base (MIB) is different in Storage Management than Array Manager. You may need to modify applications that have been customized to receive SNMP traps from Array Manager.
- **Event Numbering.** The numbering scheme for Storage Management alerts or events is different than the numbers used for the corresponding Array Manager events. See the Storage Management online help for more information.

Storage Management Command Line Interface

See the *Server Administrator Command Line Interface User's Guide* for information about running the Storage Management Service from the command line. If you have the Storage Management installed, you can also refer to the online help for information about the expanded **omreport** and **omconfig** command line options.

Displaying Online Help

Server Administrator provides context-sensitive online help. To access the online help, click **Help** on the global navigation bar. This navigation is available for all windows accessible to the user based on user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

The Storage Management provides additional online help. This help is available when the **Storage** or a lower-level tree object is selected.

The online help of the Storage Management Service:

- Provides conceptual information on storage concepts such as virtual disks, RAID, and so on
- Describes the graphical user interface components in the various windows of the application
- Gives detailed, step-by-step instructions on the tasks that you can perform in the graphical user interface
- Describes the available CLI commands and their subcommands

The Storage Management online help is available in two formats:

- **Context-sensitive Help**. To access the context-sensitive online help, click **Help** on the global navigation bar.
- **Table of Contents**. The help screens for the context-sensitive help contain links to the online help Table of Contents. To access the Table of Contents, first click **Help** on the global navigation bar. Next, click the **Back to Storage Management Contents Page** link to display the Table of Contents. This link is displayed at the top and bottom of each help screen. Use the Table of Contents to access all topics covered in the online help.

10

Server Administrator Logs

Overview

Server Administrator allows you view and manage hardware, alert, POST, and command logs. All users can access logs and print reports from either the Server Administrator home page or from its command line interface. Users must be logged in with Admin privileges to clear logs or must be logged in with Admin or Power User privileges to e-mail logs to their designated service contact.

See the *Server Administrator Command Line Interface User's Guide* for information about viewing logs and creating reports from the command line.

When viewing Server Administrator logs, you can click **Help** on the global navigation bar for more detailed information about the specific window you are viewing. Server Administrator log help is available for all windows accessible to the user based on user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed system.

Integrated Features

Clicking a column heading sorts by the column or changes the sort direction of the column. Additionally, each log window contains several task buttons that can be used for managing and supporting your system.

Log Window Task Buttons

- Click **Print** to print a copy of the log to your default printer.
- Click **Export** to save a text file containing the log data (with the values of each data field separated by a customizable delimiter) to a destination you specify.
- Click **Email** to create an e-mail message that includes the log content as an attachment.
- Click **Clear Log** to erase all events from the log.
- Click **Save As** to save the log content in a **.zip** file.
- Click **Refresh** to reload the log content in the action window data area.

See "Task Buttons" for additional information about using the task buttons.

Server Administrator Logs

Server Administrator provides the following logs:

- Hardware Log
- Alert Log
- POST Log
- Command Log

Hardware Log

Use the hardware log to look for potential problems with your system's hardware components. On Dell™ PowerEdge™ *x8xx* and *x9xx* systems, the hardware log status indicator will change to a red X ( )when the log file reaches 100 percent capacity. There are two available hardware logs, depending on your system: the Embedded System Management (ESM) log and the System Event Log (SEL). The ESM log and SEL are each a set of embedded instructions that can send hardware status messages to systems management software. Each component listed in the logs has a status indicator icon next to its name. A green check mark ( ) indicates that a component is healthy (normal). A yellow triangle containing an exclamation point ( ) indicates that a component has a warning (noncritical) condition and requires prompt attention. A red X ( ) indicates that a component has a critical (failure) condition and requires immediate attention. A blank space ( ) indicates that a component's health status is unknown.

To access the hardware log, click **System**, click the **Logs** tab, and click **Hardware**.

Information displayed in the ESM and SEL logs includes:

- The severity level of the event
- The date and time that the event was captured
- A description of the event

Maintaining the Hardware Log

The status indicator icon next to the log name on the Server Administrator homepage will change from a green check mark ( ) to a yellow triangle containing an exclamation point ( ) when the log file reaches 80 percent capacity. Be sure to clear the hardware log when it reaches 80 percent capacity. If the log is allowed to reach 100 percent capacity, the latest events are discarded from the log.

Alert Log

NOTE: If the Alert log displays invalid XML data (for example, when the XML data generated for the selection is not well formed), click **Clear Log** and then redisplay the log information.

Use the Alert log to monitor various system events. The Server Administrator generates events in response to changes in the status of sensors and other monitored parameters. Each status change event recorded in the Alert log consists of a unique identifier called the event ID for a specific event source

category and an event message that describes the event. The event ID and message uniquely describe the severity and cause of the event and provide other relevant information such as the location of the event and the monitored component's previous state.

To access the Alert log, click **System**, click the **Logs** tab, and click **Alert**.

Information displayed in the Alert log includes:

- The severity level of the event
- The event ID
- The date and time that the event was captured
- The category of the event
- A description of the event

NOTE: The log history may be required for future troubleshooting and diagnostic purposes. Therefore, it is recommended that you save the log files.

See the *Server Administrator Messages Reference Guide* for detailed information about alert messages.

POST Log

Use the POST log to view and analyze events from the POST that your system performs during boot. Before the operating system loads when you turn on your system, the POST tests various system components, such as RAM, the hard drives, and the keyboard.

NOTE: The POST log is not supported on all systems.

To access the POST log, click **System**, click the **Logs** tab, and click **POST**.

Information displayed in the POST log includes:

- The POST code
- A description of the code

Command Log

NOTE: If the Command log displays invalid XML data (for example, when XML data generated for the selection is not well formed), click **Clear Log** and then redisplay the log information.

Use the Command log to monitor all of the commands issued by Server Administrator users. The Command log tracks logins, logouts, systems management software initialization, and shutdowns initiated by systems management software, and records the last time the log was cleared.

To access the Command log, click **System**, click the **Logs** tab, and click **Command**.

Information displayed in the Command log includes:

- The date and time that the command was invoked
- The user that is currently logged into the Server Administrator home page or the CLI
- A description of the command and its related values

NOTE: The log history may be required for future troubleshooting and diagnostic purposes. Therefore, it is recommended that you save the log files.

11

Troubleshooting

Setting Alert Actions for Systems Running Supported Red Hat® Enterprise Linux and SUSE® Linux Enterprise Server Operating Systems

When you set Alert Actions for an event, you can specify the action to "display an alert on the server." To perform this action, Server Administrator writes a message to **/dev/console**. If the Server Administrator system is running an X Window System, you will not see that message by default. To see the alert message on a Red Hat Enterprise Linux system when the X Window System is running, you must start **xconsole** or **xterm -C** before the event occurs. To see the alert message on a SUSE Linux Enterprise Server system when the X Window System is running, you must start **xterm -C** before the event occurs.

When you set Alert Actions for an event, you can specify the action to "broadcast a message." To perform this action, Server Administrator executes the **wall** command, which sends the message to everybody logged in with their message permission set to "yes." If the Server Administrator system is running an X Window System, you will not see that message by default. To see the broadcast message when the X Window System is running, you must start a terminal such as **xterm** or **gnome-terminal** before the event occurs.

NOTE: On SUSE Linux Enterprise Server (Version 9), messages sent by **wall** are displayed by the **xterm** terminal program but not by the **Konsole** terminal program.

When you set Alert Actions for an event, you can specify the action to "execute an application." There are limitations on the applications that Server Administrator can execute. Follow these guidelines to ensure proper execution:

- Do not specify X Window System based applications because Server Administrator cannot execute such applications properly.
- Do not specify applications that require input from the user because Server Administrator cannot execute such applications properly.

- Redirect **stdout** and **stderr** to a file when specifying the application so that you can see any output or error messages.
- If you want to execute multiple applications (or commands) for an alert, create a script to do that and put the full path to the script in the "application to execute" box.

  Example 1:

  ```
  ps -ef >/tmp/psout.txt 2>&1
  ```

  The command in Example 1 executes the application **ps**, redirects **stdout** to the file **/tmp/psout.txt**, and redirects **stderr** to the same file as **stdout**.

  Example 2:

  ```
  mail -s "Server Alert" admin </tmp/alertmsg.txt >/tmp/mailout.txt
  2>&1
  ```

  The command in Example 2 executes the mail application to send the message contained in the file **/tmp/alertmsg.txt** to Red Hat Enterprise Linux user or SUSE Linux Enterprise Server user, and Administrator, with the subject "Server Alert." The file **/tmp/alertmsg.txt** must be created by the user before the event occurs. In addition, **stdout** and **stderr** are redirected to the file **/tmp/mailout.txt** in case an error occurs.

