NetIQ Sentinel 7.0.1 Quick Start Guide

April 2012

Getting Started

Use the following information to get Sentinel installed and running quickly.

- "Meeting System Requirements" on page 1
- "Installing Sentinel" on page 1
- "Accessing the Sentinel Web Interface" on page 2
- "Collecting Data" on page 3
- "What's Next" on page 5

Meeting System Requirements

Verify that you meet the minimum system requirements to install Sentinel.

Hardware requirements for 500 EPS:

- **Memory:** 6.7 GB
- **Hard Disk:** 4 x 500 GB, 7.2K RPM drivers running on RAID 1 with 256 MB cache or an equivalent storage network area (SAN)
- **Processors:** One Intel Xeon X5470 3.33 GHz (4 core) CPU

Operating systems:

- SUSE Linux Enterprise Server (SLES) 11 SP1
- Red Hat Enterprise Linux (RHEL) 6

Virtual Machines:

- VMWare ESX 4.0
- Xen 4.0
- Hyper-V Server 2008 R2DVD ISO file only

DVD ISO:

- Hyper-V Server 2008 R2
- Hardware without an operating system installed

For hardware requirements if the EPS is above or below 500 EPS, see "Meeting System Requirements" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

Installing Sentinel

You can install Sentinel either as a stand-alone install or as an appliance install.

- "Installing on Hardware" on page 1
- "installing the Appliance" on page 2

Installing on Hardware

The standard installation of Sentinel installs all of the Sentinel components on one machine. If you want to perform a custom installation or install Sentinel as a user other than `root`, see "Installing Sentinel" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

To install Sentinel:

1 Download the Sentinel installation file from the Novell Downloads Web page (http://download.novell.com/index.jsp):

  1a In the *Product or Technology* field, browse to and select *SIEM-Sentinel*.

  1b Click *Search*.

  1c Click the button in the *Download* column for *Sentinel 7.0 Evaluation*.

  1d Click *proceed to download*, then specify your customer name and password.

  1e Click *download* for the installation version for your platform.

2 Use the following command to extract the installation file:

```
tar xfz <install_filename>
```

Replace <*install_filename*> with the actual name of the install file.

3. Use the following command to run the `install-sentinel` script:

   ```
   ./install-sentinel
   ```

4. Specify the number for the desired language to perform the installation, then press Enter.

   The default value is 3 for English.

   The end user license agreement is displayed in the selected language.

5. Press the Spacebar to read through the license agreement.
6. Enter `yes` or `y` to accept the license and continue with the installation.

   This installation might take a few minutes to finish.

7. When you are prompted, enter 1 to proceed with the standard installation of Sentinel 7.0.
8. Specify a password twice for the default admin account that is created during the configuration.

For detailed information, see "Installing Sentinel" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

Installing the Appliance

The appliance is available for VMware ESX, Xen, and Hyper-V virtual platforms. You can also install the appliance on hardware. The following instructions are for the VMware ESX server. For instructions on the other platforms, see "Installing the Appliance" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

1. Download the VMware appliance installation file.

   The correct file for the VMware appliance has `vmx` in the filename.

2. Establish an ESX datastore to which the appliance image can be installed.
3. Log in as Administrator to the server where you want to install the appliance.
4. Use the following command to extract the compressed appliance image from the machine where the VM Converter is installed:

   ```
   tar zxvf <install_file>
   ```

   Replace <*install_file*> with the actual filename.

5. To import the VMware image to the ESX server, use the VMware Converter and follow the on-screen instructions in the installation wizard.
6. Log in to the ESX server machine.
7. Select the imported VMware image of the appliance and click the *Power On* icon.
8. Select the language of your choice, then click *Next*.
9. Select the keyboard layout, then click *Next*.
10. Read and accept the Novell SUSE Linux Enterprise Server software license agreement.
11. Read and accept the NetIQ Sentinel end user license agreement.
12. In the Hostname and Domain Name screen, specify the hostname and domain name.
13. Ensure that the *Assign Hostname to Loopback IP* option is selected.
14. Select *Next*. The hostname configurations are saved.
15. 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*, then make the desired changes.
16. Click *Next* to save the network connection settings.
17. Set the time and date, click *Next*, then click *Finish*.

    To change the NTP configuration after installation, use YaST from the appliance command line. You can use WebYast to change the time and date, but not the NTP configuration.

    If the time appears out of sync immediately after the install, run the following command to restart NTP:

    ```
    rcntp restart
    ```

18. Set the Novell SUSE Linux Enterprise Server `root` password, then click *Next*.
19. Set the `root` password, then click *Next*.
20. Set the Sentinel admin password and dbauser password, then click *Next*.
21. Click *Next*. The network connection settings are saved.

    When the installation finishes, make a note of the appliance IP address that is shown in the console.

