Dell OpenManage Server Administrator With VMware ESXi 5.0

Systems Management Guide

Notes and Cautions

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.

2011 - 08 **Rev. A00**

Contents

1

Overview

NOTE: This document is for informational purpose only. The content is provided as is, without express or implied warranties of any kind.

NOTE: The OpenManage installation bundle (VIB) version 6.5 is a VMware accepted VIB. The support provided is the best effort support.

This post provides an overview of how Dell OpenManage Server Administrator (OMSA) 6.5 can be used with VMware vSphere 5.0 on Dell PowerEdge systems.

NOTE: Dell OpenManage Server Administrator 6.5 does not fully support vSphere 5.0; the full support will be available in the next release of OpenManage.

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 OpenManage software comes packaged with Dell PowerEdge systems, and VMware vSphere is VMware's hypervisor (ESX or ESXi) packaged with additional features.

The most recent release of OpenManage Server Administrator, 6.5 was in early 2011. vSphere 5.0 was released late August of 2011. The hardware world has been pretty active in that six month gap, and VMware has packed a lot of new features in their new major release.

Server Administrator 6.5

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 remotely from the Server Administrator home page. Remotely monitored systems are 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 locally-attached Redundant Array of Independent Disks (RAID) and non-RAID disk storage on a system.

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.
- Lets you 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 uses VMware's VIB mechanism to load Dell OpenManageServer Administrator agent in ESXi.

vSphere 5.0

VMware vSphere is the industry-leading virtualization platform for building cloud infrastructures and virtualization in general. It enables you to run business-critical applications and respond to business needs faster. vSphere accelerates the shift to cloud computing for existing datacenters and underpins compatible public cloud offerings, forming the foundation for the industry's only hybrid cloud model.

NOTE: For more information on vSphere 5.0, see the **vmware.com/files/pdf/products/vsphere/vmware-what-is-new-vsphere5.pdf**.

Dell Management Plug-in for VMware vCenter

VMware vCenter is the primary console used by IT administrators to manage and monitor VMware vSphere ESXi hosts. Using the Dell Management Plug-In for VMware vCenter, administrators have new capabilities to manage and monitor Dell hardware within the virtualized environment, such as:

- Alerting and environment monitoring
- Single server monitoring and reporting
- Firmware updates
- Enhanced deployment options

NOTE: Dell OpenManage Server Administrator Agent is a prerequisite.

For more information on Dell Management Plug-in for VMware vCenter, see **support.dell.com/support/edocs/software/eslvmwre/plugin/index.htm**.

Important Information

- For documentation on ESXi 5.0, see **support.dell.com/manuals**. Navigate to **Software → Virtualization Solutions → VMware Software**.
- For documentation on systems management described in this document, see **support.dell.com/manuals**. Navigate to **Software → Systems Management** and then select the relevant product for which you seek documentation.
- 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.

2

Installing Dell OpenManage Server Administrator

Before You Begin

- For more information on supported Dell servers, including a support matrix, configuration requirements, deployment, and so on for VMware vSphere 5.0, see **support.dell.com/support/edocs/software/eslvmwre**.
- Install Server Administrator on each system to be managed.
- The managed system requirements are:
  - Minimum of 3 GB of RAM.
  - Administrator rights.
  - TCP/IP connection on the managed and remote system to facilitate remote system management.
  - 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 you install a remote access controller (RAC) 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 managed system software installation. See the relevant *Dell Remote Access Controller User's Guide* for complete software and hardware requirements.
  - The Server Administrator Storage Management Service requires that you install Server Administrator 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 are 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.

ESXi 5.0 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 ESXi 5.0

1. Log on to the host using the vSphere Client.
2. Click the **Local 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. Type the login, user name, a numeric user ID (UID), and 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 ESXi

To install Server Administrator on systems running VMware ESXi 5.0, download the **Dell_OpenManage_ESXi_OM650-offline_bundle-467660.zip** file from <Refer to the Dell TechCenter Wiki media gallery>

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 5.0 host.

Using the vSphere CLI

1. Copy the **Dell_OpenManage_ESXi_OM650-offline_bundle-467660.zip** file to the `/var/log/vmware` folder on the ESXi5.0 server.
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:

   ```
   esxcli --server <IP Address of ESXi 5.0 host>
   software vib install -d /var/log/vmware/<Dell
   OpenManage file>
   ```
5. Type the root user name and password of the ESXi host when prompted.

   The command output displays a successful update.
6. Restart the ESXi host system.

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

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

Using the VMware vSphere Management Assistant

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

1. Log on to the vMA as an administrator and type the password when prompted.
2. Copy the **Dell_OpenManage_ESXi_OM650-offline_bundle-467660.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 vMA, run the following command:

   ```
   esxcli --server <IP Address of ESXi 5.0 host>
   software vib install -d /var/log/vmware/<Dell
   OpenManage file>
   ```

5. Type the root user name and password of the ESXi host when prompted.

   The command output displays a successful update.
6. Restart the ESXi host system.

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

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

Installing the Server Administrator Web Server

You must install the Server Administrator Web Server separately on a management station. You can download the Web Server from **support.dell.com**. For installation procedure, see the *Dell OpenManage Server Administrator Installation guide* available on the *Dell Systems Management Tools and Documentation* DVD or at **support.dell.com/support/edocs/software/omswrels/index.htm**.

NOTE: Make sure that you install only Server Administrator Web Server version 6.5.

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, 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.

Configuring the SNMP Agent on Systems Running ESXi 5.0

Server Administrator supports SNMP traps on ESXi 5.0. Server Administrator does not support SNMP **Get** and **Set** operations because ESXi 5.0 does not provide the required SNMP support. Use the vSphere command-line interface to configure a system running ESXi 5.0 to send SNMP traps to a management station.

NOTE: For more information about using the vSphere CLI, see **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. Configure one or more trap destinations 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:

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 to enter it.

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

3

Using Dell OpenManage Server Administrator

You can use the Distributed Web Server (DWS) login to access ESXi systems. For more information about DWS usage, see the *Dell OpenManage Server Administrator User's Guide*.

1. Open Server Administrator Web Server.
2. Click on the **Manage Remote Node** link.
3. Type the **IP address, User Name** and **Password of the managed system**.
4. Click **Submit.**

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 or Mozilla Firefox, an intermediate warning page may appear displaying the problem with the 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 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 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 certificate's snap in option to import certificates.

Login Failure Scenarios

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

- You have provided an invalid/incorrect IP address.
- You have provided 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 the **Ignore Certificate Warning** is not selected in the login page.
- The small footprint CIM broker daemon (SFCBD) service on the ESXi system is not running.
- The web server management service on the managed system is not running.
- You have provided the IP address of the managed system and not the hostname and the **Ignore Certificate Warning** check box is not selected.

The authentication may fail while connecting to the VMware ESXi 5.0 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 *vSphere Installation and Setup* 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 **vmware.com/support/pubs**.

Unsupported Server Administrator Features With ESXi

The following features of Server Administrator are not supported in ESXi 5.0:

- 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.

Known Limitation

You cannot log on to OMSA installed on ESXi 5.0 when Distributed Web Server (DWS) is installed on Windows Server 2003 and Windows XP.

This is due to winhttp limitation on these operating systems and security enhancement on WSMAN on ESXi 5.0.