BMC Platform Events Filter Alert Messages

All possible Platform Event Filter (PEF) messages along with a description of each event is listed in Table 11-1.

Table 11-1. BMC PEF Alert Events

Event	Description
Fan Probe Failure	The fan is running too slow or not at all.
Voltage Probe Failure	The voltage is too low for proper operation.
Discrete Voltage Probe Failure	The voltage is too low for proper operation.
Temperature Probe Warning	The temperature is approaching excessively high or low limits.
Temperature Probe Failure	The temperature is either too high or too low for proper operation.
Chassis Intrusion Detected	The system chassis has been opened.
Redundancy (PS or Fan) Degraded	Redundancy for the fans and/or power supplies has been reduced.
Redundancy (PS or Fan) Lost	No redundancy remains for the system's fans and/or power supplies.
Processor Warning	A processor is running at less than peak performance or speed.
Processor Failure	A processor has failed.

Table 11-1. BMC PEF Alert Events *(continued)*

Event	Description
PPS/VRM/DCtoDC Warning	The power supply, voltage regulator module, or DC to DC converter is pending a failure condition.
Power Supply/VRM/D2D Failure	The power supply, voltage regulator module, or DC to DC converter has failed.
Hardware log is full or emptied	Either an empty or a full hardware log requires administrator attention.
Automatic System Recovery	The system is hung or is not responding and is taking an action configured by Automatic System Recovery.

Understanding Service Names

The service executable and display names of the following services have changed:

Table 11-2. Service Names

Purpose	Service Name	Previous Release	Current Release
Web Server			
	Display Name	Secure Port Server	DSM SA Connection Service
	Executable Name	Omaws[32|64]	dsm_om_connsvc[32|64] dsm_om_connsvc
Scheduling or Notification			
	Display Name	OM Common Services	DSM SA Shared Services
	Executable Name	Omsad[32|64]	dsm_om_shrsvc[32|64] dsm_om_shrsvc

Fixing a Faulty Server Administrator Installation on Supported Windows Operating Systems

You can fix a faulty installation by forcing a reinstall and then performing an uninstall of Server Administrator.

To force a reinstall:

1. Find out the version of Server Administrator that was previously installed
2. Download the installation package for that version from the Dell Support website at **support.dell.com**
3. Locate **SysMgmt.msi** from the **srvadmin\windows\SystemsManagement** directory

4 Type the following command at the command prompt to force a reinstall

```
msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vamus
```

5 Select **Custom Setup** and choose all the features that were originally installed. If you are not sure which features were installed, select all features and perform the installation.

NOTE: If you installed Server Administrator in a non-default directory, make sure to change it in the **Custom Setup** as well.

6 Once the application is installed, you can uninstall Server Administrator using Add/Remove Programs.

Glossary

The following list defines or identifies technical terms, abbreviations, and acronyms used in your system documents.

A
Abbreviation for ampere(s).

AC
Abbreviation for alternating current.

AC power switch
A switch with two AC power inputs that provides AC power redundancy by failing over to a standby AC input in the event of a failure to the primary AC input.

access
Refers to the actions a user can take on a variable value. Examples include read-only and read-write.

ACL
Abbreviation for access control list. ACL files are text files that contain lists that define who can access resources stored on a Novell® Web server.

adapter card
An expansion card that plugs into an expansion-card connector on the system's system board. An adapter card adds some specialized function to the system by providing an interface between the expansion bus and a peripheral device. Examples of adapter cards include network cards, sound cards, and SCSI adapters.

ADB
Abbreviation for assign database.

AGP
Abbreviation for advanced graphics port.

ASCII
Acronym for American Standard Code for Information Interchange. A text file containing only characters from the ASCII character set (usually created with a text editor, such as Notepad in Microsoft® Windows®), is called an ASCII file.

ASIC
Acronym for application-specific integrated circuit.

ASPI
Acronym for advanced SCSI programming interface.

asset tag code
An individual code assigned to a system, usually by a system administrator, for security or tracking purposes.

attribute
An attribute, or property, contains a specific piece of information about a manageable component. Attributes can be combined to form groups. If an attribute is defined as read-write, it may be defined by a management application.

autoexec.bat file
The **autoexec.bat** file is executed when you boot your system (after executing any commands in the **config.sys** file). This start-up file contains commands that define the characteristics of each device connected to your system, and it finds and executes programs stored in locations other than the active directory.

backup
A copy of a program or data file. As a precaution, you should back up your system's hard drive on a regular basis. Before making a change to the configuration of your system, you should back up important start-up files from your operating system.

baud rate
A measurement of data transmission speed. For example, modems are designed to transmit data at one or more specified baud rate(s) through the COM (serial) port of a system.

beep code
A diagnostic message in the form of a pattern of beeps from your system's speaker. For example, one beep, followed by a second beep, and then a burst of three beeps is beep code 1-1-3.

BGA
Abbreviation for ball grid array, an integrated circuit (IC) package that uses an array of solder balls, instead of pins, to connect to a system board.

binary
A base-2 numbering system that uses 0 and 1 to represent information. The system performs operations based on the ordering and calculation of these numbers.

BIOS
Acronym for basic input/output system. Your system's BIOS contains programs stored on a flash memory chip. The BIOS controls the following:

- Communications between the microprocessor and peripheral devices, such as the keyboard and the video adapter
- Miscellaneous functions, such as system messages

bit
The smallest unit of information interpreted by your system.

BMC
Abbreviation for baseboard management controller, which is a controller that provides the intelligence in the IPMI structure.

boot routine
When you start your system, it clears all memory, initializes devices, and loads the operating system. Unless the operating system fails to respond, you can reboot (also called warm boot) your system by pressing <Ctrl><Alt><Del>; otherwise, you must perform a cold boot by pressing the reset button or by turning the system off and then back on.

bootable diskette
You can start your system from a diskette. To make a bootable diskette, insert a diskette in the diskette drive, type `sys a:` at the command line prompt, and press <Enter>. Use this bootable diskette if your system will not boot from the hard drive.

bpi
Abbreviation for bits per inch.

bps
Abbreviation for bits per second.

BTU
Abbreviation for British thermal unit.

bus
An information pathway between the components of a system. Your system contains an expansion bus that allows the microprocessor to communicate with controllers for all the various peripheral devices connected to the system. Your system also contains an address bus and a data bus for communications between the microprocessor and RAM.

byte
Eight contiguous bits of information, the basic data unit used by your system.

C
Abbreviation for Celsius.

CA
Abbreviation for certification authority.

cache
A fast storage area that keeps a copy of data or instructions for quicker data retrieval. For example, your system's BIOS may cache ROM code in faster RAM. Or, a disk-cache utility may reserve RAM in which to store frequently accessed information from your system's disk drives; when a program makes a request to a disk drive for data that is in the cache, the disk-cache utility can retrieve the data from RAM faster than from the disk drive.

capability
Refers to the actions that an object can perform, or actions that can be taken on a managed object. For example, if a card is hot-pluggable, it is capable of being replaced while the system power is on.

CDRAM
Abbreviation for cached DRAM, which is a high-speed DRAM memory chip developed by Mitsubishi that includes a small SRAM cache.

CD-ROM
Abbreviation for compact disc read-only memory. CD drives use optical technology to read data from CDs. CDs are read-only storage devices; you cannot write new data to a CD with standard CD drives.

CHAP
Acronym for Challenge-Handshake Authentication Protocol, an authentication scheme used by PPP servers to validate the identity of the originator of the connection upon connection or any time later.

chip
A set of microminiaturized, electronic circuits that are designed for use as processors and memory in systems. Small chips can hold from a handful to tens of thousands of transistors. They look like tiny chips of aluminum, no more than 1/16 inch square by 1/30 inch thick, which is where the term "chip" came from. Large chips, which can be more than a half inch square, hold millions of transistors. It is actually only the top one thousandth of an inch of a chip's surface that holds the circuits. The rest of it is just a base.

CIM
Acronym for Common Information Model, which is a model for describing management information from the DMTF. CIM is implementation independent, allowing different management applications to collect the required data from a variety of sources. CIM includes schemas for systems, networks, applications and devices, and new schemas will be added. It provides mapping techniques for interchange of CIM data with MIB data from SNMP agents.

CIMOM
Acronym for common information model object manager.

CI/O
Abbreviation for comprehensive input/output.

CLI
Abbreviation for command line interface.

cm
Abbreviation for centimeter(s).

CMOS
Acronym for complementary metal-oxide semiconductor. In systems, CMOS memory chips are often used for NVRAM storage.

