

# Integrating OpenNMS with OpenManage Server Agent

## to Manage Dell PowerEdge Servers Running Linux

Enterprises that adopt the Red Hat® Linux® operating system (OS) and run it on Dell™ PowerEdge™ servers require a way to manage these environments. OpenNMS (Open Network Management System) is an open source network management platform that works well for managing Linux environments. OpenNMS can monitor the performance of nodes on a network through the use of Simple Network Management Protocol (SNMP). This article explains how to configure SNMP and Dell OpenManage™ Server Administrator to work with OpenNMS.

BY JOSHUA GILES

Enterprise IT departments are migrating from the UNIX® operating system (OS) to the Linux® OS at a fast pace. As an open source project, Linux offers a stable, freely available, and highly modifiable OS. In conjunction with Dell™ PowerEdge™ servers, Red Hat® Linux is becoming the enterprise OS of choice in the high-performance computing (HPC) cluster field. Administrators of these environments require an enterprise systems management tool that complements the unique qualities of the Linux OS, while providing an effective method of managing network servers.

Preventing server downtime and hardware failures that cause poor performance is important for maintaining low total cost of ownership (TCO). The use of the Server Agent component of Dell OpenManage™ Server Administrator with the enterprise-grade OpenNMS (Open Network Management System) may reduce downtime and improve performance through better management of Linux networks that use Dell servers. OpenManage Server Agent resides on individual servers to enable systems

management functionality, such as problem detection and event notification. OpenNMS is a free, widely accepted, mature software project maintained at the open source forum SourceForge. OpenNMS uses Simple Network Management Protocol (SNMP) to collect performance data for analysis of networks containing many different platforms, including Linux servers. Any server with an SNMP agent installed can send information about hardware, known as traps, to OpenNMS.

This article explains how to install and configure SNMP and OpenManage Server Agent on a network of pre-existing servers that run the Linux OS. Servers running SNMP and OpenManage Server Agent are referred to as managed nodes. OpenNMS resides on one central server in the network, known as a network management station; this station also runs the Linux OS. In addition, administrators can install and configure OpenNMS to work with OpenManage Server Agent to provide event notification and problem detection.

## Examining the network configuration

An environment configured for enterprise systems management generally includes an internal network consisting of one or more network management stations, or master nodes, dedicated to monitoring the remaining managed nodes within the network (see Figure 1). In the scenario in this article, each managed node is connected through its Ethernet interface to the Class C 192.168.0.0/24 subnet. Each managed node comprises a Dell PowerEdge 1650 server running Red Hat Linux version 7.3 on which SNMP and Dell OpenManage Server Agent are installed. The network management station has the same configuration as the managed nodes, but also has OpenNMS software installed. In the sample scenario, the Ethernet device in the network management station has an IP address of 192.168.0.2.

## Setting up SNMP, OpenManage Server Agent, and OpenNMS

OpenManage Server Agent uses SNMP to send data, in the form of SNMP traps, to the network management station. OpenNMS runs on the network management station and collects this data. OpenManage Server Agent contains an Embedded Systems Management driver (esm.o) that interfaces with the Embedded Systems Management hardware to receive status information about various PowerEdge server hardware components. Managed nodes send this hardware information in the form of SNMP traps to the network management station.

### Installing SNMP and OpenManage Server Agent

To enable SNMP, administrators must install the NET-SNMP Red Hat Package Manager (RPM™) file archive program, or package, on all managed nodes on the network. The RPM package contains the SNMP master agent and basic NET-SNMP command toolset. Although these RPM packages can be retrieved from the Red Hat/RPMS/ directory on the first Red Hat Linux 7.3 CD, the latest errata RPM package located at [www.redhat.com/errata](http://www.redhat.com/errata) should be used instead.

Install the RPM packages using the rpm program:

```
rpm -Uvh snmp_package_name.rpm
snmp_utility_package_name.rpm
```

For example:

```
rpm -Uvh net-snmp-5.0.6-6.rpm
net-snmp-utils-5.0.6-6.rpm
```

After installing the RPM packages, administrators should install OpenManage Server Agent on all managed nodes as follows:

1. Untar the DOMN32A00.tar file, which will extract the files within the tar file to the directory DOMN32A00:

```
tar -xvf DOMN32A00.tar
```

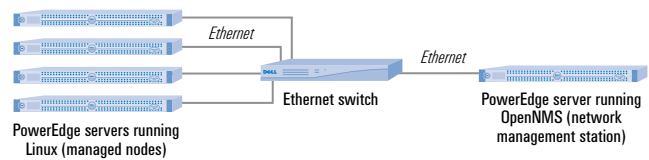


Figure 1. A network that has OpenNMS installed on the network management station

2. Change to the root of the untarred directory:

```
cd DOMN32A00
```

3. Use the following unattended installation script to install OpenManage Server Agent individually on all nodes:

```
./start_text.sh
```

Administrators can retrieve the OpenManage Server Agent version 1.2 tar file (DOMN32A00.tar) from <http://support.dell.com> and make the tar file available to all nodes to be managed. The OpenManage Server Agent unattended installation shell script, start\_text.sh, installs the necessary components to manage the PowerEdge server nodes. The OpenManage online documentation or documentation CD details the requirements necessary to install OpenManage Server Agent on a Red Hat Linux 7.3 system.

