Hewlett Packard
Enterprise

HPE Security ArcSight Data Platform Event Broker

Software Version: 2.0

Release Notes

April 17, 2017

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://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Event Broker 2.0 Release Notes

The ADP Event Broker 2.0 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 Kafka broker or cluster of brokers, you can use ADP SmartConnectors to publish data, and subscribe to that data with ADP Logger, ArcSight ESM, ArcSight Investigate (via Vertica), Apache Hadoop, or your own consumer.

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

What's New in this Release

The HPE Security ArcSight Event Broker 2.0 release introduces the following new features and enhancements.

- **New Data Format Support:** In addition to ArcSight Logger, new consumer types can now be configured to operate with Event Broker and process new data formats, including:
  - ArcSight Investigate 1.0 (via Vertica): Avro format
  - ArcSight ESM 6.11.0: Binary format
  - Third-party products, such as Hadoop
  - Customer-created applications that can read CEF.
- **ArcMC Management:** Event Broker can now be managed and monitored by ArcSight Management Center (ArcMC). ArcSight Event Broker management includes route and topic creation, as well as health and status parameter monitoring. Monitored parameters for Event Broker include CPU Usage, Memory, Disk Usage, Event Broker Throughput, Total EPS In, Event Parsing Error, Stream Processing EPS, and Stream Processing Lag.
- **Kafka Upgrade:** Event Broker 2.0 uses an upgraded version of Kafka (0.10.1.0)

For details about these features, see the ArcSight Event Broker 2.0 Administrator's Guide, available from the ArcSight Product Documentation Community on Protect 724.

For details on the changes to Kafka 0.10.1.0, see the Kafka Release Notes.

Supported Platforms and Browsers

For details on Event Broker 2.0 platform and browser support, refer to the ADP Support Matrix document available from the ArcSight Product Documentation Community on Protect 724.

Event Broker Documentation

In addition to these Release Notes, the following documents are available in PDF format for download from the ArcSight Product Documentation Community on Protect 724.

- *ArcSight Data Platform 2.1 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 2.0 Administrator's Guide:* Describes how to configure, and manage the ADP Event Broker. Available with your download in PDF format.
- *Event Broker Deployment Guides:* Describe how to deploy Event Broker in standalone (ADP) and as part of an Investigate deployment.

Known Limitations

Event Broker is known to have the following limitations.

Issue	Description
HERC-3264	In some cases, there can be a long delay before deployment is confirmed or denied. Please give the process time to complete. To check progress, connect to the Kubernetes master node and run the 'kubectl get pods' command to check the status of all pods.
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.
HERC-788	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.

Open Issues

This release contains the following open issues.

HERC-3382	If any of the Kafka nodes becomes unresponsive, as reported by Event Broker Manager as a “Yikes! Ask timed out on [ActorSelection[Anchor(akka://kafka-manager-system/),Path(/user/kafka-manager)]] after [5000 ms]” or indicated by a drop in event processing metrics in ArcMC, then it could be because of a known Kafka issue (https://issues.apache.org/jira/browse/KAFKA-3994). This requires a restart of the unresponsive Kafka node.
HERC-3347	The Add Host command in the Vertica Database Scheduler supports adding one host IP at a time. When using the Add Host command to add hosts to the Vertica database cluster, add one host IP at a time rather than a series of host IPs separated by commas.
HERC-3278	In some cases, Kafka nodes may not come back up after being stopped using ./kube-stop.sh Workaround: run the update_kubevaulttoken manually, and restart kubernetes-vault pod ./update_kubevaulttoken kubectl --namespace=core delete pod kubernetes-vault-3459593811-x70pz
HERC-3232	An error is returned when configuring a connector to send events to Event Broker, and you select the combination 'Logger 6.4 or higher/IPV6/Investigate' and enter eb-cef topic name value. This is a known issue and you can click Yes to continue.
HERC-3231	During the deployment of Event Broker on a fresh system, a set of 6 predefined Event Broker topics and 2 internal Kafka topics are created. There are certain times when a timing issue might result in only a subset of the 6 pre-defined topics being created. If this happens, connect to the master node, delete the web service pod using the kubectl command. The pod will be recreated and restarted automatically. All topics should be created as expected.
HERC-2949	Kafka version shown on the Event Broker manager is incorrectly shown as 0.10.0,0. This should be 0.10.1.0.
HERC-2928	When you change or set certain configurations (such as database configuration or number of replicas) 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 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.
HERC-954	In some circumstances, the Kafka Scheduler may stop after rebooting a Vertica node that does not have the Scheduler installed. No data is lost. Workaround: Restart Kafka Scheduler.

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 2.0)

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!