Sentinel 8.2.1 Release Notes

January 2019

Sentinel 8.2.1 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, our online community that also includes product information, blogs, and links to helpful resources. You can also share your ideas for improving the product in the Ideas Portal.

The documentation for this product is available 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 Documentation page. To download this product, see the Product Download website.

1 What’s New?

The following sections outline the key features provided by this version, as well as issues resolved in this release:

1.1 Open JDK

Sentinel 8.2.1 replaces Oracle JDK with Azul Zulu OpenJDK, an open source alternative. The only observable difference due to this change is the way you launch Control Center or Solution Designer. OpenJDK does not have Webstart. Therefore, you must launch Control Center or Solution Designer by downloading new files to launch these applications.

For more information about running these applications, see Sentinel Control Center in the Sentinel User Guide and Accessing the Solution Designer in the Sentinel Administration Guide. You must install Java 8 to launch applications on a Windows or Linux operating system.

NOTE: Micro Focus will no longer provide additional Oracle JDK updates for Sentinel. Therefore, if there are security vulnerabilities or other bugs related to Oracle JDK, the primary solution is to upgrade to Sentinel 8.2.1 or later.

1.2 Enhanced Security for Communications between Sentinel and Other Integrated Products

Sentinel now provides a new permission, **Send events and attachments**, that enables you to allow only designated users to send events or attachments from Change Guardian and Secure Configuration Manager to Sentinel. When you upgrade to Sentinel 8.2.1, Sentinel automatically assigns this permission to users in the Administrator role.

WARNING: For non-administrator users who send events or attachments to Sentinel, you must manually assign this permission. Unless you assign this permission, Sentinel will no longer receive events and attachments from Change Guardian and Secure Configuration Manager.

For more information about assigning this permission, see the Sentinel Administration Guide.

1.3 Removal of Advisor from Sentinel

With the availability of configuring the desired Threat Intelligence data sources, Sentinel no longer includes the Advisor data subscription service. Therefore, corresponding features such as Exploit Detection are no longer available in Sentinel. Once you have configured the required Threat Intelligence data sources, you can view any potential threats from low-reputation IP addresses, vulnerabilities, and potential exploitation of any vulnerabilities in the Security Health dashboard.

1.4 New Certified Platforms

Sentinel is now certified on the following platforms:

Traditional installation: Red Hat Enterprise Linux Server 6.10 (64-bit)

Data indexing: Elasticsearch 5.6.13

1.5 Software Fixes

Sentinel 8.2.1 includes software fixes that resolve the following issues:

1.5.1 Remote Collector Manager Does Not Send the Collected Events and Logs an Error

Remote Collector Manager sends the collected events and does not log an error. `(Bug 1115427)`

1.5.2 Correlated Events Contain only the Truncated Content from the Message Field

Correlated events contain the entire content of the **Message** field without truncation. `(Bug 1103774)`

1.5.3 Incorrect Information About jquery in Vulnerability Scan Reports

Issue: Vulnerability scans report issues, such as the following message, with a vulnerable version of jquery:

```
The file 'jquery-1.11.3.min.js' includes a vulnerable version of the library
'jquery'.
```

The noted vulnerability affects only versions 1.8.0 to 1.12.0, but the reported URL redirects to a much newer version of jquery (3.x). (Bug 1088099)

Workaround: This issue does not occur anymore.

2 System Requirements

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

3 Upgrading to Sentinel 8.2.1

You must first upgrade to Sentinel 8.2 or later and then upgrade to Sentinel 8.2.1.

- **Upgrading the Sentinel Appliance:** You must first upgrade to Sentinel 8.2 or later and upgrade the operating system to SLES 12 SP3 because Sentinel 8.2.1 updates are available only on the SLES 12 channel. You must then upgrade to Sentinel 8.2.1 through the Sentinel Appliance Management Console.
- **Upgrading Sentinel Appliance in High Availability:** The Sentinel 8.2 appliance does not contain the folders to launch Sentinel Appliance Management Console. For more information about launching the Sentinel Appliance Management Console, see Upgrading to Sentinel 8.2.0.1 or Later.

WARNING: After you upgrade to Sentinel 8.2.1, you must manually assign the **Send events and attachments** permission to non-administrator users who send events or attachments to Sentinel. Unless you assign this permission, Sentinel will no longer receive events and attachments from Change Guardian and Secure Configuration Manager.

For information about upgrading to Sentinel 8.2.1, see the *Sentinel Installation and Configuration Guide*.

4 Known Issues

Micro Focus strives to ensure our products provide quality solutions for your enterprise software needs. The following known 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, we will prioritize and fix the issues according to standard defect-handling policies. For more information about support polices, see Support Policies.

4.1 Sentinel 8.2 Appliance in Microsoft Hyper-V Server 2016 Does Not Start When You Reboot

Issue: In Hyper-V Server 2016, Sentinel appliance does not start when you reboot it and displays the following message:

```
A start job is running for dev-disk-by\..
```

This issue occurs because the operating system modifies the disk UUID during installation. Therefore, during reboot it cannot find the disk.

(Bug 1097792)

Workaround: Manually modify the disk UUID. For more information, see Knowledge Base Article 7023143.