COM*n*
The device names for the first through fourth serial ports on your system are COM1, COM2, COM3, and COM4. The default interrupt for COM1 and COM3 is IRQ4, and the default interrupt for COM2 and COM4 is IRQ3. Therefore, you must be careful when configuring software that runs a serial device so that you don't create an interrupt conflict.

config.sys file
The **config.sys** file is executed when you boot your system (before running any commands in the **autoexec.bat** file). This start-up file contains commands that specify which devices to install and which drivers to use. This file also contains commands that determine how the operating system uses memory and controls files.

ConsoleOne
Novell ConsoleOne is a Java-based foundation for graphical utilities that manage and administer network resources from different locations and platforms. ConsoleOne provides a single point of control for all Novell and external products.

controller
A chip that controls the transfer of data between the microprocessor and memory or between the microprocessor and a peripheral device such as a disk drive or the keyboard.

control panel
The part of the system that contains indicators and controls, such as the power switch, hard drive access indicator, and power indicator.

conventional memory
The first 640 KB of RAM. Conventional memory is found in all systems. Unless they are specially designed, MS-DOS® programs are limited to running in conventional memory.

COO
Abbreviation for cost of ownership.

cooling unit
Sets of fans or other cooling devices in a system chassis.

coprocessor
A chip that relieves the system's microprocessor of specific processing tasks. A math coprocessor, for example, handles numeric processing. A graphics coprocessor handles video rendering. The Intel® Pentium® microprocessor, for example, includes a built-in math coprocessor.

cpi
Abbreviation for characters per inch.

CPU
Abbreviation for central processing unit. See also microprocessor.

CRC
Abbreviation for cyclic redundancy code, which is a number derived from, and stored or transmitted with, a block of data in order to detect corruption. By recalculating the CRC and comparing it to the value originally transmitted, the receiver can detect some types of transmission errors.

CSR
Abbreviation for certificate signing request.

cursor
A marker, such as a block, underscore, or pointer that represents the position at which the next keyboard or mouse action will occur.

DAT
Acronym for digital audio tape.

dB
Abbreviation for decibel(s).

dBA
Abbreviation for adjusted decibel(s).

DBS
Abbreviation for Demand Based Switching. DBS is power management performed by switching to a low power state (frequency and voltage) when the processor utilization is low. It maintains application performance while lowering the average system power.

DC
Abbreviation for direct current.

Also, abbreviation for Dual Channel.

device driver
A program that allows the operating system or some other program to interface correctly with a peripheral device, such as a printer. Some device drivers—such as network drivers—must be loaded from the config.sys file (with a device= statement) or as memory-resident programs (usually, from the autoexec.bat file).

Others—such as video drivers—must load when you start the program for which they were designed.

DHCP
Abbreviation for Dynamic Host Configuration Protocol, a protocol that provides a means to dynamically allocate IP addresses to computers on a LAN.

DIMM
Acronym for dual in-line memory module. A small circuit board containing DRAM chips that connects to the system board.

DIN
Acronym for Deutsche Industrie Norm which is the standards-setting organization for Germany. A DIN connector is a connector that conforms to one of the many standards defined by DIN. DIN connectors are used widely in personal computers. For example, the keyboard connector for personal computers is a DIN connector.

DIP
Acronym for dual in-line package. A circuit board, such as a system board or expansion card, may contain DIP switches for configuring the circuit board. DIP switches are always toggle switches, with an on position and an off position.

directory
Directories help keep related files organized on a disk in a hierarchical, "inverted tree" structure. Each disk has a "root" directory; for example, a C:\> prompt normally indicates that you are at the root directory of hard drive C. Additional directories that branch off of the root directory are called subdirectories. Subdirectories may contain additional directories branching off of them.

display adapter
See video adapter.

DKS
Abbreviation for dynamic kernel support.

DMA
Abbreviation for direct memory access. A DMA channel allows certain types of data transfer between RAM and a device to bypass the microprocessor.

DMTF
Abbreviation for Distributed Management Task Force, a consortium of companies representing hardware and software providers.

dpi
Abbreviation for dots per inch.

DPMS
Abbreviation for Display Power Management Signaling. A standard developed by the Video Electronics Standards Association (VESA®) that defines the hardware signals sent by a video controller to activate power management states in a monitor. A monitor is said to be DPMS-compliant when it is designed to enter a power management state after receiving the appropriate signal from a system's video controller.

DRAC 4
Acronym for Dell™ Remote Access Controller 4.

DRAC 5
Acronym for Dell Remote Access Controller 5.

DRAC II
Acronym for Dell OpenManage™ Remote Assistant Card II.

DRAC III
Acronym for Dell Remote Access Card III.

DRAC III/XT
Acronym for Dell Remote Access Card III/XT.

DRAM
Acronym for dynamic random-access memory. A system's RAM is usually made up entirely of DRAM chips. Because DRAM chips cannot store an electrical charge indefinitely, your system continually refreshes each DRAM chip in the system.

drive-type number
Your system can recognize a number of specific hard drives. Each is assigned a drive-type number that is stored in NVRAM. The hard drive(s) specified in your system's System Setup program must match the actual drive(s) installed in the system. The System Setup program also allows you to specify physical parameters (logical cylinders, logical heads, cylinder number, and logical sectors per pack) for drives not included in the table of drive types stored in NVRAM.

DTE
Abbreviation for data terminal equipment. Any device, such as a computer system, that can send data in digital form by means of a cable or communications line. The DTE is connected to the cable or communications line through a data communications equipment (DCE) device, such as a modem.

ECC
Abbreviation for error checking and correction.

ECP
Abbreviation for Extended Capabilities Port.

EDO
Acronym for extended data output dynamic random access memory which is a type of DRAM that is faster than conventional DRAM. EDO RAM can start fetching the next block of memory at the same time that it sends the previous block to the microprocessor.

EEPROM
Acronym for electrically erasable programmable read-only memory.

EIDE
Abbreviation for enhanced integrated drive electronics. EIDE devices add one or more of the following enhancements to the traditional IDE standard:

- Data transfer rates of up to 16 MB/sec
- Support for drives other than just hard drives, such as CD and tape drives
- Support for hard drives with capacities greater than 528 MB
- Support for up to two controllers, each with up to two devices attached

EISA
Acronym for Extended Industry-Standard Architecture, a 32-bit expansion-bus design. The expansion-card connectors in an EISA system are also compatible with 8- or 16-bit ISA expansion cards.

To avoid a configuration conflict when installing an EISA expansion card, you must use the EISA Configuration Utility. This utility allows you to specify which expansion slot contains the card and obtains information about the card's required system resources from a corresponding EISA configuration file.

EMC
Abbreviation for electromagnetic compatibility.

EMI
Abbreviation for electromagnetic interference.

EMM
Abbreviation for expanded memory manager. A utility that uses extended memory to emulate expanded memory on systems with an Intel386™ or higher microprocessor.

EMS
Abbreviation for Expanded Memory Specification.

EPP
Abbreviation for Enhanced Parallel Port which provides improved bidirectional data transmission. Many devices are designed to take advantage of the EPP standard, especially devices, such as network or SCSI adapters that connect to the parallel port of a portable computer.

EPROM
Acronym for erasable programmable read-only memory.

ERA
Abbreviation for embedded remote access.

ERA/MC
Abbreviation for embedded remote access modular computer. See modular system.

ERA/O
Abbreviation for embedded remote access option.

ESD
Abbreviation for electrostatic discharge.

ESM
Abbreviation for embedded systems management.

expanded memory
A technique for accessing RAM above 1 MB. To enable expanded memory on your system, you must use an EMM. You should configure your system to support expanded memory only if you run application programs that can use (or require) expanded memory.

expansion bus
Your system contains an expansion bus that allows the microprocessor to communicate with controllers for peripheral devices, such as a network card or an internal modem.

expansion-card connector
A connector on the system's system board or riser board for plugging in an expansion card.

extended memory
RAM above 1 MB. Most software that can use it, such as the Windows operating system, requires that extended memory be under the control of an XMM.

external cache memory
A RAM cache using SRAM chips. Because SRAM chips operate at several times the speed of DRAM chips, the microprocessor can retrieve data and instructions faster from external cache memory than from RAM.

F
Abbreviation for Fahrenheit.

FAT
Acronym for file allocation table. FAT and FAT32 are file systems that are defined as follows:

- **FAT** — A file system used by MS-DOS, Windows 3.*x*, Windows 95, and Windows 98. Windows NT® and Windows 2000 also can use the FAT file system. The operating system maintains a table to keep track of the status of various segments of disk space used for file storage.
- **FAT32** — A derivative of the FAT file system. FAT32 supports smaller cluster sizes than FAT, thus providing more efficient space allocation on FAT32 drives.

FCC
Abbreviation for Federal Communications Commission.

FEPROM
Acronym for flash erasable programmable read-only memory. Flash memory is a kind of nonvolatile storage device similar to EEPROM, but the erasing is done only in blocks or the entire chip.

