Sentinel 8.3 Service Pack 1 Release Notes

September 2020

Sentinel 8.3 SP1 resolves several previous issues and also added a few new features.

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.

- "What's New?" on page 1
- "System Requirements" on page 4
- "Installing Sentinel 8.3 SP1" on page 4
- "Upgrading to Sentinel 8.3 SP1" on page 4
- "Known Issues" on page 5
- "Contacting Micro Focus" on page 11
- "Legal Notice" on page 11

What's New?

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

- "Certificate Revocation List (STIG V-57511)" on page 2
- "Re-Indexing Event Data" on page 2
- "Azul Zulu Java Runtime Environment Upgrade" on page 2
- "Operating System (OS) Versions" on page 2
- "Software Fixes" on page 2

Certificate Revocation List (STIG V-57511)

A Certificate Revocation List (CRL) is a list of certificates that have been revoked by the issuing Certificate Authority before their scheduled expiration date. For more information, see Certificate Revocation List Implementation in an Existing Sentinel Installation, in the *Sentinel Installation and Configuration Guide*.

NOTE: If the CRL feature is enabled in the Sentinel, to use the REST endpoints refer to REST API document.

Re-Indexing Event Data

All event data partitions in the system need to be indexed for it to be searchable. During the Sentinel upgrade, the underlying data formats also get updated and the data cannot be searched. To enable the data to be searched, you must re-index all event data partitions in the system after the upgrade. For more information, see Re-indexing Event Data Partitions, in the *Sentinel Administration Guide*.

Azul Zulu Java Runtime Environment Upgrade

Sentinel includes Java 8 update242, which includes fixes for several security vulnerabilities.

Operating System (OS) Versions

Supported OS: Sentinel is now certified on the SUSE Linux Enterprise Server (SLES) 12 SP5 64-bit operating system. Fresh installations of Sentinel appliance include SLES 12 SP5.

Deprecated OS: Following OS are now deprecated since SUSE removed support for these OS:

- SLES 12 SP4
- SLES 12 SP3
- SLES 12 SP2

Software Fixes

Sentinel 8.3 SP1 includes software fixes that resolve the following issues:

- “The Sentinel Server Now Receives Events Without any Issues” on page 3
- “The Sentinel Web Console Now Displays the Correct Last Modified Timestamp” on page 3
- “The iTrac Command Now Tracks the Incident ID and Owner” on page 3
- “Though the Size of the Data is More than 4KB, Data Stores into the PostgreSQL Database” on page 3
- “The Sentinel Appliance Server Now Displays the Correct Disk Size for Configuration” on page 3
- “The DiskSpaceMonitor Now Updates the Free Space Available in the Secondary Storage” on page 3
- “Alerts are Now Displayed in the Sentinel Web Console and in the Kibana Interface” on page 3
- “The Sentinel Server Does Not Display the EFI Boot Manager Utility Error” on page 3
- “Scheduled Reports are Now Sent Via Email After Upgrading to Sentinel 8.3.1” on page 4
- “Report Sharing Option is Now Appearing for the User who Imports” on page 4
- “New Hostname Resolution Feature of Sentinel 8.2, When the Hostname is in FQDN format, it Splits into Host and Domain Fields Properly Now” on page 4

The Sentinel Server Now Receives Events Without any Issues

Issue: The Sentinel Server was not receiving events frequently because of `the error Lock held by this virtual machine.(Bug 44767)`

Fix: The Sentinel Server now receives events without any issues.

The Sentinel Web Console Now Displays the Correct Last Modified Timestamp

Issue: The Dynamic list that is created using the Sentinel Web Console was not displaying the correct last modified timestamp, after adding items to the list. `(Bug 44761)`

Fix: The Dynamic list that is created using the Sentinel Web Console now displays the correct last modified timestamp, even after adding items to the list.

The iTrac Command Now Tracks the Incident ID and Owner

Issue: The iTrac command was unable to track the incident ID and owner who completes the incident. `(Bug 44654)`

Fix: The iTrac command now tracks the incident ID and owner who completes the incident.

Though the Size of the Data is More than 4KB, Data Stores into the PostgreSQL Database

Issue: If the size of the data for TargetAttributeValue (RV43) is more than 4KB, data was not storing into the PostgreSQL database. `(Bug 44532)`

Fix: Now TargetAttributeValue (RV43) data is stored into the PostgreSQL database by truncating the data beyond the size limit of 4KB.

