Managing My Environment With Dell OpenManage Essentials

This Dell technical white paper explains how to configure Dell devices so that they can be managed using Dell OpenManage Essentials.
Managing My Environment With Dell OpenManage Essentials

Contents

Executive Summary ......................................................................................................................... 5
Introduction .................................................................................................................................. 6
Managing Servers Agentless ........................................................................................................ 6
Managing Servers With Agent (OMSA) Installed ......................................................................... 7
Configuring iDRAC7 and Later for Agentless Management and Monitoring: ................................ 8
I. Using OpenManage Essentials: ............................................................................................... 8
II. Using iDRAC console: ............................................................................................................ 11
Configuring iDRAC6 for Agentless Management ......................................................................... 13
I. Using OpenManage Essentials ............................................................................................... 13
II. Using iDRAC Console ............................................................................................................. 13
Configuring Servers With OMSA (Agent) Installed ..................................................................... 15
I. Configuring Dell PowerEdge Windows Servers With OMSA ................................................... 15
II. Configuring Dell PowerEdge Linux Servers With OMSA ....................................................... 18
III. Configuring Dell PowerEdge ESXi Servers With OMSA ....................................................... 22
Configuring iDRAC6 and Later for Agentless System Update Tasks ........................................ 22
I. Prerequisites for Performing System Update Using the iDRAC Update Method: ................. 22
Configuring Dell Client Systems using Dell Command Monitor .............................................. 23
Configuring Dell Equallogic (EQL) Storage Devices ................................................................ 23
Configuring Dell Force10 Networking Switches ......................................................................... 24
Configuring Dell PowerConnect Networking Switch ................................................................. 24
I. Using Serial Console or SSH Session: .................................................................................... 24
II. Using Web Console ................................................................................................................. 25
Configuring Dell Chassis Management Controller (CMC) ......................................................... 13
I. Using Chassis Web Console .................................................................................................... 13
II. Using OME ............................................................................................................................ 14
Configuring Dell PowerVault Modular Disk Storage Array ....................................................... 26
Configuring Dell Power Distribution Unit (PDU) ......................................................................... 27
Configuring Dell Universal Power Supply (UPS) ....................................................................... 28
Conclusion ................................................................................................................................... 30
Figures

Figure 1. Creating a Command Line Task in OME ................................................................. 9
Figure 2. Selecting Target Devices for the Command Line Task ........................................... 10
Figure 3. Providing Schedule and Credentials for the Command Line Task ............................. 11
Figure 4. Enabling Alerts on iDRAC7 and later From the iDRAC Console ............................... 12
Figure 5. Setting Up the SNMP Trap Destination From the iDRAC Console ............................. 12
Figure 6. Enabling Alerts From the CMC Console ................................................................. 14
Figure 7. Setting Trap Destination From CMC Console ........................................................... 14
Figure 8. Setting the SNMP Trap Destination on a Windows Server ..................................... 16
Figure 9. Setting SNMP Community String on a Windows Server .......................................... 17
Figure 10. Enabling Network Discovery on Windows Server 2008 and 2008 R2 ...................... 18
Figure 11. Configuring Dell EQL Devices for SNMP Discovery and Trap Destination .............. 23
Figure 12. Configuring Dell PowerConnect Switches for Setting Trap Destination .................. 25
Figure 13. Configuring Dell PowerConnect Switch to Setup SNMP Community String ............ 26
Figure 14. Configuring Trap Destination on MD Array ............................................................ 27
Figure 15. Configuring Trap Destination in Dell PDUs ............................................................. 28
Figure 16. Configuring Trap destination in Dell UPS ............................................................... 29
Figure 17. Configuring SNMP on Dell UPS ............................................................................... 29
Executive Summary

OpenManage Essentials is a one-to-many systems management tool which helps in monitoring servers, storage devices, printers, KVMs, UPSs, PDUs, chassis and network devices, etc. With the highest configuration supported (i.e., 8 GB RAM and 8 core processor) on the server running OpenManage Essentials, a maximum of 4000 devices can be monitored using OpenManage Essentials v2.1.