Fibre Channel
A data transfer interface technology that allows for high-speed I/O and networking functionality in a single connectivity technology. The Fibre Channel Standard supports several topologies, including Fibre Channel Point-to-Point, Fibre Channel Fabric (generic switching topology), and Fibre Channel Arbitrated Loop (FC_AL).

firmware
Software (programs or data) that has been written onto read-only memory (ROM). Firmware can boot and operate a device. Each controller contains firmware which helps provide the controller's functionality.

flash bios
A BIOS that is stored in flash memory rather than in ROM. A flash BIOS chip can be updated in place, whereas a ROM BIOS must be replaced with a newer chip.

flash memory
A type of EEPROM chip that can be reprogrammed from a utility on diskette while still installed in a system; most EEPROM chips can only be rewritten with special programming equipment.

format
To prepare a hard drive or diskette for storing files. An unconditional format deletes all data stored on the disk.

FPBGA
Abbreviation for field programmable gate array, a programmable logic chip (PLD) with a high density of gates.

FRU
Abbreviation for field replaceable unit.

ft
Abbreviation for feet.

FTP
Abbreviation for file transfer protocol.

g
Abbreviation for gram(s).

G
Abbreviation for gravities.

GB
Abbreviation for gigabyte(s). A gigabyte equals 1024 megabytes or 1,073,741,824 bytes.

gcc
Abbreviation for gnu C compiler.

graphics coprocessor
See coprocessor.

graphics mode
A video mode that can be defined as x horizontal by y vertical pixels by z colors.

GUI
Acronym for graphical user interface.

h
Abbreviation for hexadecimal. A base-16 numbering system, often used in programming to identify addresses in the system's RAM and I/O memory addresses for devices. The sequence of decimal numbers from 0 through 16, for example, is expressed in hexadecimal notation as: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10. In text, hexadecimal numbers are often followed by h.

HBA
Abbreviation for host bus adapter. A PCI adapter card that resides in the system whose only function is to convert data commands from PCI-bus format to storage interconnect format (examples: SCSI, Fibre Channel) and communicate directly with hard drives, tape drives, CD drives, or other storage devices.

heat sink
A metal plate with metal pegs or ribs that help dissipate heat. Most microprocessors include a heat sink.

HMA
Abbreviation for high memory area. The first 64 KB of extended memory above 1 MB. A memory manager that conforms to the XMS can make the HMA a direct extension of conventional memory. Also see XMM.

host adapter
A host adapter implements communication between the system's bus and the controller for a peripheral device. (hard drive controller subsystems include integrated host adapter circuitry.) To add a SCSI expansion bus to your system, you must install or connect the appropriate host adapter.

hot plug
The ability to remove and replace a redundant part while the system is still running. Also called a "hot spare."

HPFS
Abbreviation for the High Performance File System option in the Windows NT operating systems.

HTTP
Abbreviation for Hypertext Transfer Protocol. HTTP is the client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents.

HTTPS
Abbreviation for HyperText Transmission Protocol, Secure. HTTPS is a variant of HTTP used by Web browsers for handling secure transactions. HTTPS is a unique protocol that is simply SSL underneath HTTP. You need to use "https://" for HTTP URLs with SSL, whereas you continue to use "http://" for HTTP URLs without SSL.

Hz
Abbreviation for hertz.

ICES
Abbreviation for Interference Causing Equipment Standard (in Canada).

ICMP
Abbreviation for Internet Control Message Protocol. ICMP is a TCP/IP protocol used to send error and control messages.

ICU
Abbreviation for ISA Configuration Utility.

ID
Abbreviation for identification.

IDE
Abbreviation for Integrated Drive Electronics. IDE is a computer system interface, used primarily for hard drives and CDs.

I/O
Abbreviation for input/output. The keyboard is an input device, and a printer is an output device. In general, I/O activity can be differentiated from computational activity. For example, when a program sends a document to the printer, it is engaging in output activity; when the program sorts a list of terms, it is engaging in computational activity.

IHV
Abbreviation for independent hardware vendor. IHVs often develop their own MIBs for components that they manufacture.

interlacing
A technique for increasing video resolution by only updating alternate horizontal lines on the screen. Because interlacing can result in noticeable screen flicker, most users prefer noninterlaced video adapter resolutions.

internal microprocessor cache
An instruction and data cache built in to the microprocessor. The Intel Pentium microprocessor includes a 16-KB internal cache, which is set up as an 8-KB read-only instruction cache and an 8-KB read/write data cache.

IP address
Abbreviation for Internet Protocol address. See TCP/IP.

IPMI
Abbreviation for Intelligent Platform Management Interface, which is an industry standard for management of peripherals used in enterprise computers based on Intel architecture. The key characteristic of IPMI is that inventory, monitoring, logging, and recovery control functions are available independent of the main processors, BIOS, and operating system.

IPX
Abbreviation for internetwork packet exchange.

IRQ
Abbreviation for interrupt request. A signal that data is about to be sent to or received by a peripheral device travels by an IRQ line to the microprocessor. Each peripheral connection must be assigned an IRQ number. For example, the first serial port in your system (COM1) is assigned to IRQ4 by default. Two devices can share the same IRQ assignment, but you cannot operate both devices simultaneously.

ISA
Acronym for Industry-Standard Architecture. A 16-bit expansion bus design. The expansion-card connectors in an ISA system are also compatible with 8-bit ISA expansion cards.

ISV
Abbreviation for independent software vendor.

ITE
Abbreviation for information technology equipment.

Java
A cross-platform programming language developed by Sun Microsystems.

JSSE
Abbreviation for Java Secure Socket Extension.

jumper
Jumpers are small blocks on a circuit board with two or more pins emerging from them. Plastic plugs containing a wire fit down over the pins. The wire connects the pins and creates a circuit. Jumpers provide a simple and reversible method of changing the circuitry in a printed circuit board.

K
Abbreviation for kilo-, indicating 1000.

KB
Abbreviation for kilobyte(s), 1024 bytes.

KB/sec
Abbreviation for kilobyte(s) per second.

Kbit(s)
Abbreviation for kilobit(s), 1024 bits.

Kbit(s)/sec
Abbreviation for kilobit(s) per second.

key combination
A command requiring you to press multiple keys at the same time. For example, you can reboot your system by pressing the <Ctrl><Alt><Del> key combination.

kg
Abbreviation for kilogram(s), 1000 grams.

kHz
Abbreviation for kilohertz, 1000 hertz.

LAN
Acronym for local area network. A LAN system is usually confined to the same building or a few nearby buildings, with all equipment linked by wiring dedicated specifically to the LAN.

lb
Abbreviation for pound(s).

LCC
Abbreviation for leaded or leadless chip carrier.

LIF
Acronym for low insertion force. Some systems use LIF sockets and connectors to allow devices, such as the microprocessor chip, to be installed or removed with minimal stress to the device.

LED
Abbreviation for light-emitting diode. An electronic device that lights up when a current is passed through it.

local bus
On a system with local-bus expansion capability, certain peripheral devices (such as the video adapter circuitry) can be designed to run much faster than they would with a traditional expansion bus. Some local-bus designs allow peripherals to run at the same speed and with the same width data path as the system's microprocessor.

LPT*n*
The device names for the first through third parallel printer ports on your system are LPT1, LPT2, and LPT3.

LRA
Abbreviation for local response agent.

m
Abbreviation for meter(s).

mA
Abbreviation for milliampere(s).

mAh
Abbreviation for milliampere-hour(s).

managed system
A managed system is any system that is monitored and managed using Server Administrator. Systems running Server Administrator can be managed locally or remotely through a supported Web browser. See remote management system.

math coprocessor
See coprocessor.

Mb
Abbreviation for megabit.

MB
Abbreviation for megabyte(s). The term megabyte means 1,048,576 bytes; however, when referring to hard drive storage, the term is often rounded to mean 1,000,000 bytes.

MB/sec
Abbreviation for megabytes per second.

Mbps
Abbreviation for megabits per second.

MBR
Abbreviation for master boot record.

MCA
Abbreviation for Micro Channel Architecture, which is designed for multiprocessing. MCA eliminates potential conflicts that arise when installing new peripheral devices. MCA is not compatible with either EISA or XT bus architecture, so older cards cannot be used with it.

memory
A system can contain several different forms of memory, such as RAM, ROM, and video memory. Frequently, the word memory is used as a synonym for RAM; for example, an unqualified statement such as "a system with 16 MB of memory" refers to a system with 16 MB of RAM.

memory address
A specific location, usually expressed as a hexadecimal number, in the system's RAM.

memory manager
A utility that controls the implementation of memory in addition to conventional memory, such as extended or expanded memory.

memory module
A small circuit board containing DRAM chips that connects to the system board.

MHz
Abbreviation for megahertz.

