Hewlett Packard
Enterprise

HPE Security ArcSight Event Broker

Software Version: 2.11

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 2.11 Release Notes

The ArcSight 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.

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.

What's New in this Release

Event Broker 2.11 addresses and resolves issues found in Event Broker 2.10. For a list of issues fixed in this release, see Fixed Issues.

This version of Event Broker supports upgrade from either Event Broker 2.02 or Event Broker 2.10.

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 Support Matrix:* Provides integrated support information such as platform and browser support for ADP ArcMC, Event Broker, and SmartConnectors.
- *Event Broker Administrator's Gide* Describes how to configure, and manage ArcSight Event Broker.
- *Event Broker Deployment Guide:* Describes how to deploy and configure Event Broker.

Upgrading from Event Broker 2.02 to Event Broker 2.11

The process of upgrading Event Broker from version 2.02 to version 2.11 consists of two steps: first, upgrading the ArcSight Installer from version 1.10 to 1.30, and second, upgrading to Event Broker 2.11 itself.

Note: The complete upgrade process may take up to 2 hours.

Prerequisites

The technical prerequisites for upgrade are the same as for a fresh install. Refer to the Event Broker Deployment Guide for a list of pre-requisites and configuration steps required for a fresh installation.

Before Any Upgrade

Make sure that no proxy is used between the master and worker nodes. Verify that the IP addresses of the master and worker nodes are included in the $no_proxy environmental variable on all nodes.

Upgrading from Installer 1.10 to Installer 1.30

1. Download the file `arcsight-installer-upgrade-1.10to1.30.zip` and copy the ZIP archive to the master node (for example, to `/opt/arcsight/upgrade/arcsight-installer-upgrade-1.10to1.30.zip`)

2. Download new version of ArcSight installer and copy the ZIP archive to the master node (for example, to `/opt/arcsight/upgrade/arcsight-installer-1.30.<buildnumber>.zip`)

3. Download the tar files with Event Broker 2.11 images.(The images will be automatically uploaded to the local repository after platform upgrade.)

4. Unzip `arcsight-installer-upgrade-1.10to1.30.zip`

5. Change the working directory to the upgrade folder:

```
cd /opt/arcsight/upgrade/arcsight-installer-upgrade-1.10to1.30.zip
```

6. Run the upgrade script, with parameters `-i` for the location to zipped new version of the ArcSight installer, `-c` for the cluster name, and and optionally `-f` for the location of the tar files with new Event Broker version. For example:

```
sh upgrade.sh -i arcsight-installer-upgrade-1.10to1.30.zip -c <EB_cluster_
name>
```

or

```
sh upgrade.sh -i /opt/arcsight/upgrade/arcsight-installer-upgrade-
1.10to1.30.zip -c <EB_cluster_name> -f /opt/arcsight/upgrade/images
```

You will be prompted for the cluster password.

This will upgrade platform on the master node and all workers. If the -f parameter was specified, images with products will be uploaded to local repository.

Upgrading Event Broker

If the `-f` parameter was used, and upgrade finished successfully, log in to the new ArcSight Installer at the URL `<master_hostname>:5443`. Then, on the **Deployment** tab, next to **Event Broker**, click **Upgrade**.

If the -f parameter was not used, use `downloadimages.sh` and `uploadimages.sh` from `/opt/arcsight/kubernetes/scripts/` and then upgrade Event Broker as described above.

Upgrading from Event Broker 2.10 to Event Broker 2.11

The process of upgrading Event Broker from version 2.10 to version 2.11 consists of two steps: first, upgrading the ArcSight Installer from version 1.20 to versio n 1.30, and second, upgrading to Event Broker 2.11 itself.

Note: The complete upgrade process may take up to 2 hours.

Prerequisites

The technical prerequisites for upgrade are the same as for a fresh install. Refer to the Event Broker Deployment Guide for a list of pre-requisites and configuration steps required for a fresh installation.

Before Any Upgrade

Make sure that no proxy is used between the master and worker nodes. Verify that the IP addresses of the master and worker nodes are included in the $no_proxy environmental variable on all nodes.