The goal of this white paper is to provide information on configuring various types of Dell devices such that they can be managed using Dell OpenManage Essentials (OME). After the devices are properly configured, they can be discovered and classified in OME’s device tree. The device tree shows the health status and discovery and inventory (asset data) information about these devices. OME can also be used to receive alerts (SNMP traps or Platform Event Traps) from properly configured devices when an alert is generated in the device.

NOTE: All the references to external links are at the time of print of current version of this white paper.
Introduction

The goal of this white paper is to describe how to configure the Dell devices that you want to manage and monitor using Dell OpenManage Essentials. When configuring Dell PowerEdge servers for management, it is possible to choose management using either the Dell agent (OpenManage Server Administrator or “OMSA”) or without the agent (agentless management), if the servers are 11th generation and later.

SNMP discovery of servers using OMSA requires SNMP settings to be configured on the operating system that has OMSA installed. OMSA is supported on Windows, Linux (Red Hat/SUSE Linux), XenServer, and ESXi operating systems. Details on how to configure SNMP settings for such operating systems is mentioned in this document.

Note: There may be slight variations in commands and screenshots used in this white paper depending on the operating system. Please refer to the OMSA User’s Guide or specific operating system details for the exact configuration.

Note: For performing any of the configurations described in this document, it is necessary to have administrator privilege on the device.

Dell’s 11th generation or later PowerEdge servers support agentless management by communicating directly with the server’s integrated Dell Remote Access Controller (iDRAC). The servers can be managed even if the operating system is shut down or not present. Configuration for agentless management is possible through a web console or by using the command line interface. Details on how to configure iDRACs for agentless management of Dell servers is also outlined in this white paper.

The configuration of Dell hardware devices such as switches, storage arrays, or PDUs is typically done using a console with a graphical user interface or alternately by using a command line interface (CLI).

The following table presents the features that are supported for various generations of Dell PowerEdge servers through agentless management as well as management through the Dell OMSA agent.

Version 2.1 of this white paper has been updated to provide information on 13th generation of PowerEdge servers, and includes the latest racadm commands and information on configuring CMC.

Managing Servers Agentless

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Discovery and Inventory</th>
<th>Monitoring</th>
<th>System Updates</th>
<th>Remote Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Generation</td>
<td>Discovery and Inventory</td>
<td>Complete Server health including attached storage, All SNMP v1/v2 alerts and Platform event traps</td>
<td>Perform BIOS, Application and firmware updates through iDRAC, Refer: Configuring iDRAC6/iDRAC7/iDRAC8 for Agentless System Update Tasks</td>
<td>RACADM, IPMI, generic and OMSA command line tasks</td>
</tr>
<tr>
<td>13G/12G</td>
<td>• Classifies as RAC • Software and hardware inventory fetched from iDRAC7 and later</td>
<td>Refer: Configuring iDRAC7/iDRAC8 for Agentless Management</td>
<td>Refer: Configuring iDRAC7/iDRAC8 for Agentless Management</td>
<td></td>
</tr>
</tbody>
</table>
### Managing Servers With Agent (OMSA) Installed


For the OMSA Support Matrix, refer to: [http://en.community.dell.com/techcenter/systems-management/w/wiki/1760](http://en.community.dell.com/techcenter/systems-management/w/wiki/1760)

#### Table 2. Support of Servers Through OMSA

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Discovery and Inventory</th>
<th>Monitoring</th>
<th>System Updates</th>
<th>Remote Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Refer: Configuring Dell PowerEdge Windows Servers With OMSA | - Classifies as Server in the OME device tree  
- Detailed hardware Inventory | - Complete server health  
- SNMP v1/v2 alerts from OMSA | Perform BIOS, application, firmware, and driver updates through OMSA | OMSA Command Line Tasks |
| **Linux**                 |                         |                          |                                                     |                                                  |
| Refer: Configuring Dell PowerEdge Linux Servers With OMSA | - Classifies as Server in the OME device tree  
- Detailed Hardware Inventory | - Complete server health  
- SNMP v1/v2 alerts from OMSA | Perform BIOS, application, and firmware updates through OMSA | OMSA Command Line Tasks |
| **ESXi/XenServer**        |                         |                          |                                                     |                                                  |
| Configuring Dell PowerEdge ESXi Servers With OMSA | - Classifies as Server in the OME device tree  
- Detailed hardware Inventory | - Complete Server Health  
- SNMP v1/v2 Alerts from OMSA | Not supported | Not Supported |