MIB
Acronym for management information base. The MIB is used to send detailed status/commands from or to an SNMP managed device.

microprocessor
The primary computational chip inside the system that controls the interpretation and execution of arithmetic and logic functions. Software written for one microprocessor must usually be revised to run on another microprocessor. CPU is a synonym for microprocessor.

MIDI
Acronym for musical instrument digital interface.

mm
Abbreviation for millimeter(s).

modem
A device that allows your system to communicate with other systems over telephone lines.

modular system
A system that can include multiple server modules. Each server module functions as an individual system. To function as a system, a server module is inserted into a chassis which includes power supplies, fans, a system management module, and at least one network switch module. The power supplies, fans, system management module, and network switch module are shared resources of the server modules in the chassis. See server module.

MOF
Acronym for managed object format, which is an ASCII file that contains the formal definition of a CIM schema.

mouse
A pointing device that controls the movement of the cursor on a screen. Mouse-aware software allows you to activate commands by clicking a mouse button while pointing at objects displayed on the screen.

MPEG
Acronym for Motion Picture Experts Group. MPEG is a digital video file format.

ms
Abbreviation for millisecond(s).

MS-DOS
Acronym for Microsoft Disk Operating System.

MTBF
Abbreviation for mean time between failures.

multifrequency monitor
A monitor that supports several video standards. A multifrequency monitor can adjust to the frequency range of the signal from a variety of video adapters.

mV
Abbreviation for millivolt(s).

name
The name of an object or variable is the exact string that identifies it in an SNMP Management Information Base (MIB) file or in a CIM Management Object File (MOF).

NDIS
Abbreviation for Network Driver Interface Specification.

NIC
Acronym for network interface controller.

NIF
Acronym for network interface function. This term is equivalent to NIC.

NMI
Abbreviation for nonmaskable interrupt. A device sends an NMI to signal the microprocessor about hardware errors, such as a parity error.

noninterlaced
A technique for decreasing screen flicker by sequentially refreshing each horizontal line on the screen.

ns
Abbreviation for nanosecond(s), one billionth of a second.

NTFS
Abbreviation for the Windows NT File System option in the Windows NT operating system. NTFS is an advanced file system designed for use specifically within the Windows NT operating system. It supports file system recovery, extremely large storage media, and long file names. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes. See also FAT and FAT32.

NTLM
Abbreviation for Windows NT LAN Manager. NTLM is the security protocol for the Windows NT operating system.

NuBus
Proprietary expansion bus used on Apple Macintosh personal computers.

NVRAM
Acronym for nonvolatile random-access memory. Memory that does not lose its contents when you turn off your system. NVRAM is used for maintaining the date, time, and system configuration information.

OID
Abbreviation for object identifier. An implementation-specific integer or pointer that uniquely identifies an object.

online access service
A service that typically provides access to the Internet, e-mail, bulletin boards, chat rooms, and file libraries.

OTP
Abbreviation for one-time programmable.

PAM
Acronym for Pluggable Authentication Modules. PAM allows system administrators to set an authentication policy without having to recompile authentication programs.

parallel port
An I/O port used most often to connect a parallel printer to your system. You can usually identify a parallel port on your system by its 25-hole connector.

parameter
A value or option that you specify to a program. A parameter is sometimes called a switch or an argument.

partition
You can divide a hard drive into multiple physical sections called partitions with the fdisk command. Each partition can contain multiple logical drives. After partitioning the hard drive, you must format each logical drive with the format command.

PC card
A credit-card sized, removable module for portable computers standardized by PCMCIA. PC Cards are also known as "PCMCIA cards." PC Cards are 16-bit devices that are used to attach modems, network adapters, sound cards, radio transceivers, solid state disks and hard disks to a portable computer. The PC Card is a "plug and play" device, which is configured automatically by the Card Services software.

PCI
Abbreviation for Peripheral Component Interconnect. The predominant 32-bit or 64-bit local-bus standard developed by Intel Corporation.

PCMCIA
Personal Computer Memory Card International Association. An international trade association that has developed standards for devices, such as modems and external hard drives, that can be plugged into portable computers.

PERC
Acronym for PowerEdge Expandable RAID controller.

peripheral device
An internal or external device—such as a printer, a disk drive, or a keyboard—connected to a system.

PGA
Abbreviation for pin grid array, a type of microprocessor socket that allows you to remove the microprocessor chip.

physical memory array
The physical memory array is the entire physical memory of a system. Variables for physical memory array include maximum size, total number of memory slots on the motherboard, and total number of slots in use.

physical memory array mapped
The physical memory array mapped refers to the way physical memory is divided.

For example, one mapped area may have 640 KB and the other mapped area may have between 1 MB and 127 MB.

PIC
Acronym for programmable interrupt controller.

PIP
Acronym for peripheral interchange program.

pixel
A single point on a video display. Pixels are arranged in rows and columns to create an image. A video resolution, such as 640 x 480, is expressed as the number of pixels across by the number of pixels up and down.

PKCS #7
Abbreviation for Public Key Cryptography Standard #7. PKCS #7 is an RSA Data Security, Inc., standard for encapsulating signed data such as a certificate chain.

PKIS
Abbreviation for Novell Public Key Infrastructure Services.

PLCC
Abbreviation for plastic leaded chip carrier.

Plug and Play
An industry-standard specification that makes it easier to add hardware devices to personal computers. Plug and Play provides automatic installation and configuration, compatibility with existing hardware, and dynamic support of mobile computing environments.

PME
Abbreviation for Power Management Event. A PME is a pin on a peripheral component interconnect that allows a PCI device to assert a wake event.

POST
Acronym for power-on self-test. Before the operating system loads when you turn on your system, the POST tests various system components such as RAM, the disk drives, and the keyboard.

power supply
An electrical system that converts AC current from the wall outlet into the DC currents required by the system circuitry. The power supply in a personal computer typically generates multiple voltages.

power unit
A set of power supplies in a system chassis.

ppm
Abbreviation for pages per minute.

PPP
Abbreviation for Point-to-Point Protocol.

PQFP
Abbreviation for plastic quad flat pack, a type of microprocessor socket in which the microprocessor chip is permanently mounted.

program diskette set
The set of diskettes from which you can perform a complete installation of an operating system or application program. When you reconfigure a program, you often need its program diskette set.

protected mode
An operating mode supported by 80286 or higher microprocessors, protected mode allows operating systems to implement:

- A memory address space of 16 MB (80286 microprocessor) to 4 GB (Intel386 or higher microprocessor)
- Multitasking
- Virtual memory, a method for increasing addressable memory by using the hard drive

The Windows NT, OS/2®, and UNIX® 32-bit operating systems run in protected mode. MS-DOS cannot run in protected mode; however, some programs that you can start from MS-DOS, such as the Windows operating system, are able to put the system into protected mode.

provider
A provider is an extension of a CIM schema that communicates with managed objects and accesses data and event notifications from a variety of sources. Providers forward this information to the CIM Object Manager for integration and interpretation.

PS
Abbreviation for power supply.

PS/2
Abbreviation for Personal System/2.

PXE
Abbreviation for Pre-boot eXecution Environment.

QFP
Abbreviation for quad flat pack.

RAC
Acronym for remote access controller.

RAID
Acronym for redundant array of independent drives.

RAM
Acronym for random-access memory. A system's primary temporary storage area for program instructions and data. Each location in RAM is identified by a number called a memory address. Any information stored in RAM is lost when you turn off your system.

RAMDAC
Acronym for random-access memory digital-to-analog converter.

RAW
Unprocessed. The term refers to data that is passed along to an I/O device without being interpreted. In contrast, cooked refers to data that is processed before being passed to the I/O device. It often refers to uncompressed text that is not stored in any proprietary format. The term comes from UNIX, which supports cooked and raw modes for data output to a terminal.

RBAC
Abbreviation for role-based access control.

RDRAM
Acronym for Rambus DRAM. A dynamic RAM chip technology from Rambus, Inc. Direct RDRAMs are used in systems. Direct RDRAM chips are housed in RIMM modules, which are similar to DIMMs but have different pin settings. The chips can be built with dual channels, doubling the transfer rate to 3.2 GB/sec.

read-only file
A read-only file is one that you are prohibited from editing or deleting. A file can have read-only status if:

- Its read-only attribute is enabled.
- It resides on a physically write-protected diskette or on a diskette in a write-protected drive.
- It is located on a network in a directory to which the system administrator has assigned read-only rights to you.

readme file
A text file included with a software package or hardware product that contains information supplementing or updating the documentation for the software or hardware. Typically, readme files provide installation information, describe new product enhancements or corrections that have not yet been documented, and list known problems or other things you need to be aware of as you use the software or hardware.

real mode
An operating mode supported by 80286 or higher microprocessors, real mode imitates the architecture of an 8086 microprocessor.

refresh rate
The rate at which the monitor redraws the video image on the monitor screen. More precisely, the refresh rate is the frequency, measured in Hz, at which the screen's horizontal lines are recharged (sometimes also referred to as its vertical frequency). The higher the refresh rate, the less video flicker can be seen by the human eye. The higher refresh rates are also noninterlaced.

remote management system
A remote management system is any system that accesses the Server Administrator home page on a managed system from a remote location using a supported Web browser. See managed system.

