

Dell OpenManage
With VMware ESX/ESXi 4
**Systems Management
Guide**



Notes, Cautions, and Warnings



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



CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.



WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

© 2010 Dell Inc. All rights reserved.

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

Trademarks used in this text: Dell™, the DELL logo, PowerEdge™, and OpenManage™ are trademarks of Dell Inc. Microsoft®, Windows®, and Internet Explorer® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® and vSphere™ are registered trademarks or trademarks of VMware, Inc. in the United States or other countries.

Other trademarks and trade names may be used in this publication 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.

September 2010

Rev. A01


Contents

1	Contents	3
2	Overview	7
	Supported Dell OpenManage Components	8
	Server Administrator	9
	Dell Systems Build and Update Utility	9
	DUPs	10
	SUU	10
	ITA	11
	DRAC and iDRAC	11
	IPMI BMC	11
	DMC	12
	Dell Lifecycle Controller	14
	Deployment Toolkit	14
	Important Information	15
	Getting Help	17
	Contacting Dell	17
3	Installing Dell OpenManage Server Administrator	19
	Before You Begin	19
	Security Management	20
	RBAC	20
	User Privileges	20
	ESX 4 Authentication	22


ESXi 4 Authentication	22
Creating Server Administrator Users for ESX/ESXi 4	22
Installing Server Administrator for ESX 4	23
Prerequisites for Installing Managed System Software	23
Installing Managed System Software Using Dell-Provided Media	24
Dependent RPMs for Remote Enablement	29
Uninstalling Managed System Software	29
Installing Server Administrator for ESXi	30
Using the vSphere CLI	31
Using the VMware vSphere Management Assistant	32
Installing the Server Administrator Web Server	33
Troubleshooting the vihostupdate Command	33
Enabling Server Administrator Services on the Managed System	34
Uninstalling Managed System Software	36
Configuring the SNMP Agent	37
Configuring the SNMP Agent on Systems Running ESX 4	37
Configuring the SNMP Agent on Systems Running ESXi 4	43

4	Using Dell OpenManage Server Administrator	45
	Starting Your Server Administrator Session	45
	Central Web Server Login	45
	Login Failure Scenarios.	46
	Unsupported Server Administrator Features With ESXi	48
	Server Administrator Home Page	48
	System Tree.	49
	Action Window	50
	Using the Online Help	52
	Using the Preferences Home Page	53
	Controlling Server Administrator	53
	Starting Server Administrator	54
	Stopping Server Administrator	54
	Restarting Server Administrator	54
	Using the Server Administrator Command Line Interface.	54
	Server Administrator Logs.	55
	Integrated Features	55
	Log Window Task Buttons	55
	Server Administrator Logs.	56
	Hardware Log.	56
	Alert Log	57
	Command Log.	57

Overview

 **NOTE:** Dell OpenManage components and documents may be updated after the release of this document. See support.dell.com/manuals for the latest information on each of the Dell OpenManage components.

This document provides installation steps, usage guidelines, and support information for running the Dell OpenManage systems management software suite on VMware ESX 4 and VMware ESXi 4 software for Dell PowerEdge systems.

 **NOTE:** To download and install ESX 4.x and ESXi 4.x, see the *VMware vSphere 4 on Dell PowerEdge Systems Getting Started Guide* at support.dell.com/manuals.

 **NOTE:** For information on the Dell OpenManage support for ESX/ESXi 3.5.x, see the *Dell OpenManage With VMware ESX/ESXi 3.5 Systems Management Guide* at support.dell.com/manuals.

Dell OpenManage systems management software is a suite of applications for your Dell systems. This software enables you to manage your systems with proactive monitoring, diagnosis, notification, and remote access.

Dell systems management software comprises of the following media:

- *Dell Systems Management Tools and Documentation* media
- *Dell Server Updates* media
- *Dell Management Console* media

Supported Dell OpenManage Components


 **NOTE:** For information on the compatibility between Dell OpenManage components and ESX/ESXi 4, see the *Dell Systems Software Support Matrix* at support.dell.com/manuals.

Table 1-1. Supported Dell OpenManage Components

Dell OpenManage Component	ESX	ESXi
Server Administrator	Yes	Yes
Dell Systems Build and Update Utility	Yes	Yes
Dell Update Packages (DUPs)	Yes	No
Server Update Utility (SUU)	Yes	No
Dell IT Assistant (ITA)	Yes	Yes
Dell Remote Access Controller (DRAC) and integrated DRAC (iDRAC)	DRAC and iDRAC are independent of the operating system and supported in ESX and ESXi.	
Intelligent Platform Management Interface (IPMI) Baseboard Management Controller (BMC)	Yes	ESXi does not support any consoles and IPMI tools cannot be executed from ESXi. However, IPMI commands can be executed remotely using DRAC or iDRAC.
Dell Management Console (DMC)	Yes	Yes
Dell Lifecycle Controller	USC/USC-LCE is independent of the operating system and supported in ESX and ESXi.	
Deployment Toolkit	Yes	Yes

Server Administrator

Server Administrator provides a comprehensive set of integrated management services designed for system administrators to manage systems locally and remotely on a network. Server Administrator is the sole installation on the managed system 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.

The Storage Management Service provides enhanced features for managing a system's locally-attached RAID and non-RAID disk storage.

The Storage Management Service:

- Enables you to view the status of local and remote storage attached to a monitored system.
- Supports SAS, SCSI, SATA, and ATA, but 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 interface or a CLI, without the use of the controller BIOS utilities.
- Protects your data by configuring data redundancy, assigning hot spares, or rebuilding failed drives.

Dell Systems Build and Update Utility

You can use the Dell Systems Build and Update Utility to:

- Update your system firmware and install an operating system.
- Update the firmware and BIOS in a pre-operating system environment on multiple systems.
- Configure your system hardware.
- Customize the Server Update Utility (SUU) and use it to update your system.

