Sentinel 8.0 Release Notes

November 2016

Sentinel 8.0 includes new features, improves usability, and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Sentinel forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click the comment icon on any page in the HTML version of the documentation posted at the Sentinel NetIQ Documentation page. To download this product, see the Sentinel Product Upgrade website.

For the latest version of this release notes, see *Sentinel 8.0 Release Notes*.

1 What’s New?

The following sections outline the key features and enhancements, and also the issues resolved in this release:

1.1 Hadoop-Based Scalable Storage and Event Visualization

You can now configure Sentinel with Cloudera's Distribution Including Apache Hadoop (CDH) framework to store and manage large data. Hadoop-based scalable storage provides you with the ability to seamlessly scale up data collection and visualization to a large EPS with a single Sentinel server. You can horizontally scale the scalable storage system to meet the needs of your environment.

Sentinel with scalable storage is referred to as **Sentinel Scalable Data Manager (SSDM)**. The SSDM version of Sentinel provides powerful and customizable event visualization dashboards that help you to search, view, and analyze events in detail. You can combine SSDM and Sentinel with traditional storage in a tiered system to perform more advanced analytical functions such as alerting, correlation, and anomaly detection.

Scalable storage is optional. Depending on the EPS load, you can choose to use scalable storage or traditional storage. For more information about scalable storage, see "Data Storage Considerations" in the *NetIQ Sentinel Installation and Configuration Guide*.

NOTE: Scalable storage configuration is available only in new installations of Sentinel. To use this feature, you must apply an updated license key that is available through the Customer Care Portal or from NetIQ Support.

1.2 Sentinel Main Interface

The Sentinel web console is now referred to as the Sentinel Main interface.

1.3 Threat Response Dashboard

Sentinel 8.0 introduces the Threat Response Dashboard, which provides an overview of your current workload by breaking down alerts in groups, such as status, assignment, and priority. With the alerts grouped in this way, you can focus on and triage the high priority alerts assigned to you before triaging other alerts.

For users in the Operator role, the Threat Response Dashboard is the main user interface for viewing and triaging alerts. Any user with permission to manage alerts can also use the Threat Response Dashboard. Users who wish to use alert views in the Sentinel Main interface can click Sentinel Main in the left side navigation.

1.4 Updates to Certified Platforms

There are several updates to the Sentinel certified platforms:

1.4.1 New Certified Platforms

Sentinel is now certified on the following platforms:

Traditional installation:

- SUSE Linux Enterprise Server 12 SP1 64-bit
- Red Hat Enterprise Linux Server 7.2 64-bit

Appliance installation: VMware ESX 6.0 (for both ISO and OVF)

Event Source: Security Agent for UNIX 7.5

Web Browser: Microsoft Edge

1.4.2 Deprecated Platforms

Sentinel deprecates the following platforms:

Traditional Installation:

- SUSE Linux Enterprise Server 11 SP3 64-bit
- Red Hat Enterprise Linux Server 6.6 64-bit

Appliance Installation: Citrix XenServer 6.5 (for both ISO and OVF)

Web Browser: Microsoft Internet Explorer 10

Data Synchronization: Microsoft SQL Server 2005

For more information about the certified platforms, see the Technical Information for Sentinel page.

1.5 Deprecation of Active Views

Sentinel deprecates Active Views in Sentinel Control Center so that you no longer need to switch to multiple user interfaces to view events in real time. You can use the Real-time Event Views in the Sentinel Main interface, which provides advanced options to view the events in real time.

For more information, see "Viewing Events in Real-Time" in the *NetIQ Sentinel User Guide*.

1.6 TenantID Event Field

Sentinel now includes a new event field named **TenantID (tid)** that generates a unique ID for each tenant. This unique ID remains the same even if the TenantName changes. You can now use the **tid** event field to search events for a specific tenant. SSDM segregates events and raw data tenant-wise, based on the tid field.

1.7 Enhancements

Sentinel 8.0 includes the following enhancements:

1.7.1 Support of Higher TLS Versions for Enhanced Secure Communication

Some Sentinel components allow TLSv1.0 for communication. To improve the security posture and to prevent known vulnerabilities, you can now disable TLSv1.0 so that Sentinel can use a higher version of TLS such as TLSv1.1 and TLSv1.2. For more information, see "Enabling Higher Versions of TLS for Communication" in the *NetIQ Sentinel Administration Guide*.

