How to Configure VMware ESX Classic Server for discovery in OpenManage Essentials

This Dell Technical White Paper addresses the steps required to configure VMware ESX Classic server to show OMSA and VMware agent data for OpenManage Essentials discovery.

Sean Kim

Dell Enterprise Product Group

February 2012| Version 1.0

Contents

Introduction

On ESX Classic 4.0 server, the VMWare SNMP provider is its own daemon (*vmware-hostd*) and does not register with the system default SNMP daemon (*snmpd*), requiring a management console to request VMWare SNMP data on another port than what OMSA registers with (*snmpd*). This document includes steps to configure the VMWare SNMP daemon and the system default SNMP daemon so that they both can provide SNMP data on the default SNMP daemon port 161.

The objective of this configuration is to allow ESX4.0 server to be managed through a single default port 161 using SNMP protocol. To do this, snmpd is configured to use the default port 161 and vmware-hostd is configured to use a different, unused, port (e.g. 171). Any SNMP request on the VMWare MIB branch will be rerouted to vmware-hostd using the proxy feature of the snmpd daemon.

Download and install OMSA from your ESX server

Using the `curl` command, in the ESX console, download the OMSA package for your ESX server.

```
curl -O http://downloads.dell.com/FOLDER00553825M/1/OM-SrvAdmin-Dell-Web-LX-7.1.0-5304.ESX40.i386_A00-00.tar.gz
```

This example may work for other server models; however, the URL is for OMSA 7.1 for a R710 server running ESX classic 4.0.

URL for the OMSA packages can be found at http://downloads.dell.com by navigating through the menu selecting system type (i.e. PowerEdge), model (i.e. PowerEdge R710), then selecting the 'System Management' link.

Extracting the OMSA package

- Browse to the location where you downloaded the file and unzip the package using the following command:

  ```
  unzip OM-SrvAdmin-Dell-Web-LX-7.1.0-5304.ESX40.i386_A00-00.tar.gz
  ```

- Un-tar the package using the following command:

  ```
  tar -xvf OM-SrvAdmin-Dell-Web-LX-7.1.0-5304.ESX40.i386_A00-00.tar
  ```

Installing OMSA

- Change current directory to the location where the files were extracted.
- Run the following command to start the install process. (The following shell script should be available at the root of the folder where the OMSA package was extracted.)

  ```
  ./setup.sh
  ```

- Alternatively, you can navigate to */linux/supportscripts* and run the following command.

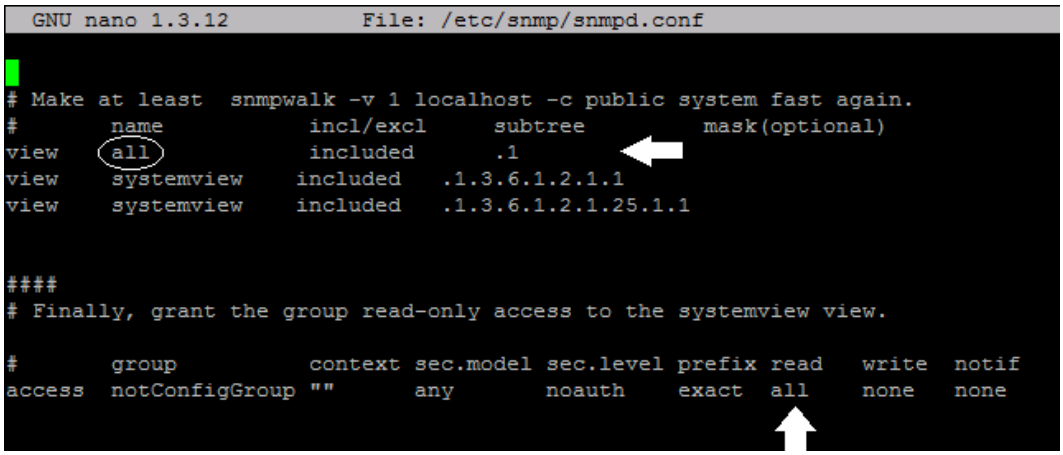
  `./srvadmin-install.sh`

- Select option 7 and then select 'i' to install, and when the install completes, select yes to start the OMSA services.

