opentext™

ArcSight SmartConnectors

Software Version: CE 24.2.1

SmartConnector Release Notes

Document Release Date: May 2024
Software Release Date: May 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Release Notes for ArcSight SmartConnector CE 24.2.1

This Release Notes document describes how to apply this latest release of ArcSight SmartConnector and ArcSight SmartConnector Load Balancer, and provides other information about the most recent changes, known limitations, and software fixes.

SmartConnector is an application that collects log messages from log sources, processes them into ArcSight security events, and transports them to destination consumers for analytic, storage, and compliance reporting.

You can apply SmartConnectors CE 24.2.1 (v8.4.5.P1) to:

- Perform a fresh install of the SmartConnectors.
- Upgrade the SmartConnectors from SmartConnectors CE 24.2 (v8.4.5).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- Technical Requirements Guide for SmartConnector, which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- Installation and User Guide for SmartConnectors, which provides detailed information about installing SmartConnectors.
- Configuration Guides for ArcSight SmartConnectors, which provides information about configuring SmartConnectors to collect events from different sources.
- Configuration Guide for SmartConnector Load Balancer, which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the

bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products.

Release Highlights

The SmartConnector CE 24.2.1 (v8.4.5.P1) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Upgrade of Zulu OpenJDK to 8u412
- Software fixes for Amazon CloudWatch, Amazon S3, and Check Point Syslog

For detailed information, see "What's New" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the ArcSight Idea Exchange portal, will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnectors CE 24.2.1 (v8.4.5.P1) incorporates the following SmartConnector updates:

- Security Updates
- Software Fixes

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Zulu OpenJDK to 8u412. The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade: • CVE-2023-41993 • CVE-2024-21011 • CVE-2024-21068 • CVE-2024-21085 • CVE-2024-21094 • CVE-2024-21003 • CVE-2024-21005 • CVE-2024-21002 • CVE-2024-21004

Software Fixes

The following issues are fixed in the CE 24.2.1 (v8.4.5.P1) release:

Application Modules Software Fixes	Number	Description
Amazon CloudWatch	OCTCR33I889094	The deployment of the Amazon CloudWatch connector failed because AWS Lambda support was discontinued for the Java 8 and Python 2.7 runtimes. Syntax issues also emerged in the heartbeat function's Python code that was originally written in Python 2. **Fix**: To resolve this issue, the Java runtime has been transitioned from Java 8 to java8.al2, and adjustments have been made to the heartbeat function to comply with the Python 3 syntax.
Amazon S3	OCTCR33I883037	The Amazon S3 connector encountered the following errors: • `Not a CloudTrail log` - the connector was displaying this fatal exception while processing digest files in the Amazon S3 bucket for the CloudTrail events when digest files were present in the S3 bucket. • `[com.arcsight.common.flow.stock.h][send]No consumer specified for thisoutput connector` - the connector was continuously throwing this [ERROR] in the agent.log file. **Fix**: The following fixes have been implemented to resolve the issues: • The connector will skip processing the digest files even if they are present in the Amazon S3 bucket without throwing any error. • Code changes were made to resolve the underlying issue of incomplete event alignment.

Application Modules Software Fixes	Number	Description
Check Point Syslog	OCTCR33I886016	The Check Point Syslog connector encountered parsing issues for events in which the **Name** and **Device Event Class Id** fields were populated with the **0** (Zero) that is derived from the **action** field of event log. **Fix**: The mapping regex has been updated so that if the **action** field value is **0**, then the **Name** and **Device Event Class Id** field values are mapped to the first field that is not null from the following set of fields: `Action,event_name,malware_action,auth_status,short_desc,description,message_info,activity,subscription_stat_desc,contract_name,rule_name,event_type,, scan direction, all of (one of (ProductName, product), '|', One of (subscription_stat, 'Event')), 'Scan Summary'`

Downloading and Applying the Patch

Download the appropriate executable for your platform from the Software Licenses and Downloads (SLD).

The 64-bit executable is available for download for Windows and Linux platforms. Only the 64-bit executable is available for Solaris platforms. Users should move to the Solaris 64-bit platform. There is no upgrade path from the Solaris 32-bit image to the Solaris 64-bit image.

For a successful SmartConnector installation, follow the installation procedures documented in the individual SmartConnector configuration guides available on the ArcSight Documentation website.

To apply the patch for:

- SmartConnectors, see Upgrading SmartConnectors.
- Load Balancer, see the Upgrading Load Balancer section in *Configuration Guide for SmartConnector Load Balancer*.

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.

Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:

Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command: `cd Xxxxx/lib/agent`
3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`
5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
6. Run the following command: `cd Xxxxx/lib/agent/axis`
7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Open the `Xxxxx\lib\agent` folder.
3. Search for **log4j** and delete all the entries.
4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.
5. Search for **log4j** and delete all the entries.
6. Open the `Xxxxx\lib\agent\axis` folder.
7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm-rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

   The following folders will be displayed:

   - **current** (upgraded version of the connector)
   - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector Release Notes (SmartConnectors CE 24.2.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!