NetIQ Sentinel 7.0.1 Release Notes

April 2012

NetIQ Sentinel 7.0.1, previously called Novell Sentinel, 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 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.

- Section 1, “What’s New?,” on page 1
- Section 2, “System Requirements,” on page 4
- Section 3, “Installing Sentinel 7.0.1,” on page 4
- Section 4, “Upgrading to Sentinel 7.0.1,” on page 5
- Section 5, “Known Issues,” on page 5
- Section 6, “Documentation,” on page 9
- Section 7, “Legal Notices,” on page 9

1 What’s New?

The following sections outline the key features and functions provided by this version of Sentinel.

- Section 1.1, “Monitoring Incoming Events,” on page 1
- Section 1.2, “Lengthening Event Fields,” on page 1
- Section 1.3, “Security Improvements,” on page 2
- Section 1.4, “Software Fixes and Enhancements,” on page 2

1.1 Monitoring Incoming Events

Sentinel provides an Operational EPS graph that displays the average EPS rate before applying filters at the event source, Connector, or Collector level. This allows you to determine whether the EPS rate is as expected and in compliance with the license. You can also generate reports to analyze the EPS rate over a specified time period and from specific Sentinel servers in your organization. For more information, see “Monitoring the Events Per Second Received by Sentinel”in the *NetIQ Sentinel 7.0.1 Administration Guide*.

1.2 Lengthening Event Fields

The InitiatiorServiceName (sp) and TargetServiceName (dp) fields size is increased from 32 to 256 characters to accommodate more characters in these fields. If you have created a Data Sync policy in Sentinel 7.0 that synchronizes either or both of the event fields, you need to modify the target column

size in the external database table to reflect the increased size of the fields. For more information about Data Sync, see "Configuring Data Synchronization" in the *NetIQ Sentinel 7.0.1 Administration Guide*.

1.3 Security Improvements

Sentinel 7.0.1 includes the following security improvements:

- Fixes the Directory traversal vulnerability CVE-2011-5028 issue. Users authenticated to the Sentinel Web interface now do not have access to files in the server.
- The Java Runtime Environment (JRE) is upgraded to version 1.6.0_30.
- MongoDB is upgraded to version 2.0.2.

1.4 Software Fixes and Enhancements

Sentinel 7.0.1 includes the following software fixes and enhancements that improve the functionality and usability of the product:

- Section 1.4.1, "Resolves an Issue with Renaming the Role Name," on page 2
- Section 1.4.2, "Resolves an Issue with the Total Event Count Number in the Dashboard," on page 2
- Section 1.4.3, "Resolves an Issue with the View Triggers Link," on page 3
- Section 1.4.4, "Resolves an Issue with the Responsible Drop-down List," on page 3
- Section 1.4.5, "Resolves an Issue with the clean_db.sh Script," on page 3
- Section 1.4.6, "Resolves the Issue with Viewing the Baseline Data," on page 3
- Section 1.4.7, "Resolves an Issue with the Shutting Down the System," on page 3
- Section 1.4.8, "Resolves an Issue with Running Incidents-Based Reports," on page 3
- Section 1.4.9, "Resolves an Issue with Non-root Installation," on page 3
- Section 1.4.10, "Resolves an Issue with Creating Dashboards," on page 4
- Section 1.4.11, "Resolves an Installation Issue on RHEL Systems," on page 4
- Section 1.4.12, "Resolves an Issue with Accessing the Group By List," on page 4
- Section 1.4.13, "Improves Raw Data Processing," on page 4

NOTE: For the list of software fixes and enhancements in Sentinel 7.0, see the Sentinel 7.0 Release Notes (http://www.novell.com/documentation/sentinel70/s70_readme/data/s70_readme.html).

1.4.1 Resolves an Issue with Renaming the Role Name

Issue: When you rename a role in the Sentinel Web interface, Sentinel does not update the name in the Roles list. (BUG 712723)

Fix: Sentinel now updates the role when you rename it.

1.4.2 Resolves an Issue with the Total Event Count Number in the Dashboard

Issue: When the event count range is between 1000000 and1100000, the total event count value is not correct. For example, if the event count is approximately 1071110, the total event count shows 1.7M. (BUG 710747)

Fix: The Security Intelligence dashboard now summarizes the total event count properly.