4.2 Error When Upgrading to Sentinel 8.2 HA Appliance

Issue: When you upgrade to Sentinel 8.2 HA appliance, Sentinel displays the following error:

```
Installation of novell-SentinelSI-db-8.2.0.0-<version> failed:
with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Command exited
with status 1.
Abort, retry, ignore? [a/r/i] (a):
```

(Bug 1099679)

Workaround: Before you respond to the above prompt, perform the following:

1. Start another session using PuTTY or similar software to the host where you are running the upgrade.
2. Add the following entry in the `/etc/csync2/csync2.cfg` file:

   ```
   /etc/opt/novell/sentinel/config/configuration.properties
   ```

3 Remove the `sentinel` folder from `/var/opt/novell`:

```
rm -rf /var/opt/novell/sentinel
```

4 Return to the session where you had initiated the upgrade and enter `r` to proceed with the upgrade.

4.3 Installation of Collector Manager and Correlation Engine Appliance Fails in Languages Other than English in MFA Mode

Issue: Installation of Collector Manager and Correlation Engine appliance fails in MFA mode if the operating system language is other than English. `(Bug 1045967)`

Workaround: Install Collector Manager and Correlation Engine appliances in English. After the installation is complete, change the language as needed.

4.4 Internet Explorer 11 Cannot Launch Event Visualization Dashboard

Workaround: Use a different browser to view or modify the visualization dashboard. `(Bug 981308)`

4.5 Usability Issues in the Appliance Installation Screens

Issue: The **Next** and **Back** buttons in the appliance installation screens do not appear or are disabled in some cases, such as the following:

- When you click **Back** from the Sentinel precheck screen to edit or review the information in the Sentinel Server Appliance Network Settings screen, there is no **Next** button to proceed with the installation. The **Configure** button allows you to only edit the specified information.
- If you have specified incorrect network settings, the Sentinel Precheck screen indicates that you cannot proceed with the installation due to incorrect network information. There is no **Back** button to go the previous screen to modify the network settings.

`(Bug 1089063)`

Workaround: Restart the appliance installation.

4.6 Error Message During Sentinel Start Up

Issue: Sentinel displays the following message during start up in the `server.log` file:

```
Value for attribute rv43 is too long
```

`(Bug 1092937)`

Workaround: Ignore the exception. Although the message is displayed, Sentinel works as expected.

4.7 SSDM Displays an Exception When Deleting Events Whose Retention Period Has Expired

Issue: When there is a large number of events whose retention period has expired and SSDM tries to delete those events from Elasticsearch, the following exception is displayed in the `server.log` file:

```
java.net.SocketTimeoutException: Read timed out
```

`(Bug 1088511)`

Workaround: Ignore the exception. This exception occurs due to the time taken to delete the large amount of data. Although the exception is displayed, SSDM successfully deletes the events from Elasticsearch.

4.8 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: Uninstall the Collector and configure the Sentinel server and Collector Manager to resolve hostname to IP address or vice versa. For more information, see "Resolving Hostnames and IP Addresses" in the *Sentinel Administration Guide*.

4.9 Collector Manager Runs Out of Memory if Time Synchronization is Enabled in open-vm-tools

Issue: If you manually install and enable time synchronization in open-vm-tools, they periodically synchronize time between the Sentinel appliance (guest) and the VMware ESX server (host). These time synchronizations can result in moving the guest clock either behind or ahead of the ESX server time. Until the time is synchronized between the Sentinel appliance (guest) and the ESX server (host), Sentinel does not process events. As a result, a large number of events are queued up in the Collector Manager, which may eventually drop events once it reaches its threshold. To avoid this issue, Sentinel disables time synchronization by default in the open-vm-tools version available in Sentinel. `(Bug 1099341)`

Workaround: Disable time synchronization. For more information about disabling time synchronization, see Disabling Time Synchronization.

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

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

Workaround: Use SQL authentication for Agent Manager.

4.11 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.

4.12 Internet Explorer 11 Does Not Load Dashboards as Expected

Issue: In Internet Explorer 11, when you launch the dashboards:

- Alert and Threat Hunting dashboard redirects to **My Dashboard**.
- User Activity dashboard displays an error.

This issue occurs due to the URL length limitation in Internet Explorer 11. (Bug 1068418)

Workaround: Perform the following:

1. Launch Event Visualization dashboard.
2. Click **Management > Advanced Settings**.
3. Set the value of **storeInSessionStorage** to `true`.

4.13 Keytool Command Displays a Warning

Issue: While using Keytool command, the following warning is displayed: `The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12which is an industry standard format using "keytool -importkeystore -srckeystore /<sentinel_install_directory>/etc/opt/novell/sentinel/config/.webserverkeystore.jks -destkeystore /<sentinel_install_directory>/etc/opt/novell/sentinel/config/.webserverkeystore.jks -deststoretype pkcs12". (Bug 1086612)`

Workaround: The warning is expected and you can safely ignore it. Although the warning is displayed, Keytool command works as expected.

4.14 Sentinel Does Not Process Threat Intelligence Feeds In FIPS Mode

Issue: In FIPS mode, when processing out-of-the-box threat Intelligence feeds from URLs, Sentinel displays the following error: `Received fatal alert: protocol_version. This issue occurs because the out-of-the-box threat feeds now support only TLS 1.2, which does not work in FIPS mode. (Bug 1086631)`

Workaround: Perform the following:

1. Click **Sentinel Main** > **Integration** > **Threat Intelligence Sources**.
2. Edit each URL to change the protocol from `http` to `https`.

4.15 Logging Out From Sentinel Main Does Not Log Out of Dashboards And Vice Versa in MFA mode

Issue: If Sentinel is integrated with Advanced Authentication Framework MFA mode, you do not get logged out of Sentinel dashboards when you log out of **Sentinel Main** and vice versa. This is due to an issue in the Advanced Authentication Framework. (Bug 1087856)

Workaround: Until a fix is available in the Advanced Authentication Framework, refresh the screen to view the login screen.

5 Legal Notice