NetIQ Sentinel Log Manager 1.2.2 Readme

July 2014

Sentinel Log Manager collects data from a wide variety of devices and applications, including intrusion detection systems, firewalls, operating systems, routers, Web servers, databases, switches, mainframes, and antivirus event sources. Sentinel Log Manager provides high event rate processing, long-term data retention, regional data aggregation, and simple searching and reporting functionality for a broad range of applications and devices.

Sentinel Log Manager 1.2.2 provides several enhancements and resolves specific previous issues. This document outlines why you should install this service pack.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable inputs. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the Sentinel Community Support Forums, our community Web site that also includes product notifications, blogs, and product user groups.

1 What's New?

The following sections outline the enhancements provided and the issues resolved in this service pack:

1.1 Latest Plug-ins

The upgrade installation of Sentinel Log Manager 1.2.2 updates the Syslog Integrator to version 2011.1r1, which includes significant performance improvements.

1.2 Enhancements

This service pack includes the following enhancements:

1.2.1 Performance Improvements

This service pack improves the Sentinel Log Manager system performance in the areas of Searching and Reporting.

1.2.2 Limitations to Support Collector Pack Reports

Sentinel Log Manager no longer includes the Collector Packs for Collector plug-ins. The Collector pack reports included hard-coded device-specific filters, which had limited options to customize these reports. These reports are now labeled as deprecated in Sentinel Log Manager. Instead, you can use similar reports available in the Sentinel Core Solution Pack, which allows you to use a base report with a wide range of user specified filters at run-time, including the device-specific filters. For more information about Sentinel Core Solution Pack, see the Solution Pack documentation on the Sentinel Plug-ins Web site.

1.2.3 Java 7 Upgrade

Sentinel Log Manager 1.2.2 now includes the Java 7 update 55, which includes fixes for several security vulnerabilities. Also, Sentinel Log Manager 1.2.2 supports client computers installed with Java 7 update 55.

1.3 Software Fixes

Sentinel Log Manager 1.2.2 provides software fixes for the following issues:

1.3.1 Event Source Management Does Not Launch on Java 7 Update 45

Issue: Event Source Management (ESM) does not launch on client computers that have Java 7 Update 45 installed. `(BUG 847156)`

Fix: ESM now launches on client computers that have Java 7 Update 45 installed.

1.3.2 Sentinel Log Manager Deletes the License Key When the Disk Space is Full

Issue: When the disk space is full, Sentinel Log Manager deletes the license key. Users are unable to log in to the Web console. `(BUG 821015)`

Fix: Sentinel Log Manager no longer deletes the license key when the disk space is full.

1.3.3 Sentinel Log Manager Displays a Java Exception When You Export Query Results

Issue: Sentinel Log Manager displays the Java exception `java.io.FileNotFoundException` while exporting query results. `(BUG 834486)`

Fix: Sentinel Log Manager now exports the query results successfully and no longer displays an exception.

[Return to Top]

2 System Requirements

You can upgrade to Sentinel Log Manager 1.2.2 from Sentinel Log Manager 1.2 or later.

Sentinel Log Manager 1.2.2 requires the SUSE Linux Enterprise Server 11 Service Pack 3 (64-bit). Therefore, you must first ensure that the operating system is upgraded to SLES 11 Service Pack 3 before you upgrade to Sentinel Log Manager 1.2.2.

For more information about system requirements, see "System Requirements" (http://www.novell.com/documentation/novelllogmanager12/log_manager_install/data/bjx8zq7.html) in the *Sentinel Log Manager 1.2 Installation Guide*.

[Return to Top]

3 Upgrading to Sentinel Log Manager 1.2.2

To upgrade to Sentinel Log Manager 1.2.2, see "Upgrading Sentinel Log Manager" (http://www.netiq.com/documentation/novelllogmanager12/log_manager_install/data/bp52vsc.html) in the Sentinel Log Manager 1.2.2 Installation Guide. After performing the upgrade procedure, restart the Sentinel Log Manager server to apply updates for SLES 11 Service Pack 3.

IMPORTANT: If you are upgrading Sentinel Log Manager appliance on an operating system prior to SLES 11 SP3, you must upgrade the appliance by using the zypper command line utility because user interaction is required to complete the upgrade. WebYaST is not capable of facilitating the required user interaction. For information about using zypper to upgrade the appliance, see "Upgrading the Appliance by Using zypper" in the Sentinel Log Manager 1.2.2 Installation Guide.

[Return to Top]

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

For the list of known issues in the supported SLES 11 Service Pack, see the SUSE Release Notes.

For the list of known issues in previous releases, see the Sentinel Log Manager 1.2.1 Documentation Web site.

4.1 Sentinel Log Manager Overwrites the Specified IP Address in the Configuration File After Restart

Issue: If there are multiple IP addresses available, Sentinel Log Manager selects one of the IP addresses as default. If you manually change the default IP address in the `configuration.xml` file, after restart, Sentinel Log Manager reverts it to the default IP address. `(BUG 848148)`

Workaround: To set the default IP address:

1. Create the `/etc/opt/novell/sentinel_log_mgr/config/start_tomcat.properties` file.
2. Add the following parameter in the `start_tomcat.properties` file:

   `SERVER_IP=` *`IP_address`*

3. Restart the Sentinel Log Manager.

4.2 Sentinel Log Manager Web Console Does Not Launch on Internet Explorer 9 and 10

Issue: Sentinel Log Manager Web console does not launch successfully in Internet Explorer version 9 and 10 and displays as blank. `(BUG 785504)`

Workaround: To launch the Sentinel Log Manager Web console on Internet Explorer version 9 and 10:

1. In the Internet Explorer, Press F12 to view the Developer tools.
2. Click **Document Mode**.
3. Select **Internet Explorer 8 standards**.