SNMP changes made by OMSA install

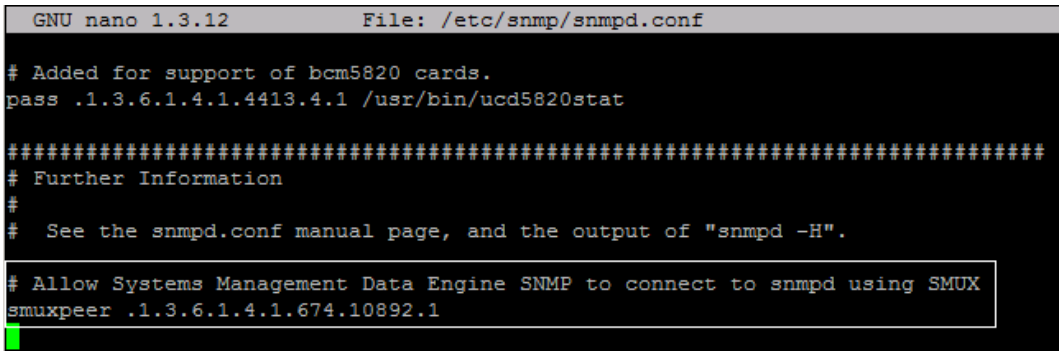
- Open *snmpd.conf* in a text editor. (i.e. nano or vi text editor)
- The default location for `snmpd.conf` is `root/etc/snmp/snmpd.conf`
- Installing OMSA adds a "view" configuration named "all" in the *snmpd.conf* file and changes the "read" attribute of the group access to "all" from the default "systemview."

Figure 1. View configuration added by OMSA installation



- Following lines are added to the bottom of the `SNMP.conf` file:

Figure 2. SMUX added by OMSA installation



Configure SNMP on ESX Classic

- Using the default text editor, nano, enter the following command line at the prompt:

  `nano /etc/vmware/snmp.xml`

- Locate the communities tag; by default, the community string is `public`.
- Replace the communities string with an appropriate read-only community strings for your environment, separated by commas.
- Locate the enable tag, and then confirm it is set to *true*.
- Locate the port tag, and then confirm it is set to *171* (or any other available port you prefer).
- Locate the targets tag, and then confirm it is set to `127.0.0.1@161/`*c-string*.
- Replace *c-string* with the community string you provided in step 3, above.
- Save `snmp.xml`, and then close your editor.
- Press Ctrl+X to close nano, and then enter 'Y' then Enter to save snmp.xml.

Alternatively, VMware vSphere CLI utility can be used to accomplish the above steps.

Download RCLI utility tool from the VMware website.

- Go to *https://my.vmware.com/web/vmware/downloads*
- From the `Product Download Index`
  - Select "`VMware vSphere`" under "`Datacenter & Cloud Infrastructure`"
- The site will default to the download page of the latest version available.
- Select the applicable version of vSphere hypervisor architecture.
  - Links for other versions are located above the "Product Downloads" tab.
- Select the "`Drivers & Tools`" tab, then expand the "`Automation Tools and SDKs`" list.
  - Download the applicable version of "`VMware vSphere CLI`".
- The VMWare SNMP configuration file can be modified manually on the ESX server or by running VMWare RCLI command `vicfg-snmp` from a remote system (Windows or Linux).
- Use `vicfg-snmp.pl` command to modify the SNMP configuration settings which includes the SNMP listening port, community string, the trap target IP_Address/port, trap community name and then enable the VMWare SNMP service.

  ```
  vicfg-snmp.pl --server <ESX_IP_addr> --username root --password
  <password> -c public -p 171 -t 127.0.0.1@162/public
  ```