RFI
Abbreviation for radio frequency interference.

RGB
Abbreviation for red/green/blue.

RIMM
Acronym for Rambus In-line Memory Module, which is the Rambus equivalent of a DIMM module.

RMI
Acronym for Remote Method Invocation. RMI is a part of the Java programming language library that enables a Java program running on one system to access the objects and methods of another Java program running on a different system.

ROM
Acronym for read-only memory. Your system contains some programs essential to its operation in ROM code. Unlike RAM, a ROM chip retains its contents even after you turn off your system. Examples of code in ROM include the program that initiates your system's boot routine and the POST.

rpm
Abbreviation for revolutions per minute.

RPM
Abbreviation for Red Hat® Package Manager.

RTC
Abbreviation for real-time clock. Battery-powered clock circuitry inside the system that keeps the date and time after you turn off the system.

SAN
Acronym for storage area network.

SAS
Acronym for Secure Authentication Services or Serial-attached SCSI. When referring to security protocols or authentication, SAS is Secure Authentication Services. When referring to computer peripheral devices that employ a serial (one bit at a time) means of digital data transfer over thin cables, SAS is Serial-attached SCSI.

SCA
Abbreviation for single connector attachment.

schema
A collection of class definitions that describes managed objects in a particular environment. A schema is a collection of class definitions used to represent managed objects that are common to every management environment, which is why CIM is called the Common Information Model.

SCSI
Acronym for small computer system interface. An I/O bus interface with faster data transmission rates than standard ports. You can connect up to seven devices (15 for some newer SCSI types) to one SCSI interface.

SEL
Acronym for system event log.

SDMS
Abbreviation for SCSI device management system.

sec
Abbreviation for second(s).

SEC
Abbreviation for single-edge contact.

secure port server
An application that makes Web pages available for viewing by Web browsers using the HTTPS protocol. See Web server.

serial port
An I/O port used most often to connect a modem to your system. You can usually identify a serial port on your system by its 9-pin connector.

settings
Settings are conditions of a manageable object help to determine what happens when a certain value is detected in a component. For example, a user can set the upper critical threshold of a temperature probe to 75 degrees Celsius. If the probe reaches that temperature, the setting results in an alert being sent to the management system so that user intervention can be taken. Some settings, when reached, can trigger a system shutdown or other response that can prevent damage to the system.

server module
A modular system component that functions as an individual system. To function as a system, a server module is inserted into a chassis which includes power supplies, fans, a system management module, and at least one network switch module. The power supplies, fans, system management module, and network switch module are shared resources of the server modules in the chassis. See modular system.

service tag number
A bar code label that identifies each system in the event that you need to call for customer or technical support.

SGRAM
Acronym for synchronous graphics RAM.

shadowing
A computer's system and video BIOS code is usually stored on ROM chips. Shadowing refers to the performance-enhancement technique that copies BIOS code to faster RAM chips in the upper memory area (above 640 KB) during the boot routine.

SIMD
Abbreviation for Single Instruction Multiple Data.

SIMM
Acronym for single in-line memory module. A small circuit board containing DRAM chips that connects to the system board.

SIP
Acronym for single in-line package, which is a type of housing for electronic components in which the connecting pins protrude from one side. A SIP is also called a Single In-line Pin Package (SIPP).

SKU
Acronym for stock keeping unit.

SMART
Acronym for Self-Monitoring Analysis and Reporting Technology. A technology that allows hard drives to report errors and failures to the system BIOS, which then displays an error message on the screen. To take advantage of this technology, you must have a SMART-compliant hard drive and the proper support in the system BIOS.

SMBIOS
Acronym for system management BIOS.

SMD
Abbreviation for surface mount device.

SMTP
Abbreviation for Simple Mail Transfer Protocol.

SNMP
Abbreviation for Simple Network Management Protocol. SNMP, a popular network control and monitoring protocol, is part of the original TCP/IP protocol suite. SNMP provides the format in which vital information about different network devices, such as network servers or routers, can be sent to a management application.

SODIMM
Acronym for small outline-DIMM. A DIMM module with a thinner profile due to the use of TSOP chip packages. SODIMMs are commonly used in portable computers.

SOIC
Abbreviation for Small Outline IC, a small-dimension, plastic, rectangular, surface mount chip package that uses gull-wing pins extending outward.

SOJ
Abbreviation for small outline package J-lead, a small-dimension, plastic, rectangular surface mount chip package with j-shaped pins on its two long sides.

SRAM
Abbreviation for static random-access memory. Because SRAM chips do not require continual refreshing, they are substantially faster than DRAM chips.

SSL
Abbreviation for secure socket layer.

state
Refers to the condition of an object that can have more than one condition. For example, an object may be in the "not ready" state.

status
Refers to the health or functioning of an object. For example, a temperature probe can have the status normal if the probe is measuring acceptable temperatures. When the probe begins reading temperatures that exceed limits set by the user, it reports a critical status.

SVGA
Abbreviation for super video graphics array. VGA and SVGA are video standards for video adapters with greater resolution and color display capabilities than previous standards.

To display a program at a specific resolution, you must install the appropriate video drivers and your monitor must support the resolution. Similarly, the number of colors that a program can display depends on the capabilities of the monitor, the video driver, and the amount of video memory installed in the system.

switch
On a system board, switches control various circuits or functions in your computer system. These switches are known as DIP switches; they are normally packaged in groups of two or more switches in a plastic case. Two common DIP switches are used on system boards: slide switches and rocker switches. The names of the switches are based on how the settings (on and off) of the switches are changed.

syntax
The rules that dictate how you must type a command or instruction so that the system understands it. A variable's syntax indicates its data type.

system board
As the main circuit board, the system board usually contains most of your system's integral components, such as the following:

- Microprocessor
- RAM
- Controllers for standard peripheral devices, such as the keyboard
- Various ROM chips

Frequently used synonyms for system board are motherboard and logic board.

system configuration information
Data stored in memory that tells a system what hardware is installed and how the system should be configured for operation.

system diskette
System diskette is a synonym for bootable diskette.

system memory
System memory is a synonym for RAM.

System Setup program
A BIOS-based program that allows you to configure your system's hardware and customize the system's operation by setting such features as password protection and energy management. Some options in the System Setup program require that you reboot the system (or the system may reboot automatically) in order to make a hardware configuration change. Because the System Setup program is stored in NVRAM, any settings remain in effect until you change them again.

system.ini file
A start-up file for the Windows operating system. When you start Windows, it consults the **system.ini** file to determine a variety of options for the Windows operating environment. Among other things, the **system.ini** file records which video, mouse, and keyboard drivers are installed for Windows.

Running the Control Panel or Windows Setup program may change options in the **system.ini** file. On other occasions, you may need to change or add options to the **system.ini** file manually with a text editor, such as Notepad.

table
In SNMP MIBs, a table is a two dimensional array that describes the variables that make up a managed object.

TCP/IP
Abbreviation for Transmission Control Protocol/Internet Protocol. A system for transferring information over a computer network containing dissimilar systems, such as systems running Windows and UNIX.

termination
Some devices (such as the last device at each end of a SCSI cable) must be terminated to prevent reflections and spurious signals in the cable. When such devices are connected in a series, you may need to enable or disable the termination on these devices by changing jumper or switch settings on the devices or by changing settings in the configuration software for the devices.

text editor
An application program for editing text files consisting exclusively of ASCII characters. Windows Notepad is a text editor, for example. Most word processors use proprietary file formats containing binary characters, although some can read and write text files.

TFTP
Abbreviation for Trivial File Transfer Protocol. TFTP is a version of the TCP/IP FTP protocol that has no directory or password capability.

text mode
A video mode that can be defined as x columns by y rows of characters.

threshold values
Systems are normally equipped with various sensors that monitor temperature, voltage, current, and fan speed. The sensor's threshold values specify the ranges (min and max values) for determining whether the sensor is operating under normal, noncritical, critical or fatal conditions. Server Administrator-supported threshold values are

- UpperThresholdFatal
- UpperThresholdCritical
- UpperThresholdNon-critical
- Normal
- LowerThresholdNon-critical
- LowerThresholdCritical
- LowerThresholdFatal

time-out
A specified period of system inactivity that must occur before an energy conservation feature is activated.

tpi
Abbreviation for tracks per inch.