DUPs

As the central component of the OpenManage systems management family, DUPs help you to update system software on your PowerEdge systems in a scalable, non-intrusive way. DUPs include:

- Self-extracting files that allow you to update system software including BIOS, firmware, and drivers
- Pre-installation checks for prerequisites, such as system model, operating system version and dependent software, to help you avoid sequencing errors
- Intuitive dialogs to help simplify installation
- Scriptable and silent capabilities that can enable unattended installation

SUU

SUU is a media-based application for identifying and applying updates to a Dell system. You can use SUU to update your Dell system or to view the updates available for any system supported by SUU. SUU compares the versions of components currently installed on your system with update components packaged on the *Dell Server Updates* media. SUU then displays a comparison report of the versions and provides the option of updating the components.



NOTE: SUU is used for system updates and may not work on newly released Dell systems that have not received any system updates.

ITA

ITA provides an integrated view of Dell's comprehensive suite of system monitoring and reporting tools. It includes one-to-many management for Dell systems.

Table 1-2. ITA Support for Virtualization

Virtualization Environment	ITA Features Supported	ITA Features Not Supported
ESX 4	Grouping of host and guests on the Devices tree and display of host-guest association information, power monitoring, alerting, application launch, tasks, software updates (BIOS, firmware, and driver), and inventory.	Performance monitoring
ESXi 4	ESXi 4 traps are displayed. Systems with ESXi 4 are discovered under the Unknown category.	Grouping of host and guests on the Devices tree and display of host-guest association information, performance and power monitoring, application launch, tasks, software updates, and inventory.



NOTE: ITA is a legacy software. It is recommended to use Dell Management Console (DMC).

You can download and install ITA from support.dell.com.

DRAC and iDRAC

DRAC and iDRAC are designed to allow anywhere, anytime Lights Out monitoring, troubleshooting, and system repairs or upgrades independent of the operating system status.

IPMI BMC

IPMI BMC provides a standard interface for monitoring and managing PowerEdge systems. You can use the OpenSource IPMI tool to configure BMC settings in a non-instrumented environment to manage ESX.

DMC

DMC is the next generation one-to-many systems management application that provides similar functionality as ITA and also provides enhanced discovery, inventory, monitoring, and reporting features. It is a web-based GUI, which is installed on a management station in a networked environment. DMC can discover virtualization systems. It also supports hardware inventory and health monitoring for the host systems.

You can install DMC from the *Dell Management Console* media or download and install it from dell.com/openmanage.

Supported features in DMC for ESX and ESXi are:

- Discovery

For ESX: DMC discovers the host device by using the VMware Simple Network Management Protocol (SNMP) agent. The prerequisites to discover the host are:

- Enabling SNMP service on the server
- Enabling SNMP in the connection profile that is used in the **Discovery** task.

For ESXi: DMC discovers the host device by using the Common Information Model (CIM) providers provided by VMware. The prerequisites to discover the host are:

- Enabling WS-Management (WSMAN) service on the server.
- Enabling WSMAN in the connection profile that is used in the **Discovery** task.

- Host-Virtual Machine Association
 - Virtual host server is identified based on the hypervisor operating system running on these host servers.
 - Virtual host servers are shown in **All Devices** tree under Virtual Host node.
 - Virtual machines running on the server are discovered independently over the network.
 - The association between the host and virtual machines running on the host are created post discovery using the MAC address, IP address, and UUID of the virtual machines.
 - Virtual machines associated to a host are shown on the right pane when you click the host server in the left pane.

- Inventory

For ESX: The hardware inventory is shown using the Server Administrator SNMP agent. Prerequisites for inventorying the ESX servers are:

- Server Administrator is installed on the server.
- SNMP service is enabled on the server.
- SNMP is enabled in the connection profile that is used in the inventory task.

For ESXi: The hardware inventory is shown using the CIM providers provided by VMware. The information is gathered using the WSMAN protocol. Prerequisites for inventorying ESXi are:

- WSMAN service is enabled on the server.
- WSMAN is enabled in the connection profile that is used in the inventory task.

Dell Lifecycle Controller

The Unified Server Configurator/ Unified Server Configurator-Lifecycle Controller Enabled (USC/USC-LCE) software is built upon the iDRAC6 Express card and the Unified Extensible Firmware Infrastructure (UEFI) system firmware.

Features of USC/USC-LCE are:

- iDRAC6 works together with the UEFI firmware to access and manage hardware, including component and subsystem management that is beyond the traditional BMC capabilities.
- Remote server management uses the network for programmed web services.
- CLI and GUI are provided by the iDRAC6 card in an environment independent of the operating system and system-power-state.
- The UEFI environment provides the local console interface and the infrastructure for locally and remotely managing system components. The remote services functionality enables consoles, such as DMC and partner consoles, to access LC 1.4 features in a pre-operating system environment.
- USC/USC-LCE provides an embedded solution on the local system to assist with provisioning in a pre-operating system environment.

Deployment Toolkit

Deployment Toolkit provides quick and easy configuration of multiple systems from bare metal to the deployment of the operating system. It also provides a framework for updating the BIOS.

Important Information

- For documentation on ESX/ESXi 4, see support.dell.com/manuals. Navigate to **Software**, select **Virtualization Solutions**, and then select **VMware Software**.
- For documentation on systems management described in this document, see support.dell.com/manuals. Navigate to **Software**, select **Systems Management**, and then select the relevant product for which you seek documentation. The following Dell OpenManage documents are available:
 - *The Dell Unified Server Configurator User's Guide* provides information on using Unified Server Configurator.
 - *The Dell Management Console User's Guide* has information about installing, configuring, and using DMC.
 - *The Dell Systems Build and Update Utility User's Guide* provides information on using the Systems Build and Update Utility.
 - *The Dell Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage components that can be installed on these systems.
 - *The Dell OpenManage Server Administrator User's Guide* describes the installation and use of Server Administrator.
 - *The Dell OpenManage Server Administrator SNMP Reference Guide* documents the 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 CIM provider, which is an extension of the standard management object format (MOF) file. This guide explains the supported classes of management objects.
 - *The Dell OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed in the Server Administrator home page Alert log, or on your operating system's event viewer. This guide explains the text, severity, and cause of each 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 OpenManage IT Assistant User's Guide* has information about installing, configuring, and using ITA. ITA provides a central point of access to monitor and manage systems on a LAN or WAN. By allowing an administrator a comprehensive view across the enterprise, ITA can increase system uptime, automate repetitive tasks, and prevent interruption in critical business operations.
 - 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 *Integrated Dell Remote Access Controller User's Guide* provides complete information about configuring and using iDRAC to remotely manage and monitor your system and its shared resources through a network.
 - The *Dell Update Packages User's Guide* provides information about obtaining and using DUPs as part of your system update strategy.
 - The *Dell OpenManage Server Update Utility User's Guide* provides information on using SUU.
 - The software kit (media) contain readme files for applications found on the media.
- For more information about Dell OpenManage software, see dell.com/openmanage.
 - VMware documents are available at support.vmware.com.
 - Dell Technology Center maintains a wiki, which provides a collaborative environment where customers and Dell engineers share knowledge, experiences, and information about Dell technology in customer environments. To access the wiki, see delltechcenter.com.
 - The Dell Community at en.community.dell.com is an online community for Dell customers for solutions, advice and general information.