Columns:
- **Functionality**
- **Operating System**
- **Discovery and Inventory**
- **Monitoring**
- **System Updates**
- **Remote Tasks**
Configuring iDRAC7/iDRAC8 for Agentless Management and Monitoring:

I. Using OpenManage Essentials:

If iDRAC7 or later are discovered in OME, then RACADM command line tasks can be used to configure SNMP settings on the discovered iDRACs. This method helps you avoid configuring all the iDRACs individually.

Separate RACADM command line tasks must be created in OME to enable Alerts, set the destination IP address (OME server IP), set the community name, and enable all possible alerts. For more information on RACADM commands and configuring iDRAC7 and later, refer:


Note: The following example configures IPv4 settings. For information on configuring IPv6, refer to the earlier mentioned links.

The following is the list of RACADM commands required to remotely configure iDRAC7 and later to enable all alerts, set the community string, and set the OME server as the destination:

- `eventfilters set -c idrac.alert.all -a none -n snmp`
- `set iDRAC.IPMILan.AlertEnable Enabled`
- `set iDRAC.IPMILan.CommunityName {The_Community_Name}`
- `set idrac.snmp.alert.1.destaddr {OME_Server_IP_Addr}`
- `set idrac.snmp.alert.1.enable 1`

To configure iDRAC7 or above using the OME Remote Task Wizard:

1. Navigate to Manage >> Remote Tasks.
2. Click Create Command Line Task.
3. Provide a name for the task and select task type as RACADM Command Line.
4. Enter the following RACADM command in the Command box to enable all the alerts:
   ```
   eventfilters set -c idrac.alert.all -a none -n snmp
   ```
5. Select the Ping device option, if necessary. This pings the device first and if the ping fails then no attempt is made to run the command.
6. Select the Output to File option. Though optional, it is recommended that you select this option. Selecting this option creates a log file for each command that will run during this task.
Figure 1. Creating a Command Line Task in OME
8. Navigate to the **Task Target** tab and select the task targets that must be configured.

**Figure 2. Selecting Target Devices for the Command Line Task**
10. Navigate to **Schedule and Credentials**, provide the credentials, and select the time when you want to run this task.

11. Repeat steps 2-9 with the commands mentioned earlier. Separate RACADM task needs to be created for each setting. The same task can be cloned and edited to just change the command which is to be executed. To clone the task, right-click the task and select **Clone**.

12. [Optional]: To send a test trap from iDRAC to OME, create a command line task with the following command:

   \[ \text{Testtrap} \ - \text{i} \ 1 \]

   **Figure 3.  Providing Schedule and Credentials for the Command Line Task**

   ![Create a Command Line Task](image)

   All these settings can be found in iDRAC console under the **Alerts** section.

**II. Using iDRAC console:**

To enable SNMP alerts through the iDRAC console:

1. Log in to the iDRAC console.
2. Navigate to **Alerts**.
3. Under **Alerts**, select **Enabled** and click **Apply**.

**Figure 4.** Enabling Alerts on iDRAC7 and later From the iDRAC Console

4. Navigate to **SNMP and Email Settings**.

5. Select the check box next to **Alert Destination1** and enter the OME IP address in **Destination Address** box.

6. Provide the SNMP Community String and click **Apply**.

7. To check correct configuration and communication to OME, use the “Test SNMP Trap” button. This will send test alert from iDRAC to OME and the message reads “The iDRAC generated a test trap event”.

**Figure 5.** Setting Up the SNMP Trap Destination From the iDRAC Console

**Note:** These idrac snmp settings along with many other idrac, bios & firmware setting can be captured / exported in a xml ‘server profile’ file for mass deployment needs.