1.7.2 Lengthening of the Message Event Field

The Message (msg) event field size is now increased from 4000 to 8000 characters. If you created a data synchronization policy in a previous version of Sentinel that synchronizes the Message (msg) event field to an external database, you need to modify the target column size in the external database table to reflect the increased size of the field. For more information about data synchronization, see "Configuring Data Synchronization" in the *NetIQ Sentinel Administration Guide*.

1.7.3 Enhancement to Collector Manager and Correlation Engine Installation Permissions

Any user in the Administrator role can now install Collector Manager and Correlation Engine.

Previously, only the admin user had permissions to install Collector Manager and Correlation Engine. This meant that the person installing Collector Manager and Correlation Engine had to be given access to the admin user credentials, which could lead to nonobservance of security practices of the organization. Now you can use the credentials of any user in the Administrator role to install Collector Manager and Correlation Engine. (Bug 982716)

1.7.4 Modifications to Default User Role Permissions

Sentinel 8.0 modifies the default permissions for the User role to reflect best practices based on the principle of least privilege. The modified User role does not have the “Modify incidents” permission. To avoid disrupting existing environments, the modified permissions do not apply to upgrades. If you are upgrading to Sentinel 8.0, NetIQ encourages you to manually modify the permissions for the User role. For more information, see “Configuring Roles and Users” in the *NetIQ Sentinel Administration Guide*.

1.7.5 New Directory for Sentinel Temporary Files

To help you more easily manage the temporary data Sentinel generates, Sentinel 8.0 adds the following directory for Sentinel temporary files:

`/var/opt/novell/sentinel/tmp`

The existing `/tmp` directory now only contains operating system temporary files.

1.7.6 Java Runtime Environment Upgrade

Sentinel 8.0 includes Java 8 update102, which includes fixes for several security vulnerabilities.

1.8 Software Fixes

Sentinel 8.0 includes software fixes that resolve several issues.

1.8.1 Sentinel Does Not Clean Up the Event Associations Data

Issue: Sentinel does not clean up the event associations data in the exported associations directory. As a result, the directory increases in size and might cause performance issues. (Bug 891686)

Fix: Sentinel now retains the event associations data present in the exported associations directory for 14 days by default. However, you can change this retention period. For more information about configuring the retention period for event associations data, see “Configuring the Retention Period for the Event Associations Data” in the *NetIQ Sentinel Administration Guide*.

1.8.2 Collector Instance Uses a Single CPU Thread to Process Data

Issue: Collector instances use a single CPU thread to process data. As a result, a large amount of data from event sources can overwhelm the collector, even if there are unused CPU resources on the computer. (Bug 908321)

Fix: You can configure a collector instance to use multiple threads. This enhancement allows the collector to process a higher number of events per second.

To configure the number of threads, in the Edit Collector dialog box, click the Configure Collector tab. Set **Number of Threads** to the number of threads you want to use. For more information, see "Connecting to Event Sources" in *NetIQ Sentinel Administration Guide*.

NOTE: This change does not affect event sources that require multiple messages to parse a single event.

1.8.3 Conversion to FIPS Mode Fails If 32-bit and 64-bit NSS RPMs are Present

Issue: When you convert Sentinel to FIPS mode, if the 32- and 64-bit RPMs for NSS are both on the computer, the conversion process fails. An error message incorrectly states that the process could not find one or more of the required 64-bit NSS packages. (Bug 978639)

Fix: The conversion process now correctly recognizes the 64-bit NSS RPMs.

1.8.4 Synchronization Needs to be Started Manually in Sentinel High Availability When You Modify Configuration Files in the Active Node

Issue: In Sentinel High Availability (HA), when you customize Sentinel by updating configuration files or by making changes in the Sentinel Main interface in the active node, the changes are not reflected in the passive node. Synchronization needs to be started manually.

For example, you must start synchronization manually in the following scenarios:

- When you change the communication protocol to SSL, by updating the `/etc/opt/novell/sentinel/config/databasePlatforms.xml` file for the following property:

  ```
  ssl=require
  ```

- When Sentinel is in FIPS mode, the synchronization to convert all the passive nodes to FIPS mode is not performed completely. When failover occurs in such scenario, the Sentinel Main interface does not launch.
- When you change the LDAP configuration in the active node, it is not synchronized to the passive nodes. Because of this, you will not be able to authenticate LDAP accounts in the passive nodes.

