Hewlett Packard
Enterprise

# HPE Security ArcSight Data Platform Event Broker

Software Version: 2.01

Release Notes

June 13, 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 2.01 Release Notes

The ADP Event Broker 2.01 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 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 2.01 release resolves issues present in Event Broker 2.0. For details about issues resolved in this release, see "Fixed Issues" on the next page.

## Supported Platforms and Browsers

For details on Event Broker 2.01 platform and browser support, refer to the ADP Support Matrix document available from the ArcSight 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 2.11 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 2.01 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 mode (part of ADP) and as part of an ArcSight Investigate deployment.

# Fixed Issues

This release contains the following fixed issues.

| Issue | Description |
|---|---|
| EB-146 | The Avro transformation was inserting the string "NONE" for CEF values that were not encountered in a CEF message. This is incorrect, as changed the meaning of the CEF data. The value used will instead be 'null.' |
| EB-103 | In some cases, Kafka nodes could become 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. This issue has been resolved. |
| EB-30 | Because of a timing issue, on some deployments of Event Broker on a fresh system, a subset of 6 predefined Event Broker topics could be created, instead of the expected 6. This issue has been resolved and all topics will be created as expected. |

# 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. |
| 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. |
| 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. |
| INST-66 | 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. |

# Open Issues

This release contains the following open issues.

| Issue | Description |
|---|---|
| INST-34 | 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. |
| INST-18 | 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. |
| INST-12 | In some cases, Kafka nodes may not come back up after being stopped using ./kube-stop.shWorkaround: run the update_kubevaulttoken manually + restart kubernetes-vault pod./update_kubevaulttokenkubectl --namespace=core delete pod kubernetes-vault-<random string> |
| EB-678 | 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. |
| EB-641 | If you invoke Investigate from ESM, and the query does not return results, it is possible that there are differences in leading and trailing white spaces between the values in Investigate and ESM.Workaround:Check whether the string values in ESM contain leading or training white spaces.If they do, manually change the Investigate query to use the 'contains' operator and remove leading and trailing white space from the value.Rerun the query.This issue will be addressed in future releases. |
| EB-630 | The Kafka version shown on the Event Broker manager incorrectly shown as 0.10.1.0. It should show 0.10.1.1. |

# 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 2.01)**

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!