- To find an unused port, you may look at the */etc/services* file for the port assignment for defined system services. Also, make sure that the port selected is not currently being used by any application/service, run the following command on the ESX server.

  netstat -a --numeric-ports

- To enable VMWare SNMP service, run the following command:

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

- To view the configuration settings run the following command:

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

- After the modification, the configuration file will look like this:

vSphere CLI output	/etc/vmware/SNMP.xml
Current SNMP agent settings: Enabled: 1 UDP port: 171 Communities: public Notification targets: 127.0.0.1@162/public	<config> <snmpSettings> <communities>public</communities> <enable>true</enable> <port>171</port> <targets>127.0.0.1@162/public</targets> </snmpSettings> </config>

Configure SNMP on ESX Classic (continued):

- Enter *service snmpd stop* to stop SNMP service.
- Open `snmpd.conf` in a text editor.
- The default location for `snmpd.conf` is `root/etc/snmp/snmpd.conf`.
- Using the default text editor, nano, enter the following command line at the prompt:

  ```
  nano /etc/snmp/snmpd.conf
  ```

- Edit *snmpd.conf* and add the following lines to the bottom of file:

  ```
  proxy -v 1 -c public udp:127.0.0.1:171 .1.3.6.1.4.1.6876
  ```

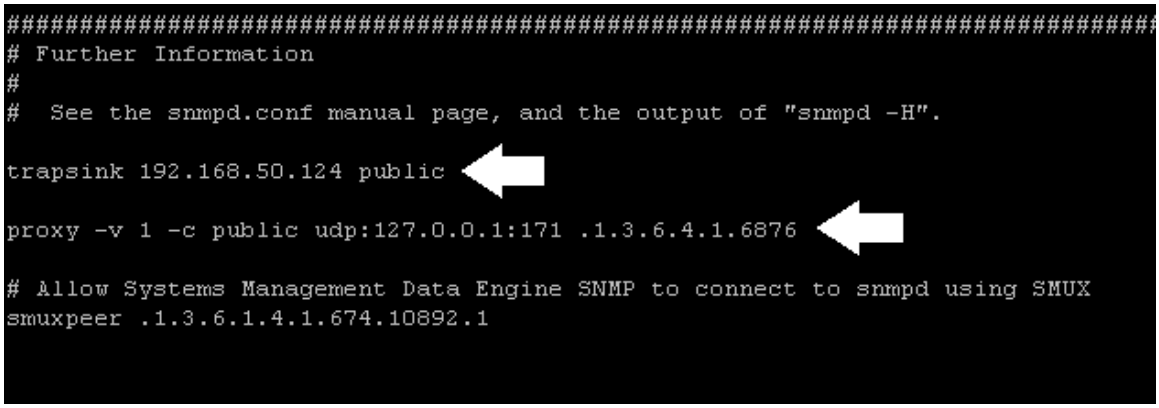
  - This line sends the VMWare agent SNMP data to the local host (127.0.0.1) using port 171, which was configured in the `/etc/vmware/snmp.xml` file in a previous step.
  - Replace the community string accordingly.

- Edit snmpd.conf and add the following lines to the bottom of the file to configure SNMP trap destination.

  ```
  trapsink 192.168.50.124 public
  ```

  - `trapsink <OME_IP_Address> <community>`

Figure 3. Net-SNMP proxy and Trap Destination



- Save changes made to *snmpd.conf* and then close the editor.
    - Press Ctrl+X to close nano, and then enter 'Y', then Enter to save snmpd.conf.