The Sentinel Appliance Server Now Displays the Correct Disk Size for Configuration

Issue: The Sentinel Appliance server was not displaying the correct disk size details for configuration. `(Bug 45433)`

Fix: The Sentinel Appliance server now displays the correct disk size details.

The DiskSpaceMonitor Now Updates the Free Space Available in the Secondary Storage

Issue: After the event data was deleted, the DiskSpaceMonitor was not updating the free space available in the secondary storage. `(Bug 43993)`

Fix: Whenever event data is deleted from secondary storage, the DiskSpaceMonitor now updates the free space available in the secondary storage. This ensures that you do not delete more than the required memory.

Alerts are Now Displayed in the Sentinel Web Console and in the Kibana Interface

Issue: The alerts were not displaying in the Sentinel console and in the Kibana interface. `(Bug 43994)`

Fix: Now alerts are displayed in the Sentinel console and in the Kibana interface.

The Sentinel Server Does Not Display the EFI Boot Manager Utility Error

Issue: The Sentinel server was displaying the EFI boot manager utility error. `(Bug 45606)`

Fix: Now the Sentinel server does not display the EFI boot manager utility error.

Scheduled Reports are Now Sent Via Email After Upgrading to Sentinel 8.3.1

Issue: After upgrading to Sentinel 8.3, emails were not received for reports that were scheduled before upgrade.(Bug 78001)

Fix: Scheduled reports are now sent via email after upgrading to Sentinel 8.3.1.

Report Sharing Option is Now Appearing for the User who Imports

Issue: After creating user under administrator with report sharing permission, share icon for the report was not appearing.(Bug 45699)

Fix: User under administrator now can share the report to others having report permission.

New Hostname Resolution Feature of Sentinel 8.2, When the Hostname is in FQDN format, it Splits into Host and Domain Fields Properly Now

Issue: IP to Hostname resolution feature introduced in Sentinel 8.2, in FQDN format, it was not splitting into host and domain fields properly.(Bug 43989)

Fix: Now when the hostname is in FQDN format, it splits into host and domain fields properly.

System Requirements

For more information about hardware requirements, supported operating systems, and browsers, see the Sentinel System Requirements.

Installing Sentinel 8.3 SP1

For information about installing Sentinel 8.3 SP1, see the *Sentinel Installation and Configuration Guide*.

Upgrading to Sentinel 8.3 SP1

You can upgrade to Sentinel 8.3 SP1 from Sentinel 8.2.

IMPORTANT: There is a change in the upgrade procedure of Traditional and Appliance installation. Please refer to the respective upgrade section in the Sentinel Installation and Configuration Guide and follow the steps.

WARNING: If you are upgrading from versions prior to Sentinel 8.3, 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 8.3 SP1, see the *Sentinel Installation and Configuration Guide*.

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.

- "Unable to View Storage Capacity Forecasting Chart" on page 6
- "Unavailability of Sharing Permissions for Tenant Users" on page 6
- "Error When Launching a Kibana Dashboard After Upgrading Sentinel" on page 6
- "Cannot Copy the Alert Links of All the Alerts in an Alert View in Mozilla Firefox and Microsoft Edge" on page 6
- "Installing Sentinel, Collector Manager, and Correlation Engine as an OVF Appliance Image Does Not Display the Login Screen" on page 6
- "Sentinel 8.2 Appliance in Microsoft Hyper-V Server 2016 Does Not Start When You Reboot" on page 7
- "Error When Upgrading to Sentinel 8.2 HA Appliance" on page 7
- "Installation of Collector Manager and Correlation Engine Appliance Fails in Languages Other than English in MFA Mode" on page 7
- "Usability Issues in the Appliance Installation Screens" on page 8
- "Error Message During Sentinel Start Up" on page 8
- "SSDM Displays an Exception When Deleting Events Whose Retention Period Has Expired" on page 8
- "Collector Manager Runs Out of Memory if Time Synchronization is Enabled in Open-vm-tools" on page 8
- "Agent Manager Requires SQL Authentication When FIPS 140-2 Mode is Enabled" on page 9
- "Sentinel High Availability Installation in Non-FIPS 140-2 Mode Displays an Error" on page 9
- "Keytool Command Displays a Warning" on page 9
- "Sentinel Does Not Process Threat Intelligence Feeds In FIPS Mode" on page 9
- "Logging Out From Sentinel Main Does Not Log You Out of Dashboards And Vice Versa in Multi-factor Authentication mode" on page 10
- "The Kibana Custom Dashboard is not Displayed After Upgrading to Sentinel 8.3.1" on page 10
- "When you Launch the Application Performance Monitoring (APM) from the Kibana, an Internal Server Error Message is Displayed" on page 10
- "When you Launch Kibana the Conflict Error Message is Displayed" on page 10
- "When you Reboot OS Redhat 8.1, Sentinel 8.3 is not Started Automatically" on page 10
- "When You Open Sentinel Appliance Management Console an Error Message is Displayed" on page 11