Getting Help

Contacting Dell

Dell provides technical assistance for this product. For support in the United States, call 800-WWW-DELL(800-999-3355).



NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability of the services varies by country and product. Certain services may not be available in your area. If you are located outside the United States:

- 1 Go to support.dell.com.
- 2 Choose your country or region from the top of the page, and then select the type of support you require.

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

Installing Dell OpenManage Server Administrator

Before You Begin

- Read the applicable Dell OpenManage readme files and the *Dell Systems Software Support Matrix* at support.dell.com/manuals. These files contain the latest information about software, firmware, and driver versions, in addition to information about known issues.
- Server Administrator must be installed on each system to be managed.
- The managed system requirements are:
 - A minimum of 2 GB RAM.
 - A minimum of 512 MB of free space for installation.
 - Administrator rights.
 - A TCP/IP connection on the managed system and the remote system to facilitate remote system management.
 - 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 pixels. The recommended screen resolution is 1024 x 768 pixels.
 - The Server Administrator Remote Access Controller service requires that a remote access controller (RAC) be installed on the system to be managed. See the relevant Dell Remote Access Controller User's Guide for complete software and hardware requirements.



NOTE: The RAC software is installed as part of the **Typical Setup** installation option, when installing managed system software, provided that the managed system meets all of the RAC installation prerequisites. See the relevant Dell Remote Access Controller User's Guide for complete software and hardware requirements.

- The Server Administrator Storage Management Service requires that Server Administrator be installed on the system in order to be properly managed. See the *Dell OpenManage Server Administrator Storage Management User's Guide* for software and hardware requirements.

Security Management

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

RBAC

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



NOTE: ESXi does not support setting up user privileges in the **omarolemap** file.

Server Administrator grants different access rights based on the user's assigned group privileges. The four user levels are: User, Power User, Administrator, and Elevated 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.
- *Elevated Administrators* can view and manage information.

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 administrator access to users logged in with *Administrator* and *Elevated Administrator* privileges. See Table 2-1.

Table 2-1. User Privileges

User Privileges	Access Type	
	View	Manage
User	Yes	No
Power User	Yes	Yes
Administrator	Yes	Yes
Elevated Administrator (Linux only)	Yes	Yes

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

Table 2-2. Server Administrator User Privilege Levels

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

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

Table 2-3. Legend for Server Administrator User Privilege Levels

U	User
A	Administrator
EA	Elevated Administrator

ESX 4 Authentication

ESX uses the Pluggable Authentication Modules (PAM) structure for authentication when users access the ESX Server host. The PAM configuration for VMware services is located in `/etc/pam.d/vmware-authd`, which stores paths to authentication modules.

The default installation of ESX uses `/etc/passwd` authentication, just as Linux does, but you can configure ESX to use another distributed authentication mechanism.

ESXi 4 Authentication

ESXi authenticates users accessing ESXi hosts using the vSphere/VI Client or SDK. The default installation of ESXi uses a local password database for authentication. ESXi authentication transactions with Server Administrator are also direct interactions with the `vmware-hostd` process. To make sure that authentication works efficiently for your website, perform basic tasks such as setting up users, groups, permissions, and roles, configuring user attributes, adding your own certificates, and determining whether you want to use SSL.

Creating Server Administrator Users for ESX/ESXi 4

- 1 Log on to the host using the vSphere Client.
- 2 Click the **Users & Groups** tab and click **Users**.
- 3 Right-click anywhere in the Users table and click **Add** to open the Add New User dialog box.
- 4 Enter a login, a user name, a numeric user ID (UID), and a password; specifying the user name and UID are optional. If you do not specify the UID, the vSphere Client assigns the next available UID.
- 5 To allow a user to access the host through a command shell, select **Grant shell access to this user**. Users that access the host only through the vSphere Client do not need shell access.
- 6 To add the user to a group, select the group name from the **Group** drop-down menu and click **Add**.
- 7 Click **OK**.

Installing Server Administrator for ESX 4

This section explains how to install managed system software using the following installation options:

- Using the `srvadmin-install.sh` shell script for express installs or custom installs, in interactive mode



NOTE: If you have downloaded the managed system software installer (available as `a.tar.gz` file) from support.dell.com, the `srvadmin-install.sh` shell script is present as `setup.sh` in the root directory.

- Using RPM commands for custom installs in interactive mode

Prerequisites for Installing Managed System Software

- You must be logged in as `root`.
- The `/opt` directory must have at least 250 MB of free space, and the `/tmp`, `/etc`, and `/var` directories must each have at least 20 MB of free space.
- If you use SNMP to manage your server, install the `net-snmp` package provided with the operating system. To use supporting agents for the `net-snmp` agent, install the operating system support for the SNMP standard before installing Server Administrator. For more information about installing SNMP, see the installation instructions for the operating system you are running on your system.