For more information on server profiles see: [http://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/esuprt_ent_sys_mgmt_opnmng_essentials/dell-opnmng-essentials-v2.0_white%20papers_en-us.pdf](http://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/esuprt_ent_sys_mgmt_opnmng_essentials/dell-opnmng-essentials-v2.0_white%20papers_en-us.pdf)
Managing My Environment With Dell OpenManage Essentials

Configuring iDRAC6 for Agentless Management

I. Using OpenManage Essentials

Similar to the configuration of iDRAC7 and later, RACADM commands can be used for configuring SNMP settings and alerts on iDRAC6. Four different RACADM command line tasks are needed in OME to configure iDRAC6 for enabling traps, set destination IP address, set the community name, and enable the alert destination. For more details on the RACADM commands for iDRAC6, refer:


Note: The following example configures the IPv4 settings. For information on configuring IPv6, refer to the earlier mentioned link.

The following is the list of RACADM commands required to remotely configure iDRAC6 to enable all alerts, set the community string, and set the OME server as the destination for receiving traps:

- `config -g cfgipmilan -o cfgipmilanalertenable 1`
- `config -g cfgipmiPet -o cfgipmiPetAlertEnable -l 1 1`
- `config -g cfgipmiPet -o cfgipmiPetAlertDestIPAddr -l 1 {OME_IP_Address}`
- `config -g cfgipmilan -o cfgipmilanCommunityName {community-string}`

The steps to configure trap settings on iDRAC6 using OME is same, except that the commands which are to be used are different. For detailed steps, refer Configuring iDRAC7 and Later for Agentless Management Using OpenManage Essentials.

II. Using iDRAC Console

The following sections provide the steps to enable alerts, set the trap destination, and set the community string on iDRAC6. Depending on the iDRAC6 firmware, the console GUI options may vary and may be different than what is described in this white paper.

NOTE: Platform event filters should be configured before configuring platform event trap or e-mail alert settings

Configuring Dell Chassis Management Controller (CMC)

SNMP configuration on a Dell CMC can be performed using any of the following methods:

I. Using Chassis Web Console

The following steps must be performed for configuring trap destination on a CMC using web console:

1. Log in to CMC web interface.
2. Navigate to Chassis Overview >> Alert.
4. From **Alert Filter** and **Monitored Alerts** sections, select the alerts which should be generated from chassis.

5. Click **Apply**.

**Figure 6. Enabling Alerts From the CMC Console**

6. Navigate to **Trap Settings** under Alerts

7. Select **Enabled** from any of the Destination Numbers and enter the OME IP address, SNMP community string.

8. Click **Apply**.

**Figure 7. Setting Trap Destination from CMC Console**

II. **Using OME**

SNMP configuration of a CMC can also be performed in a manner that is similar to SNMP configuration of a RAC by using OME.

The following is the list of RACADM commands needed to remotely configure CMC to enable all alerts, set the community string, and set the OME server as the destination:

- `config -g cfgAlerting -o cfgAlertingEnable 1`
- `racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>`
Managing My Environment With Dell OpenManage Essentials

where <mask value> is a hex value between 0x0 and 0xffffffff.

- `racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>`
  where <index> is a value of 1-4.
- `racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>`
  where <IP address> is a valid destination, and <index> is the index value you specified in step 4.
- `racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i <index>`
  where <community name> is the SNMP community to which the chassis belongs, and <index> is the index value you specified in steps 4 and 5.
- `racadm testtrap -i <index>`

The steps to configure the SNMP trap settings on CMC by using OME are the same, except that the commands are different and the target should be a CMC. For detailed steps, refer Configuring iDRAC7 and Later for Agentless Management Using OpenManage Essentials.


Configuring Servers With OMSA (Agent) Installed

I. Configuring Dell PowerEdge Windows Servers With OMSA

To install OMSA on a windows server:

   After the OMSA package is downloaded, double click the .exe file to extract the setup and run Setup.exe or follow the instructions on autorun.