(Bug 845850)

Fix: In Sentinel High Availability (HA), changes are now correctly reflected in the passive node when you customize Sentinel on the active node in one of the following ways:

- Update configuration files
- Make changes in the Sentinel Main interface

After you make the changes, run `csync2 -x -v` on the active node.

2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see the Technical Information for Sentinel page.

3 Installing Sentinel 8.0

For information about installing Sentinel 8.0, see the *NetIQ Sentinel Installation and Configuration Guide*.

4 Upgrading to Sentinel 8.0

To upgrade to Sentinel, you must download and install Sentinel 8.0.0.1 that includes fixes to previous issues during upgrade. For more information, see *Sentinel 8.0.0.1 Release Notes*.

5 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.

The Java 8 update included in Sentinel might impact the following plug-ins:

- Cisco SDEE Connector
- SAP (XAL) Connector
- Remedy Integrator

For any issues with these plug-ins, NetIQ will prioritize and fix the issues according to standard defect-handling policies. For more information about support polices, see Support Policies.

5.1 Errors in SSDM Event Visualization Dashboards and Searches After Installing Elasticsearch Security Plug-In

Issue: In an RPM based installation of Elasticsearch, Event Visualization dashboards and searches in SSDM do not work. (Bug 1014448)

Workaround: After installing the Elasticsearch Security plug-in, perform the following steps on each node of the Elasticsearch cluster:

1. Log in to the Elasticsearch node as the user which Elasticsearch is running as.
2. Grant the read permission to the Elasticsearch Security plug-in by adding the highlighted text in the `<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-security.policy` file as follows:

```
grant {
permission java.lang.RuntimePermission "getClassLoader";
permission java.lang.RuntimePermission "setFactory";
permission java.io.FilePermission "/usr/share/elasticsearch/-", "read";
};
```

3. Restart Elasticsearch.

5.2 SSDM in HA Mode Does Not Populate Elasticsearch Security Plug-In Configuration Files Properly

Issue: SSDM in high availability mode does not populate the appropriate IP addresses of the HA cluster nodes in the Elasticsearch security plug-in configuration files. As a result, searches and event visualization dashboards show errors.

Workaround: After installing the Elasticsearch security plug-in, perform the following steps on each node of the Elasticsearch cluster:

1. Log in to the Elasticsearch node as the user which Elasticsearch was installed as.
2. Add entries for the **physical IP address** of each active node and passive node of the HA cluster in the `<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt` file as follows:

   `<Cluster_Node_Physical_IP>:<Target_Elasticsearch_HTTP_Port>`

   Add each entry in a new line and save the file.
3. In the `<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-configuration.properties` file, set the `authServer.host` property to the **virtual IP address** of the HA cluster as follows:

   `authServer.host=<Cluster_Virtual_IP>`
4. Restart Elasticsearch.

5.3 Synchronization Needs to be Started Manually in Sentinel High Availability After You Convert the Active Node to FIPS 140-2 Mode

Issue: When you convert the active node to FIPS 140-2 mode in Sentinel HA, the synchronization to convert all the passive nodes to FIPS 140-2 mode is not performed completely. You must start the synchronization manually. `(Bug 1014472)`

Workaround: Manually synchronize all passive nodes to FIPS 140-2 mode as follows:

1. Log in as the root user on the active node.
2. Open the `/etc/csync2/csync2.cfg` file.
3. Change the following line:

```
include /etc/opt/novell/sentinel/3rdparty/nss/*;
```

to

```
include /etc/opt/novell/sentinel/3rdparty/nss;
```

4. Save the `csync2.cfg` file.
5. Start the synchronization manually by running the following command:

```
csync2 -x -v
```

5.4 Tile Map Visualizations Do Not Work in Sentinel Scalable Data Manager

Issue: In SSDM environments, if you create a tile map visualization with default options, an issue with Kibana prevents the new tile map visualization from working in the Event Visualization dashboard. For more information about the Kibana issue, see https://github.com/elastic/kibana/issues/7717. `(Bug 1001909)`

Workaround: When you create a new tile map visualization, under **Options**, select **WMS compliant map server**.