To avoid warnings related to the RPM-GPG key, import the key with a command similar to the following when installing an RPM package in VMware ESX:

```
rpm --import  
/mnt/dvdrom/SYSMGMT/srvadmin/linux/RPM-GPG-KEY
```

Installing Managed System Software Using Dell-Provided Media

The Dell OpenManage installer uses RPMs to install each component. The media is divided into subdirectories to enable easy custom installation.

If you would like to review the software before you install it, perform the following procedure:

- 1 Load the *Dell Systems Management Tools and Documentation* media into your system's optical drive.
- 2 If necessary, use the command line to mount the media using a command such as:

```
mount /dev/dvdrom /mnt/dvdrom
```

- 3 When you have mounted the media, navigate to:
`cd /mnt/dvdrom/SYSMGMT/srvadmin/linux/`
- 4 Get a listing of the directories using the `ls` command.

The directories on the media that pertain to ESX are the following:

- SYSMGMT/srvadmin/linux/custom
- SYSMGMT/srvadmin/linux/RPMS
- SYSMGMT/srvadmin/linux/supportscripts

Express Install

Use the provided shell script to perform the express installation.

- 1 Log on as `root` to the service console of the system running ESX where you want to install the managed system components.
- 2 Insert the *Dell Systems Management Tools and Documentation* media into the optical drive.
- 3 If necessary, use the command line to mount the media using a command such as:
`mount /dev/dvdrom /mnt/dvdrom`
- 4 Navigate to the `SYSMGMT/srvadmin/linux/supportscripts` directory.

5 Run the `srvadmin-install.sh` shell script as shown below, which performs an express installation. The setup program installs the following managed system software features:

- Server Administrator Web Server
- Server Instrumentation
- Storage Management
- Remote Access Controller

```
sh srvadmin-install.sh --express
```

or

```
sh srvadmin-install.sh -x
```



NOTE: The Server Administrator services do not start automatically.

6 Start the Server Administrator services after the installation by using the command: `sh srvadmin-services.sh start`

Custom Install

Managed system software provides two custom installation paths. One is RPM-based, with pre-configured custom directories, and the other is shell script-based.

Performing the Custom Installation Using Pre-Configured Custom Directories

All RPMs specific to a particular operating system are grouped together as listed in Table 2-4. You can use these RPMs to perform a custom installation using pre-configured custom directories.

Table 2-4. Custom Installation Using Pre-Configured Directories

Directory	Details
To facilitate an RPM-based custom installation, add the RPMs from the following directories:	
<code>SYSMGMT/srvadmin/linux/custom/ESX40</code>	Contains Server Administrator with command line interface for ESX (version 4)

The following is an example of custom RPMs-based installation of Server Administrator, including the installation of the Remote Enablement feature and the Storage Management Service components.

- 1 Log on as `root` to the system running ESX where you want to install the managed system components.
- 2 Insert the *Dell Systems Management Tools and Documentation* media into the optical drive.
- 3 If necessary, mount the media using a command such as:
`mount /dev/dvdrom /mnt/dvdrom.`
- 4 Navigate to the `SYSMGMT/srvadmin/linux/custom/<os>`, where `<os>` is `ESX40`. Enter the operating system specific directory corresponding to your system.
- 5 Type the following command:

```
rpm -ihv Server-Instrumentation/i386/*.rpm
add-StorageManagement/i386/*.rpm
RemoteEnablement/i386/*.rpm
```



NOTE: Ensure that you install Server Administrator web server or Remote Enablement, or Server Instrumentation before installing Remote Access Controller or Storage Management.



NOTE: If you choose to install the Remote Enablement feature, ensure that you install the dependent RPMs before installing this feature. See "Dependent RPMs for Remote Enablement" on page 29.

- 6 Start the Server Administrator services after the installation by using the command:

```
sh srvadmin-services.sh start
```



NOTE: You can install Server Administrator on any system that meets operating system dependencies. However, after installation, certain Server Administrator services may not be started on unsupported systems.

Performing the Custom Installation Using the Shell Script

You can run the Server Administrator Custom Install script in an interactive mode.

The basic usage of the script is:


```
srvadmin-install.sh [OPTION]...
```

The Server Administrator Custom Installation Utility runs in interactive mode if you do not specify any options, and it runs silently if you provide one or more options.

The options are:

- [-x|--express] installs all components (including **RAC**, if available). Any other options passed are ignored.
- [-d|--dellagent] installs **Server Instrumentation** components.
- [-c|--cimagent] installs **Remote Enablement** components.
- [-s|--storage] installs **Storage Management**, including **Server Instrumentation**.
- [-r|--rac] installs applicable **RAC** components, including **Server Instrumentation**.
- [-w|--web] installs **Server Administrator Web Server**.
- [-u|--update] updates applicable Server Administrator components.
- [-h|--help] displays this help text.

Options that can be used along with the options above:

- [-p|--preserve] preserves the screen without clearing off.
 **NOTE:** If you do not use the [-p | --preserve] option during the custom installation, the history information on the screen gets cleared off.
- [-a|--autostart] starts the installed services after components have been installed.

Performing the Custom Installation in Interactive Mode Using the Shell Script

This procedure uses the installation shell script to prompt you for the installation of specific components through the installation.

- 1 Log in as `root` to the system running ESX where you want to install the managed system components.
- 2 Insert the *Dell Systems Management Tools and Documentation* media into the optical drive.
- 3 If necessary, mount the media using the command:
`mount /dev/dvdrom /mnt/dvdrom`
- 4 Navigate to `SYSMGMT/srvadmin/linux/supportscripts` if you are using the media.
- 5 Run the script with the `sh srvadmin-install.sh` command and accept the terms of the end-user license agreement.

Executing the command displays a list of component options. If any of the components are already installed, then those components are listed separately with a check mark next to them. The Server Administrator custom installation options are displayed.

- 6 Press `<I>` to install.
Press `<C>` to copy, `<R>` to reset and start over, or `<Q>` to quit.
When the installation is complete, the script displays an option for starting the services.
- 7 Press `<N>` to exit. You can start the services manually later.