OMSA can also be installed by using the Dell Systems Management Tools and Documentation DVD. This DVD provides a setup program to install, upgrade, and uninstall Server Administrator, managed system and management station software components. More details on this DVD can be found at http://en.community.dell.com/techcenter/systems-management/w/wiki/11433.openmanage-dvd.

2. Configure SNMP service on the server and verify that the SNMP service is running. Perform the following to setup SNMP service:
   a. Open the Services console: Click the Windows Start menu and select Run. Type services.msc and click ‘OK’.
   b. Browse through the list of services and select SNMP Service.
   c. Right-click the SNMP Service and select Properties.

Note: If SNMP Service is not present, it means that it is not installed. For information on how to install SNMP service on a Windows server, refer: https://technet.microsoft.com/en-in/library/cc759570(v=ws.10).aspx
d. Navigate to the SNMP Service Properties >> Security Tab and clear the Send authentication trap option.

e. Enter the community string with READ ONLY rights.

f. Select Accept SNMP packets from any host or Accept SNMP packets from these hosts and add the OME IP address to the list of accepted hosts.

Figure 8. Setting the SNMP Trap Destination on a Windows Server

g. Navigate to SNMP Properties >> Traps tab and enter the community string to the community list.

h. Enter the OME server IP address or hostname to the trap destinations list.

i. Click OK and exit the SNMP properties window.

3. Right-click the SNMP Service from the list of services and select Restart.

4. The OME server should have received LinkUp alerts from this server.

Note: More details on configuring SNMP can be found at https://support.microsoft.com/en-us/KB/324263

A video with details on setting up SNMP for OMSA monitoring and alerts can be found at http://en.community.dell.com/techcenter/m/videos/20079605
5. **Firewall settings:**

When the firewall is enabled on a Windows operating system, it will block communication between OME and the server. SNMP uses UDP port 161 for sending and receiving requests, and port 162 for receiving traps from the managed system. Configure the firewall settings to allow port 161 and 162. Also, allow WMI (Windows Management Instrumentation) communication through the Windows firewall. Enable Remote WMI as well. For information, refer: [http://msdn.microsoft.com/en-us/library/windows/desktop/aa822854(v=vs.85).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa822854(v=vs.85).aspx)

![SNMP Service Properties (Local Computer)](image)

**Figure 9. Setting SNMP Community String on a Windows Server**

**Note:** For Windows Server 2008 and 2008 R2 only, it is necessary to Enable Network Discovery. Navigate to Control Panel >> Network and Internet >> Network and Sharing Center >> Change Advanced Sharing Settings and select the Turn on network discovery and click Save.
II. Configuring Dell PowerEdge Linux Servers With OMSA

When Dell OpenManage Server Administrator (OMSA) is installed on a Linux server, detailed hardware inventory can be obtained if the server is discovered in OME. After OMSA is installed on the target system, health monitoring, system updates, and remote tasks are also possible through the OMSA agent.

OMSA is supported only on Red Hat Enterprise Linux and SUSE Linux Enterprise operating systems. Please review the latest Dell OpenManage Software Support Matrix for supported Linux operating systems.

**Note:** You can install OMSA on all Linux systems even if the server is not supported, however complete functionality is not guaranteed.

The following steps are needed to be performed to install OMSA:

**Note:** Some of the following steps such as the pre-requisites for installing OMSA may already be complete on the target system. Therefore, you can run or skip steps as necessary.

**Note:** The commands included in this white paper may vary depending on the distribution of Linux that is installed on the server. The following commands have been verified on RHEL 6.3

1. **Install Net-SNMP Package (Pre-requisite)**
   a. Configure SNMP service and make sure that SNMP service is active and running on the Linux server.
   b. You can verify that SNMP service is running, start, or restart the service by using the following command:
      ```bash
      /etc/init.d/snmpd <start | status | restart>
      ```
      If SNMP package is not installed, install the package. The following link provides more information on configuring SNMP on a Linux server:

      http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_-_Ch22_-_Monitoring_Server_Performance#Installing_SNMPUtilities_on_a_Linux_Server
2. **Install OMSA Dependencies (Pre-requisite)**

OMSA requires several dependency RPMs for remote enablement support. These RPMs are often already installed. If the RPMs are already installed, you can skip this step.