5.5 Cannot Launch Event Visualization Dashboard

Issue: An issue with Kibana prevents Internet Explorer 11 from being able to open the Event Visualization dashboard. `(Bug 981308)`

Workaround: Use a different browser to view or modify the Visualization dashboard.

5.6 Cannot Install Sentinel on SLES 11 SP4 in FIPS Mode

Issue: If you try to install Sentinel on a computer that is running the SLES 11 SP4 operating system in FIPS mode, the installation process will fail. `(Bug 990201)`

Workaround: Ensure the operating system is not in FIPS mode, and then complete the following steps:

1. Install Sentinel. For more information, see "Installing Sentinel" in the *Sentinel Installation and Configuration Guide*.
2. Enable Sentinel Server to run in FIPS mode. For more information, see "Enabling Sentinel Server to Run in FIPS 140-2 Mode" in the *Sentinel Installation and Configuration Guide*.
3. Use the following command to enable the operating system to run in FIPS mode:

```
fips=1 /boot/grub/menu.lst
```

5.7 Cannot Receive Events through Sentinel Link Connector

Issue: Sentinel does not receive events through Sentinel Link Connector. `(Bug 989784)`

Workaround: The Sentinel Link Connector version 2011.1r4 resolves this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the preview version of the Connector from the Previews section.

5.8 Cannot Receive Events from NetIQ eDirectory

Issue: NetIQ eDirectory Instrumentation cannot connect to Audit Connector through Platform Agent. As a result, Sentinel cannot receive events from eDirectory. This issue occurs because eDirectory Instrumentation uses MD5 RSA certificate algorithm, which has been deprecated in Java 8 update 77 that is used in Sentinel 8.0. (Bug 985312)

Workaround: To enable eDirectory Instrumentation to use a custom certificate, perform the steps mentioned in NetIQ Knowledgebase Article 7017764.

5.9 When Upgrading the Sentinel Appliance from Versions Prior to 7.4 SP1, an Incorrect Warning Displays

Issue: A change to password storage in Sentinel 7.4 SP1 causes the following error to display when upgrading the appliance from versions prior to 7.4 SP1:

```
Failed to set encrypted password
```

(Bug 967764)

Workaround: The warning is expected and you can safely ignore it. There is no impact to the upgrade.

5.10 Sentinel Main Interface Displays Blank Page After Converting to Sentinel Scalable Data Manager

Issue: After you enable SSDM, when you log in to the Sentinel Main interface, the browser displays a blank page. (Bug 1006677)

Workaround: Close your browser and log in to the Sentinel Main interface again. This issue only happens once, the first time you log in to the Sentinel Main interface after you enable SSDM.

5.11 StreamingEventIndexer Job Does Not Support IPv6

Issue: The com.novell.sentinel.spark.StreamingEventIndexer job does not support IPv6. If an event contains an IPv6 address, the job fails. (Bug 1006975)

Workaround: The workaround is to change the IP type to a string. To make this change, contact technical support.

5.12 Multiple SEVERE Messages in the Server Logs After You Enable Scalable Storage

Issue: After you enable scalable storage, the SSDM server logs display multiple instances of the following message:

```
SEVERE|TimerThreadPool
pool|esecurity.ccs.comp.scalablestorage.KibanaVisualAnalyticsUtil.initializeKibana
MappingSearch

Unsuccessful in initializing the kibana mapping search call with status code 400
```

(Bug 1009662)

Workaround: You can safely ignore these messages. There is no functional impact.

5.13 Exception in the Sentinel Server Log When You Upgrade Sentinel Versions Prior to 7.3 SP1 to Versions 7.3 SP1 and Later

Issue: When you upgrade Sentinel from version 7.3 to version 7.3 SP1 and start the Sentinel server, you might see the following exception in the server log:

```
Invalid length of data object ......
```

(Bug 933640)

Workaround: Ignore the exception. There is no impact to Sentinel performance because of this exception.

5.14 Cannot View Alerts with IPv6 Data in Alert Views

Issue: Sentinel alert views and alert dashboards do not display alerts that have IPv6 addresses in IP address fields. (Bug 924874)

Workaround: To view alerts with IPv6 addresses in Sentinel, perform the steps mentioned in NetIQ Knowledgebase Article 7016555.