Using the Custom Install Script To Run in the Silent Mode

The following is an example of a silent custom installation using the `srvadmin-install.sh` shell script:


- 1 Log on as `root` to the system where you want to install the managed system components.
- 2 Insert the *Dell Systems Management Tools and Documentation* media into the optical drive.
- 3 If necessary, mount the media using a command:
`mount /dev/dvdrom /mnt/dvdrom.`
- 4 Navigate to `SYSMGMT/srvadmin/linux/supportscripts`.

- 5 To install the Storage Management Service components, type the following command.

```
sh srvadmin-install.sh --storage (these are long options)
```


or


```
sh srvadmin-install.sh -s (these are short options)
```

 **NOTE:** Long options can be combined with short options, and vice-versa. Server Administrator services do not start automatically.

- 6 Start Server Administrator services after the installation by using the command:

```
sh srvadmin-services.sh start
```

 **NOTE:** After installing Server Administrator, log out and then log in again to access the Server Administrator Command Line Interface (CLI).

 **NOTE:** The Server Administrator remains a 32-bit application when installed on a system running a 64-bit version of ESX operating system.


Dependent RPMs for Remote Enablement

If you choose to install the Remote Enablement feature, you have to install certain dependent RPMs and configure these RPMs before installing the feature.

Install the following dependent RPMs that are available in the *Dell Systems Management Tools and Documentation* media at `srvadmin/linux/RPMS/supportRPMS/opensourcecomponents/<OS>/<arch>`:

- `libwsman1`
- `openwsman-client`

Uninstalling Managed System Software

 **NOTE:** This information is applicable only to the Server Administrator installed on ESX.

You can uninstall managed system software from the ESX command line. An uninstallation script is installed when you install Server Administrator on ESX. To execute the script, type the following command:

`srvadmin-uninstall.sh`, and then press `<Enter>`.

Prerequisites for Uninstalling Managed System Software

You must be logged in as `root`.

Custom Uninstallation of Specific Components

Some individual components of Dell OpenManage can be uninstalled without uninstalling all of Dell OpenManage. Following are examples:

To uninstall only the Server Administrator Web Server, use this command:

```
rpm -e `rpm -qa | grep srvadmin-iws`
```

To uninstall the storage component, use this command:

```
rpm -e `rpm -qa | grep srvadmin-storage`
```

During an uninstallation, files in which user settings are made are preserved with the `.rpmsave` file extension. Log files are also preserved after the uninstallation.

Installing Server Administrator for ESXi

To install Server Administrator on systems running VMware ESXi 4.0 Update 1 or ESXi 4.1, download the `oem-dell-openmanage-esxi_6.3.0-A00.zip` file by performing the following steps:

- 1 Go to support.dell.com and click **Drivers and Downloads**.
- 2 Enter your Service Tag or product model.
- 3 Select **ESXi 4.0** or **ESXi 4.1** as the operating system, and then click **Systems Management**.
- 4 Click **OpenManage Offline Bundle and VIB for ESXi** to download and install the OpenManage Server Administrator.

Download vSphere Command Line Interface (vSphere CLI) from vmware.com and install it on your Microsoft Windows or Linux system. Alternately, you can import VMware vSphere Management Assistant (vMA) into your ESXi 4.0 Update 1 and ESXi 4.1 host.


Using the vSphere CLI

- 1 Copy the `oem-dell-openmanage-esxi_6.3.0-A00.zip` file to a directory on your system where the vSphere CLI is installed.
- 2 Shut down all guest operating systems on the ESXi host and run the ESXi host in maintenance mode.
- 3 If you are using Windows, navigate to the directory in which you have installed the vSphere CLI utilities to run the command mentioned in step 4.

If you are using vSphere CLI on Linux, you can run the command in step 4 from any directory.

- 4 Run the following command:

```
vihostupdate.pl --server <IP address of ESXi host>  
-i -b <path to Dell OpenManage file>
```

 **NOTE:** The `.pl` extension is not required if you are using vSphere CLI on Linux.

- 5 Enter the root user name and password of the ESXi host when prompted. The command output displays a successful update. If a failed update is displayed, see "Troubleshooting the `vihostupdate` Command" on page 33.
- 6 Restart the ESXi host system.

When you run the `vihostupdate` command, the following components are installed on your system:

- Server Administrator Instrumentation Service
- Remote Enablement
- Server Administrator Storage Management
- Remote Access Controller

After installing Server Administrator, enable Server Administrator Services. See "Enabling Server Administrator Services on the Managed System" on page 34.

Using the VMware vSphere Management Assistant

The vSphere Management Assistant (vMA) allows administrators and developers to run scripts and agents to manage ESX/ESXi systems. For more information on vMA, see vmware.com/support/developer/vima.

- 1 Log on to the vMA as an administrator and enter the password when prompted.
- 2 Copy the `oem-dell-openmanage-esxi_6.3.0-A00.zip` file to a directory on the vMA.
- 3 Shut down all guest operating systems on the ESXi host and run the ESXi host in maintenance mode.
- 4 In the vMA, run the following command:

```
vihostupdate --server <IP address of ESXi Host> -i  
-b <path to Dell OpenManage file>
```
- 5 Enter the root user name and password of the ESXi host when prompted. The command output displays a successful update. If a failed update is displayed, see "Troubleshooting the vihostupdate Command" on page 33.
- 6 Restart the ESXi host system.

When you run the `vihostupdate` command, the following components are installed on your system:

- Server Administrator Instrumentation Service
- Remote Enablement
- Server Administrator Storage Management
- Remote Access Controller

After installing Server Administrator, enable Server Administrator Services. See "Enabling Server Administrator Services on the Managed System" on page 34.

Installing the Server Administrator Web Server

You must install the Server Administrator Web Server separately on a management station.



NOTE: Ensure that you install only Server Administrator Web Server version 6.1 and later. Server Administrator Web Server version 6.0.3 is not supported for managing ESXi 4.0 and later.

Troubleshooting the vihostupdate Command

When attempting to use the `vihostupdate` command, the following errors may be displayed:

- `unpacking c:\oem-dell-openmanage-esxi_6.3.0-A00.zip`
`metadata.zip.sig does not exist`
`signature mismatch : metadata.zip`
`Unable to unpack update package.`

This error is displayed if you are using an older version of the Remote CLI. To resolve this issue, download and install the vSphere version of the CLI.