### Configuring SNMP and OpenManage Server Agent

After installing the OpenManage Server Agent, administrators must configure SNMP. To accomplish this task, they should edit the file /etc/snmp/snmp.conf by appending the following line, which allows SNMP to send all traps to the network management station:

```
trapsink 192.168.0.2 public
```

In the scenario in this article, 192.168.0.2 is the IP address of the Ethernet device located in the network management station and “public” is the SNMP community name that allows access rights to all SNMP management information base (MIB) data available on the system.

The snmpd and dellomsa services must be started to initiate SNMP traps so that the traps can be forwarded to the network management station:

- Restart the SNMP daemon:
 

```
service snmpd restart
```
- Restart the dellomsa daemon:
 

```
dellomsa restart
```

### Installing OpenNMS

OpenNMS includes a systems management Web console from which administrators can view hardware-generated traps sent by the

<b>Memory</b>	192 MB memory (256 MB suggested)
<b>CPU</b>	Intel® Pentium® III processor
<b>Free disk space</b>	15 MB in /opt 100 MB (minimum) in /var/log 8 MB per SNMP device
<b>Java Virtual Machine (JVM)</b>	Version 1.4 or greater

Figure 2. Minimum OpenNMS installation requirements

managed nodes. The basic requirements for a minimal OpenNMS installation are shown in Figure 2.

OpenNMS uses Java™ for Web-based console development. On the PowerEdge server that will be used as the network management station, administrators should install the Java 2 Software Development Kit (SDK) RPM, available from <http://java.sun.com>:

```
rpm -ivh j2sdk-1_4_0_01-fcs-linux-i386.rpm
```

If the Postgres database is already installed on the network management station, some additional steps are required for OpenNMS to install and function properly. These steps are documented in the installation guide at <http://www.opennms.org>. Otherwise, the installation steps use the Postgres RPM package that is available from the OpenNMS Web site.

A comprehensive list of the RPM packages required for a minimal OpenNMS installation are listed in Figure 3 and at <http://www.opennms.org>.

Administrators should install the packages on the network management station using the RPM utility:

```
rpm -ivh list of all RPM packages separated  
by space
```

Package name	Description
opennms-1.0.1-1.i386.rpm	OpenNMS base and Web interface
opennms-webapp-1.0.1-1.i386.rpm	Web applications for OpenNMS
perl-DBD-Pg-1.0.1-0.onms.1.i386.rpm	A PostgreSQL interface for Perl
perl-DBI-1.20-0.onms.1.i386.rpm	A database access application programming interface (API) for Perl
rrdtool-1.0.35-0.onms.1.i386.rpm	Round-robin database tool
readline41-4.1-10.i386.rpm	A library for editing command lines
tomcat4-4.0.3-0.onms.12.noarch.rpm	Tomcat, the Apache servlet engine
tomcat4-webapps-4.0.3-0.onms.12.noarch.rpm	Web applications for Tomcat
postgresql-server-7.1.3-0.onms.5.i386.rpm	Programs needed to create and run the PostgreSQL server
postgresql-7.1.3-0.onms.5.i386.rpm	The PostgreSQL client programs and libraries
postgresql-libs-7.1.3-0.onms.5.i386.rpm	The shared libraries required for PostgreSQL clients

Figure 3. RPM packages required for a minimal OpenNMS installation

For example:

```
rpm -ivh opennms-1.0.1-1.i386.rpm  
opennms-webapp-1.0.1-1.i386.rpm perl-DBD...
```

### Configuring OpenNMS by converting MIB traps to XML

After installation is complete, OpenNMS can be configured to receive information from SNMP clients on the network. Administrators should edit the `snmp-config.xml` file by adding an IP address range definition that includes addresses of machines to be managed for SNMP interaction. Figure 4 shows how the definition would look for the scenario in this article.

For events to be understood and correctly displayed for human readability by OpenNMS, MIB traps must be converted to Extensible Markup Language (XML) events using the `mib2opennms` program. This program uses a grammar based upon the Structure of Management Information (SMI) specification to convert traps into XML.

1. Install the latest `libsmi` RPM package, available from <http://rpmfind.net>:

```
rpm -ivh libsmi-0.2.16-1.i386.rpm
```

2. Build the `mib2opennms` program, which uses the `libsmi` libraries to perform the trap-to-XML event conversion:

```
cd /opt/OpenNMS/contrib/mib2opennms-0.2.2/  
sh configure  
make install
```

This procedure installs `mib2opennms` in the `/usr/local/bin` directory.