Required packages:

- `libcmpiCppImpl0`
- `libwsman1`
- `openwsman-server`
- `sblim-sfcb`
- `sblim-sfcc`

The following commands can be used to verify if the packages are installed. If they are installed, this command will return the name of the package. If no result is returned, then it means that no matching package was found.

```
- rpm -qa | grep libcmpi*
- rpm -qa | grep libwsman1*
- rpm -qa | grep openwsman*
- rpm -qa | grep sblim-sfcb*
- rpm -qa | grep sblim-sfcc*
```

If these RPMs are needed to be installed, then they can be extracted from the following folder on the **Dell Systems Management Tools and Documentation DVD**:

```
[linux\RPMS\supportRPMS\opensourcecomponents\<OS>\<architecture>]
```

The following sequence must be followed to install the required RPMs.

**Note:** `libwsman1` and `openwsman-clientx` should be installed at the same time because they have a cyclic dependency.

```
- rpm -ivh libcmpiCppImpl0-x.x.x.rpm
- rpm -ivh sblim-sfcb-x.x.x.rpm
- rpm -ivh sblim-sfcc-x.x.x.rpm
- rpm -ivh libwsman1-x.x.x.rpm openwsman-clientx.x.x.rpm
- rpm -ivh openwsman-server-x.x.x.rpm
```

3. **Install OpenManage Server Administrator on the Linux server:**

There are multiple ways to perform OMSA installation:

a. **Using the linux.dell.com Repository**:
   i. Set up the Dell OpenManage Repository at http://linux.dell.com/repo/hardware, using the following command:

   ```
   wget -q -O - http://linux.dell.com/repo/hardware/latest/bootstrap.cgi | bash
   ```
ii. Then, install OpenManage Server Administrator:

- `yum install srvadmin-all`

**Note:** You can install OMSA on all Linux systems even if the server is not supported. However, complete functionality is not guaranteed.

**Note:** More detailed information about the Dell Linux repository can be found at:

http://linux.dell.com/repo/hardware/omsa.html

b. Using the Dell Systems Management Tools and Documentation DVD:

Detailed information about the OpenManage DVD can be found at:


c. Downloading the Package From Dell TechCenter:

Information on how to install OMSA can be found at:

http://en.community.dell.com/techcenter/systems-management/w/wiki/1760

The following steps must be performed for installing the package downloaded from Dell TechCenter.

**Note:** Run the following commands to determine the Red Hat Enterprise Linux version and processor:

- `uname -a`
- `cat /etc/issue`
- `cat /etc/redhat-release`

**Note:** Run the following commands to determine the SUSE Linux version and processor:

- `uname -a`
- `cat /etc/issue`
- `cat /etc/SuSE-release`

After the appropriate package is found for the Linux version and processor (x86 or x64), download the OMSA package to that Linux system. The following commands must be used to unpack and install OMSA:

- `tar -xzf OM-SrvAdmin-Dell-Web-LX-7.1.0-5304_A00-00.tar.gz`
- `./setup.sh`

Run the following command to verify if OMSA services are running:

- `rpm -qa | grep srvadmin`

To start or restart OMSA services:

- `srvadmin-services.sh start`
- `srvadmin-services.sh restart`
Managing My Environment With Dell OpenManage Essentials

To verify SNMP settings for OMSA:

- Open the following file for editing:
  - /etc/snmp/snmpd.conf
- Verify if the following 3 lines exist or add them to the file if they do not:
  - view all included .1
  - access notConfigGroup "" any noauth exact all none none
  - smuxpeer .1.3.6.1.4.1.674.10892.1

Inventory collector must be installed on 64-bit Servers.