- `Unable to create, write or read a file as expected.I/O Error (28) on file : [Errno 28] No space left on device.`
To resolve this issue, see kb.vmware.com/kb/1012640.
- `This operation is NOT supported on 4.1.0 platform`
This error is displayed if you are using an older version of the vSphere CLI. To resolve this issue, download and install the latest vSphere CLI version.

Enabling Server Administrator Services on the Managed System

The Server Administrator Web Server communicates with the ESXi system through the Server Administrator Common Interface Model (CIM) provider. The Server Administrator CIM provider is an OEM provider on the ESXi system. CIM OEM providers are disabled by default on ESXi. Enable the CIM OEM providers on the ESXi 4.0 Update 1/ESXi 4.1 system before accessing it using Server Administrator Web Server. CIM OEM providers can be enabled using any one of the following three methods in the next sections.

Enabling CIM OEM Providers Using vSphere Client

To enable CIM OEM providers using VMware vSphere Client, you need to have the vSphere Client tool installed. You can download and install the tool from https://<IP_address_of_ESXi_host> where *<ip_address>* is the IP address of the VMware ESXi system.

To enable CIM OEM providers on the ESXi system using vSphere Client:

- 1 Log on to the ESXi host system using vSphere Client.
- 2 Click the **Configuration** tab.
- 3 Under the **Software** section on the left side, click **Advanced Settings**.
- 4 In the **Advanced Settings** dialog box, click **UserVars** on the left pane.
- 5 Change the value of the **CIMOEMProvidersEnabled** or **CIMoemProviderEnabled** field to **1**.
- 6 Click **OK**.
- 7 For the changes to take effect without restarting the system, use the **Restart Management Agents** option in the Direct Console User Interface (DCUI) on the local console of the ESXi system.

If the changes are not effective and if you cannot connect to the VMware ESXi host using Server Administrator, restart the VMware ESXi host system.

Enabling CIM OEM Providers Using vSphere CLI

- 1 If you are using vSphere CLI on Windows, navigate to the directory in which you have installed the vSphere CLI utilities.

If you are using vSphere CLI on Linux, you can run the command in step 2 from any directory.


- 2 Run the following command:

For ESXi 4.0 Update 1,

```
vicfg-advcfg.pl --server <ip_address of ESXi host>  
--username <user_name> --password <password> --set  
1 UserVars.CIMOEMProvidersEnabled
```

For ESXi 4.1,

```
vicfg-advcfg.pl --server <ip_address of ESXi host>  
--username <user_name> --password <password> --set  
1 UserVars.CIMoemProviderEnabled
```

 **NOTE:** The .pl extension is not required if you are using vSphere CLI on Linux.

- 3 For the changes to take effect without restarting the system, use the **Restart Management Agents** option in the Direct Console User Interface (DCUI) on the local console of the VMware ESXi system.

If the changes are not effective and if you cannot connect to the VMware ESXi host using Server Administrator, restart the VMware ESXi host system.

Enabling CIM OEM Providers Using vMA

- 1 Log on to the vMA as an administrator and enter the password when prompted.
- 2 Execute the following command:

For ESXi 4.0 Update 1,

```
vicfg-advcfg --server <ip_address of ESXi host> --  
username <user_name> --password <password> --set 1  
UserVars.CIMOEMProvidersEnabled
```

For ESXi 4.1,

```
vicfg-advcfg --server <ip_address of ESXi host> --  
username <user_name> --password <password> --set 1  
UserVars.CIMoemProviderEnabled
```

- 3 For the changes to take effect without restarting the system, use the **Restart Management Agents** option in the Direct Console User Interface (DCUI) on the local console of the VMware ESXi system.

If the changes are not effective and if you cannot connect to the VMware ESXi host using Server Administrator, restart the VMware ESXi host system.

Uninstalling Managed System Software



NOTE: This information is applicable only to the Server Administrator installed on ESX.

An uninstallation script is installed when you install Server Administrator on ESX. To execute the script, type the following command:

`srvadmin-uninstall.sh`, and then press <Enter>.

Configuring the SNMP Agent

Server Administrator supports SNMP—a systems management standard—on all supported operating systems. 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: The default SNMP agent configuration usually includes a SNMP community name such as **public**. For security reasons, change the SNMP community names from their default values. For information about changing SNMP community names, see the appropriate section below.



NOTE: SNMP Set operations are disabled by default in Server Administrator version 5.2 or later. Server Administrator provides support to enable or disable SNMP Set operations in Server Administrator. You can use the **Server Administrator SNMP Configuration** page under **Preferences** or the Server Administrator CLI to enable or disable SNMP Set operations in Server Administrator. For more information about the Server Administrator CLI, see the *Dell OpenManage Server Administrator Command Line Interface User's Guide*.



NOTE: For ITA to retrieve management information from a system running Server Administrator, the community name used by ITA must match a community name on the system running Server Administrator. For ITA to modify information or perform actions on a system running Server Administrator, the community name used by ITA must match a community name that allows Set operations on the system running Server Administrator. For ITA 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 ITA.

Configuring the SNMP Agent on Systems Running ESX 4

Server Administrator uses the SNMP services provided by the 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 ITA, 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 OID 1.3.6.1.4.1.674. Management applications must have access to this branch of the MIB tree to manage systems running Server Administrator.

For ESX 4 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.