4.3 Sentinel Log Manager Does Not Allow Events From Applications That Use Weak Encryption Keys

Issue: Sentinel Log Manager does not connect to applications that use encryption keys of size less than 1024 bytes. Sentinel Log Manager rejects the connection to such applications and displays an exception. For more information about this issue, see TID 7014219 in the NetIQ Support Knowledge Base. (BUG 853895)

Workaround: Perform either of the following to allow applications that use weak encryption keys to connect with Sentinel Log Manager:

- (Recommended) Update the application certificate to use encryption keys of size 1024 bytes or more.
- In the `java.security` file, delete the following restriction:

  ```
  RSA keySize < 1024
  ```

  NOTE: Ensure that you perform this workaround after every upgrade of Sentinel Log Manager because the new installation replaces the modified `java.security` file.

4.4 Sentinel Log Manager 1.2.2 Does Not Include the Remote Collector Manager 1.2.2 Fresh Installer

Issue: Sentinel Log Manager 1.2.2 includes only the remote Collector Manager 1.2.2 upgrade installer. (BUG 854442)

Workaround: To install the remote Collector Manager 1.2.2:

1. (Conditional) If you have remote Collector Manager 1.2.1 installed, download the remote Collector Manager 1.2.2 upgrade installer from the Sentinel Log Manager Web console and upgrade to version 1.2.2.
2. (Conditional) If you do not have remote Collector Manager 1.2.1 installed, perform the following steps:
   - **2a** Download and install remote Collector Manager 1.2.1 from the Sentinel Log Manager Web console.
   - **2b** Download the remote Collector Manager 1.2.2 upgrade installer from the Sentinel Log Manager Web console and upgrade to version 1.2.2.

4.5 Sentinel Log Manager Logs Errors While Installing Solution Packs

Issue: When you install solution packs in Sentinel Log Manager, Sentinel Log Manager logs the `nullpointer` exception and the `PSQL` exception in the server logs. (BUG 852813)

Workaround: Ignore the exceptions. The logged exceptions do not impact the installation of the solution packs or any functionality in Sentinel Log Manager.

4.6 Remote Collector Manager Displays an Error While Upgrading to Version 1.2.2 If You Reject the License Agreement in a Previous Attempt

Issue: If you reject the license agreement while upgrading the remote collector manager from version 1.2.1 to 1.2.2. The subsequent attempts to upgrade remote collector manager do not work and display an error. (BUG 885375)

Workaround: To upgrade remote collector manager to version 1.2.2 successfully, delete the `/opt/novell/sentinel6/.version_history_bak_1.2.2.0` file.

4.7 When You Uninstall Remote Collector Manager 1.2.2, Windows Computer Displays an Error

Issue: In a Windows computer, when you uninstall remote collector manager version 1.2.2 by using the control panel, the computer displays the error "No Java Runtime Environment (JRE) was found on this system". (BUG 885373)

Workaround: In the error message dialog box, click **OK**. Browse to the `JRE/bin/` folder in the remote collector manager installation folder, and select `java.exe`. The uninstall process completes successfully.

4.8 Remote Collector Manager 1.2.2 Service Cannot be Found After Upgrading the Operating System

Issue: In a Linux machine, after you upgrade Suse Linux Enterprise Server 11 SP2 to SP3, remote collector manager 1.2.2 service cannot be found. (BUG 881461)

Workaround: To ensure the remote collector manager 1.2.2 service works properly:

1. In the console, log in as a `root` user.
2. Navigate to the `/etc` directory and copy the modified profile file (`profile.rpmsave`) to the profile file (`profile`).

   ```
   cd /etc

   cp profile.rpmsave profile
   ```

3. Navigate to the folder where you installed the remote collector manager, back up the configuration.properties file, and copy the modified configuration.properties (`configuration.000`) file to the configuration.properties file. For example:

   ```
   cd /opt/novell/sentinel6/config

   mv configuration.properties configuration.properties_bkp

   mv configuration.000 configuration.properties
   ```

4. Navigate to the `bin` folder in the remote collector manager installation folder, back up the setenv.sh file, and copy the modified setenv.sh file (`setenv.000`) to setenv.sh file

   ```
   cd /opt/novell/sentinel6/bin

   mv setenv.sh setenv.sh_bkp

   mv setenv.000 setenv.sh
   ```

5 (Conditional) If the user ownership while copying the files is not set to `esecadm:esec`, change the user ownership to `esecadm:esec`:

```
chown esecadm:esec  /opt/novell/sentinel6/config/configuration.properties

chown esecadm:esec  /opt/novell/sentinel6/bin/setenv.sh
```

6 Start Sentinel by using the following command:

```
/etc/init.d/sentinel start
```

7 To verify the Sentinel status, execute the following command:

```
/etc/init.d/sentinel status
```

[Return to Top]

5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information Web site.

For general corporate and product information, see the NetIQ Corporate Web site.

For interactive conversations with your peers and NetIQ experts, become an active member of Qmunity, our community Web site that offers product forums, product notifications, blogs, and product user groups.

[Return to Top]

6 Legal Notice

[Return to Top]