For post-installation configuration information, see "Post-Installation Configuration for the Appliance" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

Accessing the Sentinel Web Interface

After Sentinel is installed, the next step is to access the Sentinel Web interface to perform administration tasks and configure Sentinel to collect data.

To access the Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443
```

The 8443 port is the default value.

Collecting Data

Data collection occurs through the Connectors and Collectors. By default, Sentinel has some Connectors and Collectors installed and configured.

By default, there are TCP, UDP, and SSL syslog servers installed on the Sentinel server. If you are using the appliance, the syslog servers are automatically configured when they start receiving events from the local syslog file.

You can configure syslog devices, such as a Linux server, to send information to these syslog servers. Also, you can configure additional Connectors to allow Sentinel to collect data.

- "Configuring A Linux Server to Send Syslog Information to Sentinel" on page 3
- "Configuring Data Collection for Windows" on page 3
- "Configuring Additional Connectors and Collectors" on page 5

Configuring A Linux Server to Send Syslog Information to Sentinel

The Sentinel server contains a preconfigured syslog event source server that is listening for any incoming connections to these ports:

- **TCP:** 1468
- **UDP:** 1514
- **SSL:** 1443

Use the following information to configure a Linux server to send events to the TCP syslog event source server.

To configure the syslog file on Linux:

1. Open the `/etc/syslog-ng/syslog-ng.conf` file.
2. Add the following lines of code to the bottom of the `syslog-ng.conf` file.

   ```
   # Forward all messages to Sentinel:
   #
   destination d_slm { tcp("127.0.0.1"
   port(1468)); };
   log { source(src); destination(d_slm); };
   ```

3. Change the TCP value to the IP address of the Linux server.
4. Save the file and close the file.
5. Restart the syslog service:

   ```
   /etc/init.d/syslog restart
   ```

For details about how to configure devices to send information to the Syslog Connector, see the Syslog Connector documentation located on the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Configuring Data Collection for Windows

If you have a Windows system you want to collect data from, you must configure a Windows Event (WMI) Connector. The Windows Event Connector is installed on the Collector Manager and receives events from the Windows Event Collection Service that is installed on the Windows server.

- "Configuring the Windows Event Connector" on page 3
- "Installing the Windows Event Collection Service on the Windows Server" on page 4
- "Configuring the Windows Event Collection Service" on page 5

Configuring the Windows Event Connector

1. Log into the Sentinel Web interface.

`https://<IP_Address_Sentinel_server>:8443`

   The 8443 port is the default port.

2. Click *Applications* in the toolbar, then click *Launch Control Center*.
3. Log in to the Sentinel Control Center with the administrative username and password, then click *Login*.
4. From the toolbar, click *Event Source Management* > *Live View*.
5. Add a Windows-specific Collector to the Collector Manager.

   You must have a Windows-specific Collector configured before you can add the Windows Event Connector.

   5a Right-click the Collector Manager, then click *Add Collector*.

   5b Select *Microsoft* in the *Vendor* column, then select your version of Windows or Active Directory in the *Version* column.

   5c Click *Next*.

   5d Select the scripts you want to view, then click *Next*.

   5e Change any of the configuration parameters, then click *Next*.

   5f Set additional configuration parameters for the Collector, then click *Finish*.

6. Add the Windows Event Connector to the Collector you created in Step 5:

   6a Right-click the Collector, then click *Add Connector*.

   6b Select the Windows Event Connector, then click *Next*.

   6c Configure the network settings for the Windows Event Connector server, then click *Next*.

6d Configure the SSL settings, then click *Next*.

6e Select how the Windows Event Connector is managed:

- **Manually:** Select this option to manually manage the event source.
- **Automatically:** Select this option to automatically synchronize with Active Directory.

6f Click *Next*.

6g Specify the user's credentials that are used to connect to the Windows Event Collection Service and to connect to the event source.

6h Specify the configuration parameters, then click *Finish*.

7 Add an event source for the Windows systems where you want to collect data.

7a Right-click the Windows Event Connector, then click *Add Event Source*.

7b Specify the IP address or hostname of the Windows system

or

Select a Windows system from Active Directory, then click *Next*.

7c Select a connection mode for the event source, then click *Next*.

7d Specify the configuration parameters for the event source, then click *Finish*.

Installing the Windows Event Collection Service on the Windows Server

1 Verify that you have created a user account on the Windows server with the appropriate rights to run the Windows Event Collection Service and collect events from the Windows Event logs of the remote Windows systems. The rights are:

- Permission to access the Windows Event logs
- WMI permissions
- DOCM permissions
- Read, write, and delete ACL rights must be assigned to the Distributed COM Users group for all event log types.
- Read permission to the security event log
- User must have administrative privileges to install the Windows Agent
- User must have the *Log on as a service* right.

For more information, see the Windows Event Connector documentation on the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). The permissions information is located in Chapters 4 and 5.

2 Copy the `WindowsEvent-CollectionService.msi` file from the Windows Event Connector `.zip` file to the Windows server where you want to install the Windows Event Collection Service.

3 Double-click the `WindowsEvent-CollectionService.msi` file to launch the Windows Event Collection Service Setup Wizard.

4 On the Welcome screen, click *Next*.

5 (Conditional) Read the support limitation warning, then click *Next*.

6 Accept the end user license, then click *Next*.

7 Use the following information to customize the configuration of the Windows Event Collection Service:

Additional Features: Select the features you want to install. Not all of the features are installed by default. The features are:

- **Collection Service:** Installs the Windows Event Collection Service that communicates to Sentinel.
- **Documentation:** Installs the documentation that ships with the Connector.

Location: (Optional) Change the default installation location by clicking *Browse* and selecting a new location. The default installation location is installed under `Program Files\Novell\SentinelWECS`.

Disk Usage: (Optional) Click *Disk Usage* to determine if there is enough diskspace available to install the Windows Event Collection Service.

8 Click *Next*.

9 Define the service account the Windows Event Collection Service uses to connect to external Windows event sources.

Local System Account: Select this option to run the Windows Event Collection Service as a Local System Account user. If you select this option, you need to specify the user credentials while deploying the Windows Event Connector on the Collector Manager.

This Account name: Select this option to run the Windows Event Collection Service as specific user or domain user. Use the credentials of the user that has the rights to run the Windows Event Collection Service.

The Windows Event Collection Service system must have access to read the Windows event log on each event source system to be monitored. Therefore, the users that are created should have appropriate permissions assigned on each event source system.

Start the service once installed: Select this option if you want the Windows Event Collection Service started as soon as the installation finishes.

10 Click *Next*.

11 Click *Install* to install the Windows Event Collection Service.

12 Click *Finish* to exit the configuration wizard.

After the Windows Event Collection Service is installed, it must be configured to work.

Configuring the Windows Event Collection Service

1 Open the `eventManagement.config` file using a file editor.

The default location of the file is in `Program Files\Novell\SentinelWECS`.

2 In the `<client>` section, copy the `endPoint address` line and paste it below the existing line. Replace the existing IP address with the IP address of the server (Collector Manager) where the Windows Event Collection Service connects and the port number through which it communicates with the Connector.

For example:

```
<client>
   <!-- Additional collectors/plugins can be
added with different host/
port configurations -->
    <!-- <endPoint address="tcp://
127.0.0.1:1024"
behaviorConfiguration="localhost" />-->
    <endPoint address="tcp://
<IP_address_Sentinel_server:<port_number>"
behaviorConfiguration="localhost" />-->
  </client>
```

3 You can configure as many Connectors you want by repeating Step 2. You can configure one agent to multiple connectors or one agent to one Connector.

4 Save and close the `eventManagement.config` file.

5 Open the Service window to start the Windows Event Collection Service.

5a Click *Start* > *Run* to open the Run dialog box.

5b Type `services.msc` and click *OK*.

6 Select *Sentinel Windows Event Connection Service*, then right-click and select *Start* to start the Windows Event Collection Service.

7 Close the Service window.

For more information about the Microsoft Active Directory and Windows Collector and the Window Event (WMI) Connector, see the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Configuring Additional Connectors and Collectors

The available Connectors and Collectors are installed on your Sentinel server during the Sentinel installation. However, new and updated Connectors and Collectors are often available.

Check the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) for updated versions of the Connectors and Collectors.

If you need to configure a Connector or Collector that is not configured by default, see "Adding Additional Sentinel Components" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

What's Next

At this point, Sentinel is installed. There are two guides to help you configure Sentinel: the *NetIQ Sentinel 7.0.1 Administration Guide* and the *NetIQ Sentinel 7.0.1 User Guide*.

The Administration Guide contains configuration information for tasks only a user with administration rights can perform. For example:

- "Configuring Users and Roles"
- "Configuring Data Storage"
- "Configuring Data Collection"
- "Searching and Reporting Events in a Distributed Environment"

For more information on these and other administration tasks, see the *NetIQ Sentinel 7.0.1 Administration Guide*.

The User Guide contains instructions for users to perform tasks in Sentinel. For example:

- "Searching Events"
- "Analyzing Trends in Data"
- "Reporting"
- "Configuring Incidents"

For more information on these and other user tasks, see the *NetIQ Sentinel 7.0.1 User Guide*.

You can configure Sentinel to analyze your events, add data using correlation rules, set up baselines, configure workflows to act on the information, and more. Use the information in the *NetIQ Sentinel 7.0.1 Administration Guide* to help you configure these Sentinel features.

Legal Notices: NetIQ Corporation ("NetIQ") makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, NetIQ reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

NetIQ makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, NetIQ reserves the right to make changes to any and all parts of the software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. NetIQ assumes no responsibility for your failure to obtain any necessary export approvals.

For more information, please contact, NetIQ at:

1233 West Loop South, Houston, Texas 77027

U.S.A.

www.netiq.com

.