TQFP
Abbreviation for thin quad flat pack.

TSR
Abbreviation for terminate-and-stay-resident. A TSR program runs "in the background." Most TSR programs implement a predefined key combination (sometimes referred to as a hot key) that allows you to activate the TSR program's interface while running another program. When you finish using the TSR program, you can return to the other application program and leave the TSR program resident in memory for later use. TSR programs can sometimes cause memory conflicts. When troubleshooting, rule out the possibility of such a conflict by rebooting your system without starting any TSR programs.

TSOP
Abbreviation for thin small outline package. A very thin, plastic, rectangular surface mount chip package with gull-wing pins on its two short sides.

UART
Acronym for universal asynchronous receiver transmitter, the electronic circuit that makes up the serial port.

UDP
Abbreviation for user datagram protocol.

UL
Abbreviation for Underwriters Laboratories.

UMB
Abbreviation for upper memory blocks.

unicode
A fixed width, 16-bit world wide character encoding, developed and maintained by the Unicode Consortium.

upper memory area
The 384 KB of RAM located between 640 KB and 1 MB. If the system has an Intel386 or higher microprocessor, a utility called a memory manager can create UMBs in the upper memory area, in which you can load device drivers and memory-resident programs.

UPS
Abbreviation for uninterruptible power supply. A battery-powered unit that automatically supplies power to your system in the event of an electrical failure.

URL
Abbreviation for Uniform Resource Locator (formerly Universal Resource Locator).

USB
Abbreviation for Universal Serial Bus. A USB connector provides a single connection point for multiple USB-compliant devices, such as mice, keyboards, printers, and computer speakers. USB devices can also be connected and disconnected while the system is running.

utility
A program used to manage system resources—memory, disk drives, or printers, for example.

utility partition
A bootable partition on the hard drive that provides utilities and diagnostics for your hardware and software. When activated, the partition boots and provides an executable environment for the partition's utilities.

UTP
Abbreviation for unshielded twisted pair.

UUID
Abbreviation for Universal Unique Identification.

V
Abbreviation for volt(s).

VAC
Abbreviation for volt(s) alternating current.

varbind
An algorithm used to assign an object identifier (OID). The varbind gives rules for arriving at the decimal prefix that uniquely identifies an enterprise, as well as the formula for specifying a unique identifier for the objects defined in that enterprise's MIB.

variable
A component of a managed object. A temperature probe, for example, has a variable to describe its capabilities, its health or status, and certain indexes that you can use to help you in locating the right temperature probe.

VCCI
Abbreviation for Voluntary Control Council for Interference.

VDC
Abbreviation for volt(s) direct current.

VESA
Acronym for Video Electronics Standards Association.

VGA
Abbreviation for video graphics array. VGA and SVGA are video standards for video adapters with greater resolution and color display capabilities than previous standards. To display a program at a specific resolution, you must install the appropriate video drivers and your monitor must support the resolution. Similarly, the number of colors that a program can display depends on the capabilities of the monitor, the video driver, and the amount of video memory installed for the video adapter.

VGA feature connector
On some systems with a built-in VGA video adapter, a VGA feature connector allows you to add an enhancement adapter, such as a video accelerator, to your system. A VGA feature connector can also be called a VGA pass-through connector.

video adapter
The logical circuitry that provides—in combination with the monitor—your system's video capabilities. A video adapter may support more or fewer features than a specific monitor offers. Typically, a video adapter comes with video drivers for displaying popular application programs and operating systems in a variety of video modes.

On some systems, a video adapter is integrated into the system board. Also available are many video adapter cards that plug into an expansion-card connector.

Video adapters often include memory separate from RAM on the system board. The amount of video memory, along with the adapter's video drivers, may affect the number of colors that can be simultaneously displayed. Video adapters can also include their own coprocessor for faster graphics rendering.

video driver
A program that allows graphics-mode application programs and operating systems to display at a chosen resolution with the desired number of colors. A software package may include some "generic" video drivers. Any additional video drivers may need to match the video adapter installed in the system.

video memory
Most VGA and SVGA video adapters include memory chips in addition to your system's RAM. The amount of video memory installed primarily influences the number of colors that a program can display (with the appropriate video drivers and monitor capabilities).

video mode
Video adapters normally support multiple text and graphics display modes. Character-based software displays in text modes that can be defined as *x* columns by *y* rows of characters. Graphics-based software displays in graphics modes that can be defined as *x* horizontal by *y* vertical pixels by *z* colors.

video resolution
Video resolution—800 x 600, for example—is expressed as the number of pixels across by the number of pixels up and down. To display a program at a specific graphics resolution, you must install the appropriate video drivers and your monitor must support the resolution.

virtual memory
A method for increasing addressable RAM by using the hard drive. For example, in a system with 16 MB of RAM and 16 MB of virtual memory set up on the hard drive, the operating system would manage the system as though it had 32 MB of physical RAM.

virus
A self-starting program designed to inconvenience you. Virus programs have been known to corrupt the files stored on a hard drive or to replicate themselves until a computer system or network runs out of memory. The most common way that virus programs move from one system to another is via "infected" diskettes, from which they copy themselves to the hard drive. To guard against virus programs, you should do the following:

- Periodically run a virus-checking utility on your system's hard drive
- Always run a virus-checking utility on any diskettes (including commercially sold software) before using them

VLSI
Abbreviation for very-large-scale integration.

VLVESA
Acronym for very low voltage enterprise system architecture.

vpp
Abbreviation for peak-point voltage.

VRAM
Acronym for video random-access memory. Some video adapters use VRAM chips (or a combination of VRAM and DRAM) to improve video performance. VRAM is dual-ported, allowing the video adapter to update the screen and receive new image data at the same time.

VRM
Abbreviation fro voltage regulator module.

W
Abbreviation for watt(s).

Wakeup on LAN
The ability for the power in a client station to be turned on by the network. Remote wake-up enables software upgrading and other management tasks to be performed on users' machines after the work day is over. It also enables remote users to gain access to machines that have been turned off. Intel calls remote wake-up "Wake-on-LAN."

Web server
An application that makes Web pages available for viewing by Web browsers using the HTTP protocol.

WH
Abbreviation for watt-hour(s).

win.ini file
A start-up file for the Windows operating system. When you start Windows, it consults the **win.ini** file to determine a variety of options for the Windows operating environment. Among other things, the **win.ini** file records what printer(s) and fonts are installed for Windows. The **win.ini** file also usually includes sections that contain optional settings for Windows application programs that are installed on the hard drive. Running the Control Panel or Windows Setup program may change options in the **win.ini** file. On other occasions, you may need to change or add options to the **win.ini** file manually with a text editor such as Notepad.

Windows 95
An integrated and complete Microsoft Windows operating system that does not require MS-DOS and that provides advanced operating system performance, improved ease of use, enhanced workgroup functionality, and simplified file management and browsing.

Windows NT
High-performance server and workstation operating system software developed by Microsoft that is intended for technical, engineering, and financial applications.

write-protected
Read-only files are said to be write-protected. You can write-protect a 3.5-inch diskette by sliding its write-protect tab to the open position or by setting the write-protect feature in the System Setup program.

WMI
Acronym for Windows Management Instrumentation. WMI provides CIM Object Manager services.

X.509 Certificate
An X.509 certificate binds a public encryption key to the identity or other attribute of its principal. Principals can be people, application code (such as a signed applet) or any other uniquely identified entity (such as a secure port server or Web server).

Xen
Xen is a virtual machine monitor for x86 systems.

XMM
Abbreviation for extended memory manager, a utility that allows application programs and operating systems to use extended memory in accordance with the XMS.

XMS
Abbreviation for eXtended Memory Specification.

X Window System
The graphical user interface used in the Red Hat Enterprise Linux environment.

ZIF
Acronym for zero insertion force. Some systems use ZIF sockets and connectors to allow devices such as the microprocessor chip to be installed or removed with no stress applied to the device.

ZIP
A 3.5-inch removable disk drive from Iomega. Originally, it provided 100-MB removable cartridges. The drive is bundled with software that can catalog the disks and lock the files for security. A 250-MB version of the Zip drive also reads and writes the 100-MB Zip cartridges.