Unable to View Storage Capacity Forecasting Chart

Issue: In **Sentinel Main** > **Storage** > **Health**, the **Storage Capacity Forecasting** chart is not available. This is because Zulu OpenJDK does not include the necessary fonts. (`Bug 1146879`)

Workaround: Use the following commands to install the fonts:

- yum install fontconfig
- yum install dejavu

Unavailability of Sharing Permissions for Tenant Users

Issue: When you select a tenant while creating a role, there are no permissions listed under **Sharing** for tenant users. (`Bug 1163847`)

Workaround: None. Ignore the **Sharing** label for tenant users.

Error When Launching a Kibana Dashboard After Upgrading Sentinel

Issue: Launching a Kibana dashboard displays the following message: `No default index pattern. You must select or create one to continue. (Bug 1163143)`

Workaround: To set a Kibana index pattern as the default index pattern:

1. Select any of the following:
   - alerts.alerts
   - security.events.normalized_*
2. Click **Set as Default**.

Cannot Copy the Alert Links of All the Alerts in an Alert View in Mozilla Firefox and Microsoft Edge

Issue: The **Select All** ***<number of alerts>*** **Alerts** > **Copy Alert Link** option does not work in Firefox and Edge. (`Bug 1162070`)

Workaround: Perform the following steps:

1. Manually select all the alerts on each page of the alert view using the check box that allows you to select all the alerts.
2. Click **Copy Alert Link**.
3. Paste it in the desired application.

Installing Sentinel, Collector Manager, and Correlation Engine as an OVF Appliance Image Does Not Display the Login Screen

Issue: The installer halts at the installation in progress screen and does not display the login screen even though the installation is complete.

Workaround: Reboot the virtual machine and launch Sentinel, Collector Manager, or Correlation Engine. (`Bug 1134657`)

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.

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.

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.

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 to the previous screen to modify the network settings.

`(Bug 1089063)`

Workaround: Restart the appliance installation.

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.

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.

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.

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.

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.

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_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -destkeystore
 /<sentinel_installation_path>/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.

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`.

Logging Out From Sentinel Main Does Not Log You Out of Dashboards And Vice Versa in Multi-factor Authentication mode

Issue: In multi-factor authentication mode, if you log out of **Sentinel Main** you do not get logged out of Sentinel dashboards 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.

The Kibana Custom Dashboard is not Displayed After Upgrading to Sentinel 8.3.1

Issue: The Kibana custom dashboard is not displayed when you upgrade from Sentinel 8.3 or earlier to Sentinel 8.3.1.(Bug `58001`)

Workaround: Ensure that you re-create the custom dashboard after upgrading Sentinel.

When you Launch the Application Performance Monitoring (APM) from the Kibana, an Internal Server Error Message is Displayed

Issue: After upgrading Sentinel and when you launch the APM feature from Kibana, an internal server error message is displayed.(Bug `89038`)

Ignore the internal server error message, as the APM feature is not supported in this release.

In this release, only the following Kibana features are supported:

- Discover
- Visualize
- Dashboard
- Dev tools
- Management

When you Launch Kibana the Conflict Error Message is Displayed

Issue: After installing or upgrading Sentinel and when you launch Kibana for the first time, the conflict error message is displayed.(Bug `65001`)

Workaround: Ignore the conflict error message as there is no functionality impact.

When you Reboot OS Redhat 8.1, Sentinel 8.3 is not Started Automatically

Issue: After installing Sentinel 8.3 on OS Redhat 8.1, Sentinel (Server, RCM or RCE) is not started automatically after reboot.(Bug `83167`)

Workaround: Manually perform `rcsentinel start` after reboot.

When You Open Sentinel Appliance Management Console an Error Message is Displayed

Issue: After upgrading to Sentinel 8.3, when you try to open Sentinel Appliance Management Console of the CE (Correlation Engine) or CM (Collector Manager) of HA (High Availability) servers, an error message `Error 404 - Not found` is displayed. `(Bug 93058)`

Workaround: For more information, refer to Micro Focus Knowledge Base document.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

Legal Notice

© Copyright 2001-2020 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/ (http://www.microfocus.com/about/legal/).