1.4.3 Resolves an Issue with the View Triggers Link

Issue: When a Sentinel server searches or forwards a correlation event to another Sentinel server, the associated *View Triggers* link is enabled in the Correlation Events page even though there are no triggers to display. (BUG 719301)

Fix: The *View triggers* link does not show up in the interface when you search or forward correlation events to other Sentinel servers.

1.4.4 Resolves an Issue with the Responsible Drop-down List

Issue: The *Responsible* drop-down list in the Action Manager Window includes temporary user names created by the system for job processes, such as a distributed search. (BUG 723189)

Fix: The *Responsible* drop-down list now excludes temporary user names created by the system.

1.4.5 Resolves an Issue with the clean_db.sh Script

Issue: The `clean_db.sh` script does not accept localized values when you run the script in Traditional Chinese, Brazilian Portuguese, and French languages. (BUG 723905)

Fix: The script now accepts values in the language the script is running.

1.4.6 Resolves the Issue with Viewing the Baseline Data

Issue: When you create a baseline from a category view, Sentinel generates an error message and does not return to the main dashboard page when you click the associated link. (BUG 722118)

Fix: Sentinel displays the newly created baseline data without errors.

1.4.7 Resolves an Issue with the Shutting Down the System

Issue: When the local storage is 100% full and you shut down the Sentinel server, Sentinel logs the `IllegalStateException` message continuously in the server logs and some services do not shut down in the backend. (BUG 739831)

Fix: The Sentinel services shut down successfully and exceptions are not logged continuously.

1.4.8 Resolves an Issue with Running Incidents-Based Reports

Issue: When the total number of incident events exceed 2000 and you run any incident-based report, the report does not run and Sentinel logs exceptions in the server logs. (BUG 724586)

Fix: Incident-based reports run successfully regardless of the number of incident events.

1.4.9 Resolves an Issue with Non-root Installation

Issue: When the installer files are in the root directory and you install the Sentinel server, Collector Manager, or Correlation Engine as a non-root user, the installation fails. (BUG 744215)

Fix: The installer script displays a message that indicates installation files must be placed in a directory owned by the non-root user.

1.4.10 Resolves an Issue with Creating Dashboards

Issue: When you log in with a different case than defined while creating the user account, you cannot create or view dashboards. For example, if you created the user name "admin" and log in to Sentinel as "Admin," the *Create Dashboard* link is not available. When you select existing dashboards, an error is displayed. (BUG 734495)

Fix: Sentinel allows you to create security intelligence dashboards regardless of the password case used to log in.

1.4.11 Resolves an Installation Issue on RHEL Systems

Issue: When you install Sentinel in a non-default location on RHEL systems, the installation stops after you accept the license agreement. (BUG 723588)

Fix: Installation completes successfully in non-default locations.

1.4.12 Resolves an Issue with Accessing the Group By List

Issue: In Internet Explorer 8, when you select the *Group By* drop-down list in the Correlation interface, it takes several minutes to display the list. (BUG 704962)

Fix: This release of Sentinel improves the performance time when accessing the *Group By* list.

1.4.13 Improves Raw Data Processing

Issue: When there is a large number of event sources, periodic creation and updating of raw data files in the database for each event source impacts the overall system performance. (BUG 697326)

Fix: This release of Sentinel provides performance improvements that prevents raw data file processing from impacting the system performance.

2 System Requirements

You can upgrade to Sentinel 7.0.1 from Sentinel 7.0 or perform a new installation.

For more information about system requirements, see "Meeting System Requirements" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

3 Installing Sentinel 7.0.1

To install Sentinel 7.0.1, see the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

Along with the Sentinel installation, install the supportutils RPMs as a root user on SLES systems to enable configuration information and log file retrieval for future troubleshooting. These steps are performed automatically on appliance installations of Sentinel. To install the supportutils RPMs, issue the following command:

```
rpm -Uvh supportutils*
```

4 Upgrading to Sentinel 7.0.1

To upgrade Sentinel 7.0 to Sentinel 7.0.1, see "Upgrading Sentinel" in the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*.

After upgrading from Sentinel 7.0 to Sentinel 7.0.1, perform the following post-upgrade procedures when applicable for your environment.