5.15 Bar Mitzvah Security Vulnerability in Sentinel Link Connector

Issue: The Bar Mitzvah security vulnerability exists in Sentinel Link Connector. Sentinel Link Connector uses the RC4 algorithm in SSL and TSL protocols, which might allow plaintext recovery attacks against the initial bytes of a stream. For more information, see CVE-2015-2808. (Bug 933741)

Workaround: The Sentinel Link Connector version 2011.1r4 resolves this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

5.16 The Agent Manager Connector Does Not Set the Connection Mode Property in Events If the Associated Collector Supports Multiple Connection Modes

Issue: The Agent Manager Connector version 2011.1r3 does not set the CONNECTION_MODE property in the events if the Collector parsing the events supports multiple connection modes. (Bug 880564)

Workaround: The Agent Manager Connector version 2011.1r5 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

5.17 Sentinel Agent Manager 7.3 Does Not Consider the RawDataTapFileSize Configuration

Issue: Sentinel Agent Manager 7.3 ignores the value specified in `RawDataTapFileSize` attribute in the `SMServiceHost.exe.config` file for the raw data file size configuration, and stops writing to the raw data file when the file size reaches 10 MB. (Bug 867954)

Workaround: Manually copy the content of the raw data file into another file and clear it when the file size reaches 10 MB, so that Sentinel Agent Manager can write new data into it.

5.18 Tips Table Search Does Not Return the Complete List of Alert Fields in Upgraded Sentinel Installations

Issue: In upgraded installations of Sentinel, when you search for alert attributes in the Tips table in the Sentinel Main interface, the search does not return the complete list of alert fields. However, alert fields display correctly in the Tips table if you clear the search. (Bug 914755)

Workaround: There is no workaround at this time.

5.19 Data Synchronization Fails While Synchronizing IPv6 Addresses in Human Readable Format

Issue: Data synchronization fails when you try to synchronize IPv6 address fields in a human readable format to external databases. For information about configuring Sentinel to populate the IP address fields in human readable dot notation format, see "Creating a Data Synchronization Policy" in the *NetIQ Sentinel Administration Guide*. (Bug 913014)

Workaround: To fix this issue, manually change the maximum size of the IP address fields to at least 46 characters in the target database, and re-synchronize the database.

5.20 Event Search Does Not Respond if You Do Not Have Any Event Viewing Permissions

Issue: If you run an event search when your role's security filter is blank and your role does not have event viewing permissions, the search does not complete. The search does not display any error message about the invalid event viewing permissions. (Bug 908666)

Workaround: Update the role with one of the following options:

1. Specify criteria in the **Only events matching the criteria** field. If users in the role should not see any events, you can enter **NOT sev:[0 TO 5]**.
2. Select **View system events**.
3. Select **View all event data (including raw data and NetFlow data)**.

5.21 The Event fields Panel is Missing in the Schedule Page When Editing Some Saved Searches

Issue: When editing a saved search upgraded from Sentinel 7.2 to a later version, the **Event fields** panel, used to specify output fields in the search report CSV, is missing in the schedule page. (Bug 900293)

Workaround: After upgrading Sentinel, recreate and reschedule the search to view the **Event fields** panel in the schedule page.

5.22 Sentinel Does Not Return Any Correlated Events When You Search for Events for the Deployed Rule with the Default Fire Count Search

Issue: Sentinel does not return any correlated events when you search for all correlated events that were generated after the rule was deployed or enabled, by clicking the icon next to **Fire count** in the **Activity statistics** panel in the Correlation Summary page for the rule. (Bug 912820)

Workaround: Change the value in the **From** field in the Event Search page to a time earlier than the populated time in the field and click **Search** again.

5.23 Security Intelligence Dashboard Displays Invalid Baseline Duration When Regenerating a Baseline

Issue: During Security Intelligence baseline regeneration, the start and finish dates for the baseline are incorrect and display 1/1/1970. (Bug 912009)

Workaround: The correct dates are updated after the baseline regeneration is complete.

