Novell Sentinel Log Manager 1.1 Appliance Quick Start Guide

December, 2010

Novell

Getting Started

The Novell Sentinel Log Manager appliance is a ready-to-run software appliance that combines a SUSE Linux Enterprise Server (SLES) 11 operating system and Novell Sentinel Log Manager software with an update service. This appliance offers an enhanced browser-based user interface that supports collection, storage, reporting, and searching of log data from a wide variety of devices, applications, and protocols.

The Sentinel Log Manager 1.1 appliance is available in the following formats:

- A VMware appliance image
- A Xen appliance image
- A hardware appliance live DVD image that is deployable onto a hardware server

The Sentinel Log Manager is also available in a RPM-based installer, which can be installed on the existing SLES 11 system. For more information, see the *Sentinel Log Manager 1.1 Installation Guide* (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html).

The following section describes the procedure to install Sentinel Log Manager as a VMware appliance. For information on installing the Xen appliance, DVD ISO, or the standard installer (on an existing SLES system), see the Sentinel Log Manager 1.1 Installation Guide (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html).

System Requirements

- ❑ VMware ESX/ESXi 3.5/4.0 or higher (for a production environment)
- ❑ VMware Player 3 (for a demonstration environment)
- ❑ CPU: A minimum of two CPU cores (at least 2.5 GHz and 64-bit)
- ❑ RAM: A minimum of 2 GB
- ❑ Hard disk: A minimum of 52 GB

Prerequisites

- ❑ Make sure that the hardware and software satisfy the requirements of the VMware software being used. For more information, see the VMware Web site (http://www.vmware.com/support/).
- ❑ Make sure that you have the VMware Converter to simultaneously upload the image to the VMware ESX server and convert it to a format that can run on the ESX server.
- ❑ To run a 64-bit virtual machine within VMware, the processor of the host must support hardware virtualization. For more information on the supported Intel processors, see the VMware Knowledge Base site (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003944).

Installing the VMware Appliance

1. Establish an ESX datastore on which the appliance image can be installed.
2. Log in as Administrator.
3. Specify the following command to extract the compressed appliance image folder into the machine where the VMware converter is installed:

   ```
   tar zxvf <install_file>
   ```

4 To import the VMware image to the ESX server, use the VMware converter and follow the on-screen instructions in the installation wizard.

5 Log in to the ESX server machine.

6 Select the VMware image, then click *Power On*.

7 Select the language, then click *Next*.

8 Select the Keyboard Layout, then click *Next*.

9 Read and accept the SLES 11 License Agreement.

10 Read and accept the Novell Sentinel Log Manager End User License Agreement.

11 Specify the hostname and domain name.

Ensure that the *Write hostname to /etc/hosts* option is selected.

12 Click *Next*.

13 Do one of the following:

- To use the current network connection settings, select *Use the following configuration* in the *Network Configuration II* screen.
- To change the network connection settings, select *Change*.

14 Select *Next*. The network connection settings are saved.

15 Set the Time and Date, then click *Next*.

16 Set the `root` password, then click *Next*.

17 Set the Sentinel Log Manager admin password and dbauser password, then click *Next*.

18 Click *Finish*.

19 Proceed with "Post-Installation Setup" on page 2.

20 To register for updates, see the *Sentinel Log Manager 1.1 Installation Guide* (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html).

Post-Installation Setup

To log in to the appliance Web console and initialize the software:

1 Open a Web browser and log in to https://<*IP address*>:*8443*. The Sentinel Log Manager Web page is displayed.

Replace <*IP address*> with the IP address of the virtual appliance. This IP address is displayed on the appliance console when the installation is completed.

2 Configure the Sentinel Log Manager appliance for data storage and data collection. For more information about configuring the appliance, see the *Sentinel Log Manager 1.1 Administration Guide* (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/#index).

Testing the Installation

You can configure the Data Generator to create test events as follows:

1 Log in to the Sentinel Log Manager Web user interface.

2 Select *Collection* > *Advanced*, then click *Launch* to launch ESM.

3 To add a Generic Collector:

3a Right-click *Log Manager*, then select *Add Collector.*

3b Click *Generic* in the left pane of the Add Collector dialog box.

3c Select *Event Collector* in the right pane, then click *Next* in the three subsequent dialog boxes.

3d Select the *Run* check box, then click *Finish*.

4 To add a Data Generator Connector:

4a Right-click the Generic Event Collector, then select *Add Connector*.

4b Select *Data Generator*, then click *Next*.

4c Select the *Run* check box, then click *Finish*.

5 To add a Data Generator Event Source:

5a Right-click the Data Generator Connector, then select *Add Event Source*.

5b Set the desired *Records Per Second*, then click *Next*.

5c Select the *Run* check box, then click Next.

5d Click *Finish*.

6 Right-click the Generic Event Collector, the Data Generator Connector, or the Data Generator Event Source, then select *Open Raw Data Tap* to verify that events are being created.

You can perform searches or run reports with the test events.

Collecting Data from Devices

Sentinel Log Manager is installed with a variety of plug-ins, including Connectors to connect to many devices and Collectors to parse and normalize data.

- "Automatic Data Collection Configuration" on page 3
- "Manual Data Collection Configuration" on page 3

Automatic Data Collection Configuration

Devices that work with Syslog or the Novell Audit Connector are enabled for automatic data collection after the devices are configured to send data to Sentinel Log Manager.

Manual Data Collection Configuration

For devices that do not work with Syslog or Novell Audit Connector, you can manually configure data collection by using the included plug-ins or additional plug-ins downloaded from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).

To manually configure the Collectors and Connectors:

1. Follow the instructions in the Collector documentation to configure the source device.
2. Log in to the Novell Sentinel Log Manager Web interface, then click the *Collection* tab.
3. Select the *Advanced* tab, then click *Launch* to launch Event Source Management.
4. Follow the instructions in the *Sentinel Log Manager 1.1 Administration Guide* (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/#index) to complete the configuration.

Additional Documentation

For more information on Sentinel Log Manager installation, see the Sentinel Log Manager 1.1 Installation Guide (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html).