Hewlett Packard
Enterprise

HPE Security ArcSight Data Platform Event Broker

Software Version: 2.10

Release Notes

January 2, 2018

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Event Broker 2.10 Release Notes

The ADP Event Broker centralizes event processing and delivery, helps you to scale your ArcSight environment, and opens up ArcSight event data to third party solutions. It enables you to take advantage of scalable, high-throughput, multi-broker clusters for publishing and subscribing to event data.

The ADP Event Broker provides a packaged version of Apache Kafka. After you install and configure an Event Broker cluster, you can use ADP SmartConnectors to publish data, and subscribe to that data with ADP Logger, ArcSight ESM, ArcSight Investigate (via Vertica integration), Apache Hadoop, or your own consumer.

The ADP Deployment Guide describes how to install, configure, and manage Event Broker. The ADP Administrator's Guide describes how to manage Event Broker.

New Features and Enhancements

Event Broker 2.1 includes the following new features and enhancements.

- **TLS 1.2:** Event Broker 2.1 only accepts the TLS 1.2 protocol. Note that any consumers or producers that connect to Kafka must use TLS 1.2. TLS v1 and v1.1 can be used for other communication.
- **Confluent Platform Upgrade:** Event Broker now uses Confluent Platform 3.3.0, which includes Kafka 0.11.0.0.
- **AutoPass Licensing:**AutoPass licensing and enforcement has been added to Event Broker. For more information on licensing, see the Licensing chapter of the *Event Broker Administrator's Guide*.
- **CEB (Evalulation Only):** Event Broker includes support for Connectors in Event Broker (CEB). This new functionality moves the security event normalization, categorization, and enrichment of connectors processing to the Docker containers environment of Event Broker, while reducing the work done by the system component left outside of Event Broker to collection of raw data (the new Collector).

For a list of issues fixed in this release, see Fixed Issues.

Note: Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production public alpha features.** These features are provided for your testing and evaluation only and should not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future. Consult the ArcMC Admin Guide, and directions from the ADP product team, for best practices and guidance on how to use these features. **CEB and Collectors must not in any circumstances be used in a production environment.**We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ADP product team at adp-ceb-alpha@hpe.com.

Supported Platforms and Browsers

For details on Event Broker platform and browser support, refer to the ADP Support Matrix document available from the Protect724, the HPE Software Community.

Event Broker Documentation

In addition to these Release Notes, the following documents are available in PDF format for download from the ArcSight Software Community.

- *ArcSight Data Platform Support Matrix:* Provides integrated support information such as platform and browser support for ADP Event Broker, Event Broker, and SmartConnectors.
- *ArcSight Data Platform Event Broker Administrator's Guide:* Describes how to configure, and manage the ADP Event Broker. Available with your download in PDF format.
- *Event Broker Deployment Guides:* Describes how to deploy Event Broker in standalone mode (part of ADP) and as part of an ArcSight Investigate deployment.

Fixed Issues

This release contains the following fixed issues.

Key	Description
INST-706	You can no longer specify a non-positive number for a number of Kakfa or ZooKeeper instances.
INST-635	An issue has been resolved where a Vertica table, investigation.rejected_events, was not created because of the error condition: "Exception in thread "main.
EB-767	In some cases, the incorrect IP address could show in the consumer group on Event Broker Manager when ESM consumes topics from EB in an HA environment. This issue has been resolved.
EB-683	In some cases, an intermittent issue with too many connections to ZooKeeper could cause routing to stop working. This issue has been resolved.

Known Limitations

Event Broker is known to have the following limitations.

Issue	Description
EB-629	After creating and saving a new topic in Event Broker manager, in the Goto Topic View, the values for partitions and replication factor will not be displayed without a refresh or by navigating to this page from a different page. This is a known issue with Kafka.
HERC-2994	In some cases, the incorrect IP address shows up in the consumer group on Event Broker Manager when ESM consumes topics from EB in an HA environment. This issue is specific to the underlying open source third party tool, Event Broker Manager, and ESM HA deployment. Events are in fact being processed correctly; this is just a monitoring issue.