5.24 Sentinel Server Shuts Down When Running a Search If There Are Large Number of Events in a Single Partition

Issue: Sentinel server shuts down when you run a search if there are a large number of events indexed in a single partition. (Bug 913599)

Workaround: Create retention policies in such a way that there are at least two partitions open in a day. Having more than one partition open helps reduce the number of events indexed in partitions.

You can create retention policies that filter events based on the `estzhour` field, which tracks the hour of the day. Therefore, you can create one retention policy with `estzhour:[0 TO 11]` as the filter and another retention policy with `estzhour:[12 TO 23]` as the filter.

For more information, see "Configuring Data Retention Policies" in the *NetIQ Sentinel Administration Guide*.

5.25 Error While Using the report_dev_setup.sh Script to Configure Sentinel Ports for Firewall Exceptions on Upgraded Sentinel Appliance Installations

Issue: Sentinel displays an error when you use the `report_dev_setup.sh` script to configure Sentinel ports for firewall exceptions. (Bug 914874)

Workaround: Configure Sentinel ports for firewall exceptions through the following steps:

1. Open the `/etc/sysconfig/SuSEfirewall2` file.
2. Change the following line:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   to

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Restart Sentinel.

5.26 Sentinel Generic Collector Performance Degrades When Generic Hostname Resolution Service Collector is Enabled

Issue: Sentinel Generic Collector performance degrades when Generic Hostname Resolution Service Collector is enabled on Microsoft Active Directory and Windows Collector. EPS decreases by 50% when remote Collector Managers send events. (Bug 906715)

Workaround: There is no workaround at this time.

5.27 Sentinel Cannot Access Security Intelligence, Netflow, and Alert Data in FIPS 140-2 Mode

Issue: When you install Sentinel in FIPS 140-2 mode, the connector to Security Intelligence database fails to start, and Sentinel cannot access Security Intelligence, Netflow, and alert data. (Bug 915241)

Workaround: Restart Sentinel after installing and configuring in FIPS 140-2 mode.

5.28 The Web Browser Displays an Error When Exporting Search Results in Sentinel

Issue: When exporting search results in Sentinel, the Web browser might display an error if you modify the operating system language settings. (Bug 834874)

Workaround: To export search results properly, perform either of the following:

- While exporting the search results, remove any special characters (outside the ASCII characters) from the export filename.
- Enable UTF-8 in the operating system language settings, restart the machine, and then restart the Sentinel server.

5.29 Unable to View More Than One Report Result at a Time

Issue: While you wait for one report result PDF to open, particularly report results of 1 million events, if you click another report result PDF to view, the report result is not displayed. (Bug 804683)

Workaround: Click the second report result PDF again to view the report result.

5.30 Agent Manager Requires SQL Authentication When FIPS 140-2 Mode is Enabled

Issue: When FIPS 140-2 mode is enabled in your Sentinel environment, using Windows authentication for Agent Manager causes synchronization with the Agent Manager database to fail. (Bug 814452)

Workaround: Use SQL authentication for Agent Manager when FIPS 140-2 mode is enabled in your Sentinel environment.

5.31 Sentinel High Availability Installation in Non-FIPS 140-2 Mode Displays an Error

Issue: The Sentinel High Availability installation in non-FIPS 140-2 mode completes successfully but displays the following error twice:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

(Bug 810764)

Workaround: The error is expected and you can safely ignore it. Although the installer displays the error, the Sentinel High Availability configuration works successfully in non-FIPS 140-2 mode.

5.32 Active Search Jobs Duration and Accessed Columns Inaccuracies

Issue: The Sentinel Main interface displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Main interface computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Main interface clock is set to 1:30 PM and the Sentinel server clock is set to 2:30 PM. (Bug 719875)

Workaround: Ensure the time on the computer you use to access the Sentinel Main interface is the same as or later than the time on the Sentinel server computer.

5.33 IssueSAMLToken Audit Event Displays Incorrect Information in the Security Intelligence Dashboard

Issue: When you log in to the security dashboard and perform a search for `IssueSAMLToken` audit event, the `IssueSAMLToken` audit event displays incorrect hostname (InitiatorUserName) or (IP address) SourceIP. (Bug 870609)

Workaround: There is no workaround at this time.

6 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 website.

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

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

7 Legal Notice

For information about NetIQ legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see http://www.netiq.com/company/legal/.