- Install the 32-bit version of zlib and compat-libstdc++ libraries.
- Install the srvadmin-cm package available in the /linux/RPMS/supportRPMS/srvadmin folder of the Dell Systems Management Tools and Documentation DVD.

The next step is to configure the SNMP community string. To modify the community string:

- Open the file /etc/snmp/snmpd.conf for editing
- Add the following line to snmpd.conf file:
  - rocommunity <Community_String>
- To enable the changes, restart the SNMP agent by using the following command:
  - /etc/init.d/snmpd restart

4. Configure SNMP Traps to the OME Management Station

To configure SNMP traps and set trap destination on a Linux server:

1. Open the following file for editing:
   - /etc/snmp/snmpd.conf
2. Add the following line to snmpd.conf file:
   - Trapsink <OME IP Address> <community name>
3. To enable the changes, restart the SNMP agent by using the following command:
   - /etc/init.d/snmpd restart

5. Firewall Configuration

If the firewall was enabled during the Linux installation, it will close the SNMP port blocking all external connections by default. Server Administrator will detect this and log a warning message to the system event log.

SNMP port must be opened on the server for OpenManage Essentials to communicate with it or else this will block OME from discovering, inventoring and receiving alerts for the server.
Refer to your specific Linux distribution for configuring firewall settings. IPTABLES must be configured to allow access to UDP port 161 and 162 for SNMP communication and TCP port 1311 for OMSA. There are various options that can be added to the IPTABLES file but the basic entries for allowing traffic on these ports is as follows:

- A RH-Firewall-1-INPUT -p udp -m udp --dport 161 -j ACCEPT
- A RH-Firewall-1-INPUT -p udp -m udp --dport 162 -j ACCEPT
- A RH-Firewall-1-INPUT -p udp -m udp --dport 1311 -j ACCEPT

Save the changes made to IPTABLES:

- service iptables save


III. Configuring Dell PowerEdge ESXi Servers With OMSA

Detailed instructions on installing and configuring OMSA on VMware ESXi servers can be found at [http://en.community.dell.com/techcenter/extras/m/white_papers/20071085](http://en.community.dell.com/techcenter/extras/m/white_papers/20071085)

Configuring iDRAC6/iDRAC7/iDRAC8 for Agentless System Update Tasks

Agentless system update in OME does not need OMSA on the managed system to gather inventory and deploy firmware and BIOS updates. Agentless updates are applied via Integrated Dell Remote Access Controller (iDRAC6 and later) on Dell servers.

I. Prerequisites for Performing System Update Using the iDRAC Update Method:

- 11th generation servers:
  - Modular: Minimum iDRAC6 firmware version 2.20
  - Monolithic: Minimum iDRAC6 firmware version 1.40
- 12th generation servers and later:
  - Express or Enterprise license
  - iDRAC is discovered and inventoried using WS-Man protocol


A detailed white paper on using OME to perform software updates can be found on the Dell TechCenter website at [http://en.community.dell.com/techcenter/extras/m/white_papers/20217144.aspx](http://en.community.dell.com/techcenter/extras/m/white_papers/20217144.aspx).
Configuring Dell Client Systems using Dell Command Monitor

Basic management, system health, and inventory can be achieved for Dell client systems (OptiPlex, Precision, and Latitude) with the help of Dell Command Monitor. Instructions for using Dell Command Monitor and downloads for 32-bit and 64-bit client systems can be found at http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7531.dell-command-monitor

SNMP and WMI discovery of Dell client systems is supported in OME version 2.1 and later.

Configuring Dell Equallogic (EQL) Storage Devices

The following steps must be performed after logging into the EQL management console:

1. Click Group Configuration and select SNMP tab.
2. Click Add and enter the SNMP community string.
3. Click Add in the SNMP trap Destinations pane.
4. Enter the OME IP address for SNMP trap destinations.