Server Administrator SNMP Agent Install Actions

If the 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 encounters this line, it modifies the line as follows:

```
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. To configure the object identifier with the SNMP agent during the installation, Server Administrator adds the following line to the SNMP agent configuration file, `/etc/snmp/snmpd.conf`:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

For more information on configuration, see the *Dell OpenManage Server Administrator Installation Guide* at dell.com/manuals.

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 the command:

```
service snmpd restart
```

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the ESX 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 the command:

```
service snmpd restart
```

Configuring ESX 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 the command:

```
service snmpd restart
```

Configuring the SNMP Agent on Systems Running ESX 4 to VMware MIBs


ESX4 can be managed through a single default port 161 using the SNMP protocol. To do this, configure `snmpd` to use the default port 161 and configure `vmwarehostd` to use a different (unused) port, for example, 167. Any SNMP request on the VMware MIB branch is rerouted to the `vmware-hostd` using the proxy feature of the `snmpd` daemon.

The VMware SNMP configuration file can be modified manually on ESX or by running VMware vSphere CLI command `vicfg-snmp` from a remote system. The RCLI tools can be downloaded from vmware.com.

Below are the required steps for the configuration.

- 1 Edit the VMware SNMP configuration file (`/etc/vmware/snmp.xml`) either manually or run the following `vicfg-snmp` commands to modify the SNMP configuration settings. This includes the SNMP listening port, community string, and the trap target `ipaddress/port` and trap community name and then enable the VMware SNMP service.

- a `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> -c <community name> -p X -t <DMC_IP_Address>@162/<community name>`

 **NOTE:** The `.pl` extension is not required if you are using vSphere CLI on Linux.

Where `X` represents an unused port. To find an unused port, see the `/etc/services` file for the port assignment for defined system services.

Also, to ensure that the port selected is not currently being used by any application/service, run the following command on ESX:

```
- netstat -a command
```



NOTE: Multiple IP addresses can be entered using a comma-separated list.

- b** To enable VMware SNMP service, run the following command:

```
vicfg-snmp.pl --server <ESX_IP_addr> --username  
root --password <password>  
  
-E
```
- c** To view the configuration settings, run the following command:

```
vicfg-snmp.pl --server <ESX_IP_addr> --username  
root --password <password>  
  
-s
```

After modification, the configuration file looks like:

```
<?xml version="1.0">  
<config>  
<snmpSettings>  
<enable>true</enable>  
<communities>public</communities>  
<targets>143.166.152.248@162/public</targets>  
<port>167</port>  
</snmpSettings>  
</config>
```

- 2** Stop the SNMP service if it is already running on your system by entering the following command:

```
service snmpd stop
```

- 3 Add the following line at the end of the `/etc/snmp/snmpd.conf`:

```
proxy -v 1 -c public udp:127.0.0.1:X
.1.3.6.1.4.1.6876
```

Where X represents the unused port specified above, while configuring SNMP.

- 4 Configure the trap destination using the following command: `trapsink <Destination_IP_Address> <community_name>`


The trapsink specification is required to send traps defined in the proprietary MIBs.

- 5 Restart mgmt-vmware service with the following command:

```
service mgmt-vmware restart
```

- 6 Restart the snmpd service with the following command:

```
service snmpd start
```

 **NOTE:** If the Server Administrator is installed and the services are already started, they should be restarted as they depend on the snmpd service.

- 7 Run the following command so that the snmpd daemon starts on every reboot:

```
chkconfig snmpd on
```


Enabling Firewall for SNMP

Run the following command to ensure that the SNMP ports are open before sending traps to the management station:

```
esxcfg-firewall -e snmpd
```

Configuring the SNMP Agent on Systems Running ESXi 4

Server Administrator supports SNMP traps on ESXi 4. Server Administrator does not support SNMP Get and Set operations because ESXi 4 does not provide the required SNMP support. The vSphere CLI is used to configure a system running ESXi 4 to send SNMP traps to a management station.

 **NOTE:** For more information about using the vSphere CLI, see the VMware support site at vmware.com/support.

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 ESXi system running Server Administrator to send traps to a management station, perform the following steps:


- 1 Run the following command:

```
vicfg-snmp.pl --server <server> --username  
<username> --password <password> -c <community> -t  
<hostname>/<community>
```

where <server> is the hostname or IP address of the ESXi system, <username> is a user on the ESXi system, <password> is the password of the ESXi user, <community> is the SNMP community name and <hostname> is the hostname or IP address of the management station.

- 2 Enable SNMP using the following command: `vicfg-snmp.pl --server <server> --username <username> --password <password> -E`
- 3 View the SNMP configuration using the following command:
`vicfg-snmp.pl --server <server> --username <username> --password <password> -s`
- 4 Test the SNMP configuration using the following command:
`vicfg-snmp.pl --server <server> --username <username> --password <password> -T`

 **NOTE:** The extension .pl is not required on Linux.

 **NOTE:** If you do not specify a user name and password, you are prompted.

The SNMP trap configuration takes effect immediately without restarting any services.

Using Dell OpenManage Server Administrator

Starting Your Server Administrator Session

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



NOTE: You must have preassigned user rights to log in to Server Administrator.

Central Web Server Login

The central web server login is available only when you install the Server Administrator web server component. You can use the central web server login to access ESX and ESXi systems with remote enablement. Use this login to manage the OpenManage Server Administrator central web server.

- 1 Click on the **Dell OpenManage Server Administrator** icon on your desktop. The remote login page is displayed.
- 2 Click on the **Manage Web Server Link**, located at the top right corner of the screen.

- 3 Enter the **User Name**, **Password** and **Domain name** (if you are accessing Server Administrator from a defined domain).
- 4 Click **OK**.

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.



NOTE: When you launch Server Administrator using Internet Explorer version 7.0, an intermediate warning page may appear displaying the problem with security certificate. To ensure system security, it is 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). To avoid encountering such warning messages about the certificate, the certificate used must be from a trusted CA.

Using the Ignore Certificate Option

The login screen has an **Ignore certificate** check box.



CAUTION: Use the **Ignore certificate** option with discretion. It is highly recommended that you use it only in trusted Intranet environments.

To ensure system security, it is recommended that you import a root certificate or certificate chain from a CA. See the VMware documentation for details.



NOTE: If the CA authority on the managed system is valid and if the Server Administrator web server still reports an untrusted certificate error, you can still make the managed system's CA as trusted by using the **certutil.exe** file. See your operating system documentation for details on accessing this **.exe** file. On supported Windows operating systems, you can also use the certificates snap in option to import certificates.

Login Failure Scenarios

You may not be able to login to the managed system if:

- You enter an invalid/incorrect IP address.
- You enter incorrect credentials (user name and password).
- The managed system is not powered on.
- The managed system is not reachable due to an invalid IP address or a DNS error.

- The managed system has an untrusted certificate and you do not select the **Ignore Certificate Warning** in the login page.
- Server Administrator services are not enabled on the ESX/ESXi system. For information on how to enable Server Administrator Services on the ESX/ESXi system, see the *Dell OpenManage Server Administrator Installation Guide* at support.dell.com/manuals.
- The small footprint CIM broker daemon (SFCBD) service on the ESX/ESXi system is not running.
- The web server management service on the managed system is not running.
- You enter the IP address of the managed system and not the hostname, when you do not check the **Ignore Certificate Warning** check box.
- The WinRM Authorization feature (Remote Enablement) is not configured in the managed system. For information on this feature, see the *Dell OpenManage Server Administrator Installation Guide* at support.dell.com/manuals.
- The authentication may fail while connecting to the VMware ESXi 4.0 Update 1/ ESX 4.1 operating system, due to any one of the following reasons:
 - The lockdown mode is enabled either while you are logging to the server or while you are logged into Server Administrator. For more information on lockdown mode, see the *Managing VMware ESXi* document at vmware.com.
 - The password is changed while you are logged into Server Administrator.
 - You log in to Server Administrator as a normal user without administrator privileges. For more information on roles, see the VMware documentation at vmware.com/support/pubs.

Unsupported Server Administrator Features With ESXi

The following features of Server Administrator are not supported in ESXi 4:

- Alert Management—Alert Actions
- Network—Physical NIC Interface—Administrative Status
- Network—Physical NIC Interface—DMA
- Network —Physical NIC Interface—Maximum Transmission Unit
- Network —Physical NIC Interface—Operational Status
- Preferences—SNMP Configuration
- Remote Shutdown—Power Cycle System with Shutdown OS First
- About Details—Server administrator component details not listed under Details tab

Server Administrator always displays the date in <mm/dd/yyyy> format.

Administrator 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 Administrator privileges can access critical system features such as the shutdown functionality included under the Shutdown tab.

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 in to 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.

Table 3-1 lists the GUI field names and the applicable system, when Server Administrator is installed on the system.

Table 3-1. System Availability for the Following GUI Field Names



GUI Field Name	Applicable System
Modular Enclosure	Modular System
Server module	Modular System
Main System	Modular System
System	Non-Modular System
Main system Chassis	Non-Modular System



NOTE: Administrator or Power User privileges are required to view most of the system tree objects, system components, action tabs, and data area features that are configurable. Additionally, only users logged in with Administrator privileges can access critical system features such as the shutdown functionality included under the **Shutdown** tab.

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 **Modular Enclosure** → **System/Server Module**, the major categories of system/server module components that may appear are **Main System Chassis/Main System**, **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/server module 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/Main System** object opens an action window in which the **Properties** action tab and **Health** subcategory are 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/Server Module Component Status Indicators

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

Table 3-2. System/Server Module Component Status Indicators





Symbol	Meaning
	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.

Table 3-2. System/Server Module Component Status Indicators (continued)

Symbol	Meaning
	A red X indicates that a component has a failure (critical) 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.
- Clicking **Email** creates an e-mail message addressed to your designated 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 Administrator privileges.

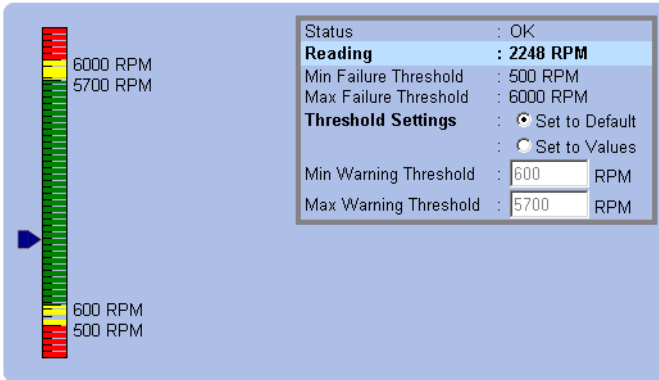
Underlined Items

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 3-1 shows readings from a system's CPU fan probe.

Figure 3-1. 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 left-hand 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.

See Table 3-3 for available Preferences home page configuration options.

Table 3-3. Preferences Home Page Configuration Options

-  General Settings
-  Server Administrator

You can view the **Preferences** tab after you log in to manage a remote system. This tab is also available when you log in to manage the Server Administrator Web server or manage the local system.

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-hand 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 or the Server Administrator Web server.
- The action window displays the available settings and preferences for the managed system or the Server Administrator Web Server.

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. This section is applicable to ESX only. For ESXi, you can use Restart Management Agent on the host to restart Dell OpenManage Services.

Starting Server Administrator

To start Server Administrator on systems, run the following command from the command line:

```
srvadmin-services.sh start
```

Stopping Server Administrator

To stop Server Administrator, run the following command from the command line:

```
srvadmin-services.sh stop
```

Restarting Server Administrator

To restart Server Administrator on systems, run the following command from the command line:

```
srvadmin-services.sh restart
```

Using the Server Administrator Command Line Interface



NOTE: The Server Administrator command line interface (CLI) is not applicable for ESXi.

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 *Dell OpenManage Server Administrator Command Line Interface User's Guide*.

Server Administrator Logs

Server Administrator allows you to view and manage hardware, alert, 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 Administrator privileges to clear logs or must be logged in with Administrator or Power User privileges to e-mail logs to their designated service contact.

See the *Dell OpenManage 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.

Server Administrator Logs

Server Administrator provides the following logs:

- Hardware Log
- Alert Log
- Command Log

Hardware Log



Use the hardware log to look for potential problems with your system's hardware components. On Dell PowerEdge x8xx, x9xx, and xx1x systems, the hardware log status indicator changes to critical status () 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 failure (critical) 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 changes from normal status () to noncritical status () 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.

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. The size of the command log file can be specified as per your requirement.

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 in to the Server Administrator home page or the CLI
- A description of the command and its related values.