- ***If you installed Sentinel in a non-default location***, you must run the following commands as the `novell` user:

  ```
  ln -s

  "$RPM_INSTALLATION_PREFIX/opt/novell/sentinel/3rdparty/activemq/activemq-all-5.4.2.jar"

  "$RPM_INSTALLATION_PREFIX/opt/novell/sentinel/lib/activemq-all-5.4.2.jar"
  ```

  where `$RPM_INSTALLATION_PREFIX` is the location of the Sentinel installation.

- Manually update the Sentinel Core Solution Pack provided with Sentinel 7.0.1. For instructions on manually upgrading the solution pack, see the Sentinel Core Solution Pack (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) documentation.

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, contact Technical Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup).

- Section 5.1, "Accessing Help Menu in the Sentinel Control Center," on page 6
- Section 5.2, "Expired Trial License Error," on page 6
- Section 5.3, "Sentinel Appliance Login," on page 6
- Section 5.4, "Filter Builder Updates," on page 6
- Section 5.5, "Action Output for Multiple Events," on page 6
- Section 5.6, "Wildcard Search in Filters," on page 7
- Section 5.7, "Sentinel Rest API Documentation," on page 7
- Section 5.8, "Solution Manager Installation of Correlation Rules," on page 7
- Section 5.9, "Sentinel Link Action Displays Incorrect Message," on page 7
- Section 5.10, "Special Characters in Password Affect iTRAC," on page 7
- Section 5.11, "Dashboard and Anamoly Definitions with Identical Names," on page 7
- Section 5.12, "Active Search Jobs Duration and Accessed Columns Inaccuracies," on page 8
- Section 5.13, "Remote Collector Manager Connection," on page 8
- Section 5.14, "Connector Version Details Inaccuracies," on page 8
- Section 5.15, "Baselining and Trending Errors," on page 8
- Section 5.16, "Sorting of Strings in Certain Languages," on page 8
- Section 5.17, "Renamed Anomalies," on page 9

- Section 5.18, “Installing the Appliance on Hardware,” on page 9
- Section 5.19, “Upgrading with Symbolic Links to Folders,” on page 9

5.1 Accessing Help Menu in the Sentinel Control Center

Issue: After you upgrade the server to Sentinel 7.0.1, the URLs in the *Sentinel Control Center* > *Help* > *Help* menu might not launch the relevant Web sites. This happens if the `.novell\sentinel\config\SentinelPreferences.properties` file was already saved in the browser location before the upgrade. (BUG 748898)

Workaround: Delete the `SentinelPreferences.properties` file and relaunch Sentinel Control Center. Sentinel downloads the latest `SentinelPreferences.properties` file.

The file is located in the following directory:

Windows: `C:\Documents and Settings\<user>\.novell\sentinel\config\SentinelPreferences.properties`

SLES: `.novell\sentinel`

RHEL: `.novell\sentinel`

5.2 Expired Trial License Error

Issue: In Sentinel 7.0.1, after the trial license is expired, when you log in or log out of the Web interface, Sentinel displays the error 403 REST. (BUG 746400)

Workaround: Ignore the error message.

5.3 Sentinel Appliance Login

Issue: If you specified a $ character in the password, Sentinel stores the password differently in the database depending on where the $ is placed in the password. If the password starts with the $ special character, Sentinel stores the password with a file name. If the $ character is somewhere in the middle of the password, Sentinel truncates the password to the location of the $ character. (BUG 734500)

Workaround: The actual password is stored in the `home/novell/.pgpass` file. Obtain the password from this file and then log in to Sentinel. For example, if you specified the password as abc$123, the Sentinel stores the password as abc in the `.pgpass` file. You can log in to Sentinel by specifying abc as the password.

5.4 Filter Builder Updates

Issue: If you change an event field name in the Sentinel Control Center, the change is not reflected in the Sentinel Web interface Filter builder. (BUG 696398)

Workaround: Refresh the Web browser and the change is then displayed in the Sentinel Web interface.

5.5 Action Output for Multiple Events

Issue: If you select multiple events in the Sentinel Web interface and select the Target/ping or Initiator/ping action, Sentinel displays the action output for the first event only. (BUG 698767)

Workaround: There is no solution at this time.

5.6 Wildcard Search in Filters

Issue: When you have at least one role containing an asterisk (*) in the name, you cannot use '*' as a wild card when searching filters with `Share with roles` selected from the Sentinel Web interface. (BUG 710004)

Workaround: To use '*' as a wild card when searching filters, rename roles that contain an asterisk.