Open Issues

This release contains the following open issues.

Key	Release Note Description	
INST-836	The arcsight-installer-worker.sh script does not check that the unzip package is installed on a worker node before attempting to install the worker node. If the unzip package is not installed, arcsight-installer-worker.sh will fail on step 8 with the following errors: bash: unzip: command not found bash: /root/arcsight-installer-worker/install: No such file or directory Manually install the unzip package on worker nodes before using arcsight-installer-worker.sh to install the worker node.	
INST-824	After deploying Kubernetes on a worker node, the deployment ZIP file is left as /tmp/arcsight-installer-worker.zip on the worker node, consuming about 800 MB of disk space. In addition, a directory containing the extracted contents of that ZIP files is left as arcsight-installer-worker in the home directory of the user that ran the installer, consuming about 2 GB of disk space. Neither this file nor this directory are automatically deleted after the installation is completed, nor are they deleted when Kubernetes is uninstalled. Workaround:You can delete this file and directory manually to reclaim the disk space.	
INST-813	In some cases, the undeploy and redeploy of Event Broker will fail, with Event Broker containers in a crash loop.	
INST-797	The pod statuses displayed on the UI do not always correspond to the ones you can see running 'kubceclt get pods'. The pod statuses we display on UI (at the moment) could be - Running, Pending, Failed. The statuses you see in kubectl are the container statues which are in most of the cases will be transformed to Pending or Running in the UI.	
INST-34	When you change or set certain configurations in the ArcSight Installer application, you will see the message "All configuration saved successfully". This means that the property has been changed. However, the change requires that pods be restarted for the configuration to propagate completely. The process of restarting pods can take some time and you may not see the change in the application immediately.Use the kubectl get pods -n arcsighteventbroker1 command on the master node to check the status of pod restarts to ensure that all pods have restarted fully (reached "Running" status) before verifying that the change was applied.	

Key	Release Note Description	
EB-909	If the stream processor stops processing events and you see “ConcurrentModificationException” with the exception stack trace pointing to “org.apache.kafka.common.internals.PartitionStates.partitionSet”, then this is known Kafka defect KAFKA-4950. Workaround: Rrestart the affected stream processor using the 'kubectl delete' command. Example if c2av stream processor is affected : # kubectl delete eb-c2av-processor-927505239-xc1ol -n arcsighteventbroker1 Example if routing stream processor is affected : # kubectl delete eb-routing-processor-0 -n arcsighteventbroker1	
EB-880	In some cases, after sending events to the eb-cef topic, a message is returned: Yikes! Ask timed out on [ActorSelection[Anchor(akka://kafka-manager-system/), Path(/user/kafka-manager)]] after [5000 ms] Workaround: Restart Event Broker Manager.	
EB-859	Occasionally, there may be no event flow from eb-cef topic to eb-internal-avro topic. In the c2av log, runkubectl logs eb-c2av-processor-0 -n arcsighteventbroker1 | grep 'Failed to lock'An exception may be found in the log, such as "LockException like "org.apache.kafka.streams.errors.LockException: task [0_N] Failed to lock the state directory for task 0_N" This is known issue for Kafka.https://issues.apache.org/jira/browse/KAFKA-5167https://issues.apache.org/jira/browse/KAFKA-5485 Workaround: Restart c2av POD by invoking:kubectl delete pod eb-c2av-processor-0 -n arcsighteventbroker	Actions
EB-631	In some cases, when Kafka goes down and then recovers, there can be a difference in the event count of CEF and Avro topics. Under failure conditions it is expected that there may be data duplication since messages are re-delivered. The redelivery leads to some duplicate events. This is a known Kafka behavior.	
EB-630	Kafka version shown on the Event Broker manager is incorrectly shown as 0.10.1.0, when it should be should be 0.11.0.0	

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 system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (Event Broker 2.10)

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 arc-doc@hpe.com.

We appreciate your feedback!