Figure 11. Configuring Dell EQL Devices for SNMP Discovery and Trap Destination
Managing My Environment With Dell OpenManage Essentials

Configuring Dell Force10 Networking Switches

The following steps must be performed to set the SNMP community string and SNMP trap destination of a Force10 networking switch:

1. Log in to the networking switch using the management IP address with a serial connection or SSH session.
2. The following commands should be run to set up the SNMP community name.
   - `snmp-server community ro/rw <community_string>`
     where ro or rw can be used accordingly to specify read-only or read-write access. Su can be used to specify SNMP administrator access. `<OME_IP_address>` represents the IP address of OME server.
     For example, `snmp-server rw public`
     or `snmp-server ro public`
3. The following command should be executed to enable SNMP traps and add a trap destination:
   - `snmp-server host <OME_IP_Address>`
     This command enables ALL available traps from a Force10 switch
   - `snmp-server enable traps`
   - `snmp-server enable traps snmp`


Configuring Dell PowerConnect Networking Switch

The following steps must be performed to set the SNMP community string and SNMP trap destination of a Dell PowerConnect Networking switch:

1. **Using Serial Console or SSH Session:**
   1. Log in to switch using management IP address with serial connection or SSH session.
   2. The following command should be run to set up the SNMP community name:
      - `snmp-server community <community_string> ro/rw <OME_IP_Address>`
      where ro or rw can be used accordingly to specify read only or read write access. Su can be used to specify SNMP administrator access. `<OME_IP_address>` represents the IP address of OME server.
3. The following command should be used to configure SNMP traps and set its SNMP community string.
   - `snmp-server host <OME_IP_address> <Community_String> <1/2>

   Where `<OME_IP_Address>` is the IP address of OME server, `<Community_String>` is the community string used for outbound traps and 1 or 2 can be either SNMP v1 traps or SNMP v2 traps, respectively.

   For example, `snmp-server host 192.168.1.10 public 2`

II. Using Web Console

   1. Log in to the web console of the Dell PowerConnect switch.
   2. Navigate to Home >> SNMP >> Global Parameters.
   3. Enable SNMP Notifications and Authentication Notifications.
   4. Click Apply Changes.

   ![Configuring Dell PowerConnect Switches for Setting Trap Destination](image)

   5. Navigate to SNMP >> Home >> Communities.
   6. Enter the SNMP community string and click Apply Changes.
   8. Enter the Recipient IP address as OME server’s IP address.
   9. Click Apply Changes.
Figure 13. Configuring Dell PowerConnect Switch to Setup SNMP Community String

Configuring Dell PowerVault Modular Disk Storage Array

For configuring SNMP traps on a PowerVault MD array, the PowerVault Modular Disk Storage Manager (MDSM) application is required. This can be found on the Dell Resource Disk that shipped with the storage device or at Dell.com/Support.

After MDSM is installed, the OME console IP address must be added to the list of destinations to send alerts from the MD array. To add the OME IP address to the list of trap destination, perform the following on MDSM:

1. Click Edit from the menu options or right-click on an array and select Configure Alerts.
2. Click SNMP from the Configure Alerts window.
3. Enter the community string and IP address of OME server to receive alerts.
4. Click Add.
5. Repeat steps 3 and 4 if you want to add more management stations for receiving alerts.
6. Click OK.
To configure SNMP on PDUs such that they can be discovered and monitored in OME using SNMP:

1. Launch PDU console by using the IP address of PDU.
2. Navigate to Administration >> Trap Receivers.
3. Click on Add Trap Receiver.
4. On the next window, check the box for Trap Generation.
5. Enter the hostname or IP address of OME Management Console.
6. Enter the Community name.
7. Click Apply.
Figure 15. Configuring Trap Destination in Dell PDUs

Configuring Dell Universal Power Supply (UPS)

To configure Dell UPS for SNMP discovery:

1. Log in to the Dell UPS console.
2. Navigate to Notified Applications.
3. Click Add NAS.
4. Enter the application Name: OME.
5. Enter the OME server IP address or hostname.
6. Enter the SNMP community string.
7. Navigate to Settings >> Access Control
8. Enable SNMP.
9. Provide the SNMP Community string.
10. Click Save.
Conclusion

OpenManage Essentials version 2.1 can be used to perform management and monitoring of Dell servers and devices that are configured as required.