5.7 Sentinel Rest API Documentation

Issue: Accessing the Sentinel REST API documentation from a browser bookmark returns an error. (BUG 719708)

Workaround: Access the Sentinel REST API documentation directly from the Sentinel Web interface *Help* menu.

5.8 Solution Manager Installation of Correlation Rules

Issue: Solution Manager does not install correlation rules when a correlation rule with an identical name already exists on the system. A `NullPointerException` error is logged in the console. (BUG 713962)

Workaround: Ensure all correlation rules have a unique name.

5.9 Sentinel Link Action Displays Incorrect Message

Issue: When you execute a Sentinel Link action from the Web interface Sentinel displays a success message even when the Sentinel Link Connector integrator test failed from the Sentinel Control Center. (BUG 710305)

Workaround: There is no solution at this time.

5.10 Special Characters in Password Affect iTRAC

Issue: When the appuser password contains any the of the following special characters, the iTrac feature does not work properly: '+', '\', '#', or ','. The administrator user password provided during a standard configuration installation is used by the `admin`, `dbuser`, and `appuser`. (BUG 717679)

Workaround: Ensure the appuser password does not contain '+', '\', '#', or ','.

5.11 Dashboard and Anamoly Definitions with Identical Names

Issue: When a Security Intelligence dashboard and an anomaly definition have identical names, the dashboard link is disabled on the Anomaly Details page. (BUG 715986)

Workaround: Ensure you use unique names when creating dashboards and anomaly definitions.

5.12 Active Search Jobs Duration and Accessed Columns Inaccuracies

Issue: The Sentinel Web interface displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Web interface computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Web 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 Web interface is the same as or later than the time on the Sentinel server computer.

5.13 Remote Collector Manager Connection

Issue: Connections to remote Collector Managers drop and are then re-established minutes later. (BUG 719244)

Workaround: For information on assessing your environment and determining how to handle the number of events generated, see Novell Technical Information Document (TID)# 7009554 "Sentinel 7.0 Performance Monitoring."

5.14 Connector Version Details Inaccuracies

Issue: After you upgrade a Connector, Sentinel might not display the latest Connector details in the Plug-in Details window. (BUG 713147)

Workaround: Refresh the ESM user interface by clicking *Reload Event Source Management Data* in the ESM toolbar to update the Connector details.

5.15 Baselining and Trending Errors

Issue: When you use forwarded ports, such as 80 or 443, or destination network-address-translation, baseline and trending does not function properly in the Security Intelligence dashboard. (BUG 694732)

Workaround: Append the default port number to the URL when accessing Sentinel baselining in the following instances:

- Sentinel has been configured to listen on the default port, 443.
- Sentinel is listening on a non-default port but port forwarding is enabled, which routes traffic from the default port to the port on which Sentinel is listening.

5.16 Sorting of Strings in Certain Languages

Issue: Sorting of localized strings does not work correctly in certain languages. If a localized language uses non-ascii characters or characters with diacritical marks, the sorting of strings in these languages does not work. (BUG 695468)

Workaround: There is no solution at this time.

5.17 Renamed Anomalies

Issue: When you filter on the new or old name of a renamed anomaly, the message `Showing X of Y total anomalies` uses the total anomaly count of both the old and new name for `X`. The message should use the number of anomalies matching the name for which you filtered. (BUG 724574)

Workaround: There is no solution at this time.

5.18 Installing the Appliance on Hardware

Issue: When installing the appliance on hardware with Extensible Firmware Interface (EFI), the installation fails.

Workaround: Disable all EFI features in the BIOS Setup. (BUG 754769)

5.19 Upgrading with Symbolic Links to Folders

Issue: The upgrade does not proceed if symbolic links are used for the following folders and subfolders:

- opt/novell (Base folder)
- etc/opt/novell (Configuration folder)
- var/opt/novell (Data folder)

Workaround: Remove symbolic links to these folders and ensure they are in the standard release directories. (BUG 701778)

6 Documentation

The online product documentation is available at the Sentinel 7.0 documentation Web site (http://novell.com/documentation/sentinel70/index.html).

7 Legal Notices

For more information, please contact NetIQ at:

1233 West Loop South, Houston, Texas 77027
U.S.A.
www.netiq.com