Index

A

about
  remote access service, 79
  server, 9, 35

AC switch, 64

action window, of home page, 48

administer, Server Administrator, 17

alert, 62, 65-69, 71

alert actions, Red Hat Enterprise Linux, 117

alert messages, BMC, 118

alert properties, RAC, 85

assign, user privileges, 19

authentication
  for Red Hat Enterprise Linux, 19
  for Windows, 18
  RAC, 91
  Server Administrator, 18-19
  single sign-on, 44-45

B

backplane, storage, 74

backup, virtual disk, 105

BIOS, manage, 64

BMC, 69, 93
  about, 93
  alert messages, 118
  configuring users, 94
  filter alerts, 95
  Serial Over LAN (SOL), 97
  serial port connection, 98
  viewing basic details, 94
  virtual LAN connection, 99
  working with, 93

BMC, manage, 69

browser setting, Windows, 45-46

C

certificate, 32

certificate management
  RAC, 89
  uploading certificate, 90
  viewing certificate, 91
  X.509, 53

channel, view details, 74

chassis, 62

chassis, intrusion, 66

command line interface (CLI), 51

components of home page
  action window, 48
  data area, 48-50
  navigation bar, 48
  system tree, 48

configuring serial port, BMC, 98

configuring SNMP Agent, 22
  for Red Hat Enterprise Linux, 26-29
  for Windows, 23-26

configuring, BMC users, 94

configuring, firewalls
  for Red Hat Enterprise Linux, 32

configuring, SNMP Agent, 23-29

connectors, manage, 70

controller, view details, 73

creating users
  Red Hat Enterprise Linux, 21

creating users, Red Hat Enterprise Linux, 21-22

creating users, Windows, 19

CSR, 90

current, manage, 65

D

data area, of home page, 48-50

diagnostics, 62

dial-in users
  DRAC, 86
  DRAC III, 86

dial-out entries, DRAC III, 87

disabling users, for Windows, 22
documentation, related, 12
DRAC
dial-in users, 86
modem settings, 86
DRAC III
adding dial-in users, 86
adding dial-out entries, 87
configuring dial-in users, 86
configuring dial-out entries, 87
modem settings, 87

E

enabling SNMP
by remote hosts, 24
enclosure management module (EMM), 75
enclosure, storage, 74
encryption, 19
Server Administrator, 19
enhanced storage, 102
enhanced storage management
battery tasks, 107
channel tasks, 107
controller tasks, 106
create virtual disk, 104-105
documentation, 109
enclosure tasks, 108
global tasks, 106
temperature tasks, 108
virtual disk, 104
virtual disk tasks, 109

F

failure, virtual disk, 106
fans, manage, 66
firewalls, configuring for Red Hat Enterprise Linux, 32
firmware, manage, 66

G

gauge indicator, home page, 50
generating CSR, 90

H

help, using, 50
home page
components, 48-50
gauge indicator, 50
preferences, 50
server, 10
status indicator, 49
system tree objects, 59
task button, 49
underlined item, 49
home page, managing
configuration options, 77
general settings, 78
Server Administrator, preferences, 78
user preferences, 78
Web server, 78
home page, Server Administrator, 46

I

installing server, requirements, 37
installing, server, 9, 35
about, 35
prerequisites, 37
procedure, 40
requirements, 38-39
silent install, 35
using Server Management CD, 35
with Citrix, 40
instrumentation
server, 10
instrumentation service, 57
intrusion, manage, 66
issues
storage management, 41
issues, storage management, 41

L

logging in, Server Administrator, 43
logging out, Server Administrator, 43
login authentication
RAC, 91
logs, 61
about, 113-114
alert log, 114
command log, 115
features, 113
hardware log, 114
POST log, 115
server, 12

M

manage
current, 65
intrusion, 66
memory devices, 67
ports, 68
power supplies, 68
processors, 68
system, 58
temperatures, 70

management
alert, 62, 65-69, 71
certificate, X.509, 53, 78
security, 17
storage, 11
storage, enhanced, 73
using install CD, 35
X.509 certificate, 32

management information base, 26

memory devices, manage, 67

MIB, 26

modem settings, DRAC, 86-87

N

navigation bar, of home page, 48

network properties, RAC, 84

network, managing, 67

O

online help, using, 50

operating system
basic information, 72
supported, 37

P

physical disks, view details, 75

port, 52

port, managing, 68

power supplies, 68

preferences of home page, 50

preferences, setting up, 52

prerequisites
certificate management, X.509, 32
for Windows, 40
install, 37
remote access service, 80
storage, 41
Storage Management Service, 102

privilege levels, Server Administrator, 18

privileges, types of
for Red Hat Enterprise Linux, 22

procedure
installing server, 40
installing server, with Citrix, 40

processors, manage, 68

protocol, systems management, 39

R

RAC users
adding, 81
configuring, 81
configuring existing user, 82

RAC, alert properties, 85

RAC, certificate management, 89-91

RAC, generating CSR, 90

RAC, login authentication, 91

RAC, network properties, 84

RAC, remote features, 88

RAC, security, 89

RAC, SNMP alert properties, 85

RAC, using, 92

Red Hat Enterprise Linux, 27

Red Hat Enterprise Linux, alert actions, 117

remote access, 10
server, 10

remote access controller, managing, 69

remote access service
about, 79
hardware prerequisites, 80
software prerequisites, 80

remote features, RAC, 88

remote shutdown, 61
remote system
management, 39
requirements
install, 37
operating system, 37
remote system, 39
system, 38-39
Web browsers, 39
Windows, checker, 40
restarting, Server
Administrator, 55

S

secure port, 52
security, 17, 44-45, 52
access control, 17
RAC, 89
Server Administrator, 17
user privileges, 17
security, management, 17
server
about, 35
features, 9
home page, 10
install, 9, 35
instrumentation, 10
logs, 12
Server Administrator, 9
about, 9
adding users, 21
authentication, 18-19
controlling, 54
creating users, Windows, 20
disabling users, Windows, 22
encryption, 19
features, integrated, 35
logs, 113
restarting, 55
security, 17
uses, 9
what's new?, 15
Server Administrator, logging
in, 43
Server Administrator, logging
out, 43
Server Administrator,
logs, 113-115
Server Administrator,
restarting, 55
on Red Hat Enterprise
Linux, 55
on Windows, 55
Server Administrator,
starting, 54
on Red Hat Enterprise
Linux, 54-55
on Windows, 54
Server Administrator,
stopping, 54
on Red Hat Enterprise
Linux, 54
on Windows, 54
Server Administrator,
using, 43
server features, integrated, 9
home page, 10
installation, 9
instrumentation, 10
logs, 12
server port, 52
server preferences, 52
server storage
management, 11
server, installing, 35
about, 35
prerequisites, 37
procedure, 40
requirements, 37
silent install, 35
using Server Management
CD, 35
Windows checker, 40
Windows, checker, 40
with Citrix, 40
service pack, Server
Administrator, 37
service, instrumentation, 57
session, Server
Administrator, 43
setting, BMC filter alerts, 95
setup, Server
Administrator, 17
Sever Administrator, CLI, 51
Sever Administrator, home
page, 46
components, 48-50
preferences, 50
shutdown, 61

single sign-on, 44
Windows, 45
slots, manage, 70
SNMP
agent configuration, 27
SNMP Agent, configuring, 22-29
SNMP alert properties, RAC, 85
SNMP community name, changing, 24
SNMP community name, for Red Hat Enterprise Linux, 27
SNMP set operations, enabling, 25
SNMP set operations, Red Hat Enterprise Linux, 28
SNMP traps, configuring
for Red Hat Enterprise Linux, 29
for Windows, 26
sockets, manage, 70
software, 71
software details, view, 71
SOL, configuring for BMC, 97
spare, virtual disk, 105
status indicator, home page, 49
stopping, Server Administrator, 54
storage, 73
backplane, 74
component severity, 77
enclosure, 74
prerequisites, 41
Storage Management Service
about, 101
enhanced storage, 102
hardware prerequisites, 102
software prerequisites, 102
storage management service
enhanced, 73
migrating basic and enhanced, 110
online help, 110
storage, issues
Linux utilities, 41
management service, 41
PERC console and FAST, 41
storage, manage, 72
switch, 64
system, 60
managing, 59
requirements, 38-39
system chassis, 62
system component, 49
system tree objects, 48, 59
system, managing, 58
systems management, protocols, 39

T

task button, home page, 49
tasks, enhanced storage management, 106-109
temperature, manage, 70
thermal, shutdown, 61
tree objects, home page, 59

U

unattended install, 35
underlined item, home page, 49
uploading certificate, RAC, 90
user preferences, 52
user privileges
assigning, for Windows, 19-20
creating, for Red Hat Enterprise Linux, 22
creating, for Windows, 19-20
security, 17
user privileges, assigning, 19
users
adding, 21
creating, for Red Hat Enterprise Linux, 21-22
creating, for Windows, 19-20
disabling, for Windows, 22
uses of server, 9
using RAC, 92

V

viewing certificate, RAC, 91

viewing, BMC basic details, 94

virtual disk, backup, 105

virtual disk, enhanced storage management, 104-105

virtual disk, failure, 106

virtual disk, spare, 105

virtual LAN, BMC, 99

voltage, manage, 71

W

Web browsers, supported, 39

Web server shutdown, 61

what's new, Server Administrator, 15