3. Use the `mib2opennms` program to convert the `10892.mib` file located in the extracted `DOMN32A00/dcpemibs/` directory to an XML file called `eventconf.txt`:

```
/usr/local/bin/mib2opennms -f  
/tmp/eventconf.txt 10892.mib
```

4. Using a text editor, insert the converted events of the `eventconf.txt` file, found at the beginning of the file, into the `eventd-configuration.xml` file after the “global” definition tag.

5. To identify all the newly created traps as “enterprise generic,” change the value of the `mevalue` tag from 0 to 6 in the `eventconf.txt` file. The `sed` command, as shown here, makes the changes globally and saves the modified file into a temporary file:

```
sed -e 's/<mevalue>0<\/mevalue>/  
<mevalue>6<\/mevalue>/' /tmp/eventconf.xml >  
/tmp/eventconf.xml.tmp
```

```
<definition version="v1">
  <range begin="192.168.0.1" end="192.168.0.254"/>
</definition>
```

Figure 4. IP address range definition for OpenNMS SNMP clients

- After checking the temporary file to verify that the changes were made, rename the temporary file as the eventconf.xml file:

```
mv -f /tmp/eventconf.xml.tmp eventconf.xml
```

After completing the last step in this procedure, the MIB traps are converted to XML. Administrators should start the OpenNMS and Tomcat services, which must be initiated before attempting to log onto the OpenNMS Web console:

```
/sbin/service opennms start
/sbin/service tomcat4 start
```

To log onto the OpenNMS Web console in the scenario in this article, administrators would access the URL <http://192.168.0.2:8080/opennms> from any browser and enter “admin” as the username and password.

### Understanding the enterprise systems management environment

After the completion of the procedures presented in this article, the OpenNMS console is ready to receive SNMP traps from all managed Red Hat Linux PowerEdge servers on the network.

Communication between the network management station and managed nodes involves hardware, OS-level drivers, and client software. If a hardware device located on a managed PowerEdge server fails or exceeds its threshold, the problem is detected by the Embedded Systems Management system. The Dell OpenManage Server Agent receives a notification through the Embedded Systems Management driver loaded on the Linux OS. The agent then forwards the notification to the NET-SNMP master agent. The master agent sends the trap over the network to the destination configured by the trapsink option in the `/etc/snmp/snmpd.conf` file. When a trap arrives to OpenNMS, it typically contains only information specific to that occurrence of the trap. At the network management station, traps are converted into events and then sent into the event subsystem (see Figure 5).

The event mask in `eventconf.xml` presents the relevant information for the traps and other similar events in an XML format, which can be viewed from a Web browser:

- From the OpenNMS Web console, click “Events” and then click “View all events”

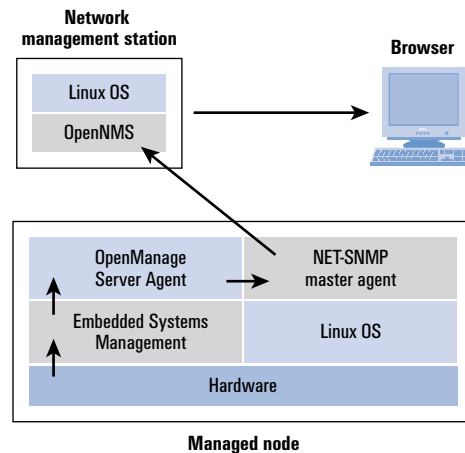



Figure 5. OpenNMS receives SNMP traps from managed PowerEdge servers on the network

- Click the first hardware-generated trap event to see a description of the event

### Integrating OpenNMS to efficiently manage Linux environments

Successfully integrating OpenNMS with Dell OpenManage Server Agent software to receive events from Dell PowerEdge servers empowers administrators to effectively manage hardware. In addition to providing information about network elements such as interfaces on switches and routers, OpenNMS also focuses on the services that network resources provide, such as Web pages, database access, Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP).

The way in which OpenNMS gathers data through the network and displays this data can be modified, and all of the OpenNMS management features are platform independent. Because OpenNMS is an open source project, all source code is available and experienced administrators can tailor the source code to the needs of any organization’s network. Therefore, OpenNMS allows network growth and design with minor systems management implications. When used together, OpenNMS and OpenManage Server Agent provide a powerful enterprise systems management solution that allows IT departments the flexibility to tailor future network and systems infrastructure development. 

**Joshua Giles** ([joshua\\_giles@dell.com](mailto:joshua_giles@dell.com)) is a Linux Systems Management Software Engineer. His interests include operating systems, Grammar- and Automata-based programming, and SVM (machine learning). Joshua has a B.S. from the New Mexico Institute of Mining and Technology.