Configure ESX Classic Firewall

- After installing OpenManage, you need to run the following commands:

```
esxcfg-firewall -o 1311,tcp,in,OpenManageRequest
esxcfg-firewall -o 162,udp,out,snmptrap
esxcfg-firewall -o 162,udp,in,snmptrap
esxcfg-firewall -o 161,tcp,in,snmp
esxcfg-firewall -o 161,tcp,out,snmp
esxcfg-firewall -o 161,udp,in,snmp
esxcfg-firewall -o 161,udp,out,snmp
```

- Enter the following command line to restart the VMware agent services:

```
service mgmt-vmware restart
```

- Enter the following command line to start the SNMP service:

```
service snmpd start
```

- Enter the following command line to auto-start SNMP service at boot-up:

```
chkconfig snmpd on
```

- Enter the following command line to allow SNMP through the ESX Server firewall:

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

Verify Configuration

Enter the following command line to confirm that SNMP polling is enabled on your ESX Server by entering the following command:

- Replace '*public*' with the applicable community string.

```
snmpwalk -v1 -c public localhost .1.3.6.1.4.1.6876 | grep 6876.1
```

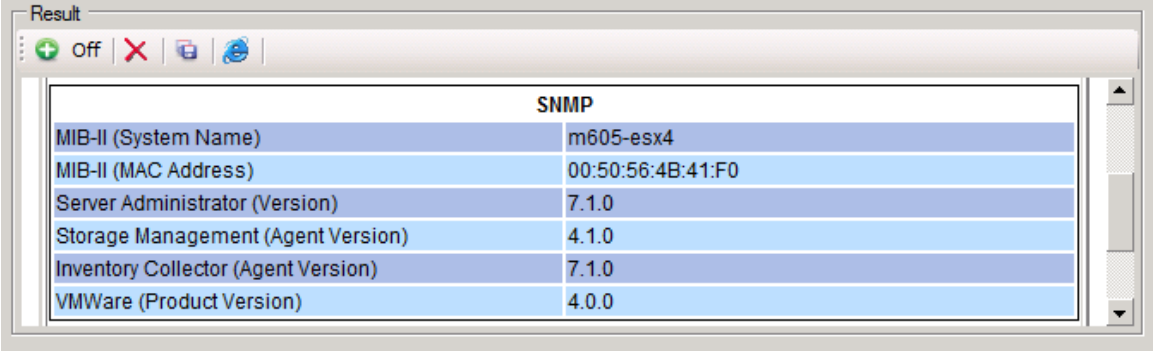
- The snmpwalk output should look like this. (The product version and build numbers will vary).
- No results will show in the ESX console if SNMP is not configured properly.

```
SNMPv2-SMI::enterprises.6876.1.1.0 = STRING: "VMware ESX"
SNMPv2-SMI::enterprises.6876.1.2.0 = STRING: "4.0.0"
SNMPv2-SMI::enterprises.6876.1.4.0 = STRING: "208167"
```

Alternatively, you can use Dell Troubleshooting Tool.

- Only the MIB-II (System Name) attribute will be shown if SNMP is not configured properly.
- All three attributes should be shown for OME to properly discovery and inventory the ESX Classic server.
- The result should look like this:

Figure 4. Dell Troubleshoot Tool Results



Alternative firewall options (optional)

- Disable firewall:

```
esxcfg-firewall -allowOutgoing
esxcfg-firewall -allowIncoming
```

- If you want it live through a reboot:

```
chkconfig firewall --level 2345 off
```

- To turn it all back on:

```
chkconfig firewall --level 2345 on
esxcfg-firewall -BlockIncoming
esxcfg-firewall -BlockOutgoing
```

Additional resources

Dell OpenManage Essentials

- For more information on Dell OpenMange Essentials visit www.dell.com/ome or www.delltechcenter.com/ome.

Dell OpenManage Administrator

- Dell OpenManage is a collection of software tools developed by Dell that helps you discover, monitor, manage, and update Dell servers.
- Documentation and downloads for OpenManage Server Administrator may be found at http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.aspx.

- Dell Brand Identity Standards
- Dell Voice Standards
- What is a White Paper?