Upgrading from Installer 1.20 to Installer 1.30

1. Download a new version of ArcSight Installer 1.30, and copy the archive to the master node of your cluster (e.g. to `/opt/arcsight/upgrade/arcsight-installer-1.30.54-master.zip`)

2. Extract the zipfile

```
cd /opt/arcsight/upgrade
```

```
unzip arcsight-installer-1.30.54-master.zip
```

3. Change the working directory to the upgrade folder.

```
cd /opt/arcsight/upgrade/arcsight-installer-1.30.54-master
```

4. Run the upgrade script with parameter --patch

```
./upgrade.sh --patch
```

5. Wait for the changes to be fully propagated while the upgrade is performed (arcsight-installer, suite-installer, and suite-db must be fully running).

6. After completion, launch the Installer and verify the application version of 1.30 on the login dialog.

Upgrading Event Broker

1. Download the Event Broker 2.11 images.

2. For offline deployment, download the Event Broker tar files from the Micro Focus site. Extract to `/opt/arcsight/upgrade/offline/eventbroker-2.11`

3. Upload images for Event Broker to the local Docker repository.

```
cd /opt/arcsight/kubernetes/scripts
```

```
./uploadimages.sh --suite eventbroker --dir
/opt/arcsight/upgrade/offline/eventbroker-2.11
```

3. Login to the new version of the ArcSight Installer at the URL `<master_hostname>:5443`. The default username is "admin" with default password "cloud". Change the default password on first login. Then, on the **Deployment** tab, next to **Event Broker**, click **Upgrade**.

Fixed Issues

This release contains the following fixed issues.

Key	Description
INST-860	Previously, when you deployed a product and a long-running background process was not finished when user session was valid, deployment would fail without notification. This issue has been resolved.
INST-824	After the deployment process, nearly 3 GB of unneeded files would be left behind and need manual deletion. These files are now deleted automatically.
INST-801	During kube redeploy or restart it was possible that some PODs were in state "MatchNodeSelector" and were not deleted by Kubernetes when new one was created, so some death PODs were in products namespaces and user had to delete them by kubectl. Now they are deleted when kubernet starts (kube-poststep.sh which is registered to kubernet service)
INST-790	In some cases, nginx-ingress-controller and kube-dns could go into a crash loop. This issue has been resolved.
INST-788	Previously, when you deployed a product and a long-running background process was not finished when user session was valid, deployment would fail without notification. This issue has been resolved.
EB-953	The API is updated to reflect the correct product version string displayed on ArcMC.
EB-910	A limitation has been resolved in using multiples source topics for event routing.
EB-866	Event Broker version is now displayed on the Deployment UI.

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	Description
INST-936	Issue: When attempting to upgrade the 1.10 or 1.20 ArcSight Installer, running the arcsight-installer-worker.sh fails. The arcsight-master.properties does not exist. Workaround: -Copy “/opt/arcsight/installer/k8s/arcsight-k8s.properties” to “/opt/arcsight/kubernetes/scripts/arcsight-master.properties”.- 1.10 -> 1.30 cp /opt/arcsight/upgrade/installer_backup/k8s/arcsight-k8s.properties /opt/arcsight/kubernetes/scripts/arcsight-master.properties add property "POD_CIDR=172.77.0.0/16" at the end of arcsight-master.properties: echo "POD_CIDR=172.77.0.0/16" >> /opt/arcsight/kubernetes/scripts/arcsight-master.properties 1.20 -> 1.30 cp /opt/arcsight/download/arcsight-installer-1.20.6/arcsight-k8s.properties /opt/arcsight/kubernetes/scripts/arcsight-master.properties
INST-895	In some cases, on RHEL 7.4 and IPv6-disabled systems, the NFS server may crash. This is related to the rpc.socket issue described here: https://access.redhat.com/solutions/2798411.
INST-840	Issue: Unable to connect to the ArcSight Installer UI. Resolution:You can recover from this state by running kube-restart.sh (/opt/arcsight/kubernetes/bin/kube-restart.sh). Run kube-restart.sh on node/master where services/pods are failing. This script stops core platform services and start it again.
INST-797	Issue:The pod statuses displayed on the UI do not always correspond to the ones you can see running 'kubceclt get pods'. The pod statuses displayed in the 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. Workaround:None.

Key	Description
EB-960	Issue: The namespace for some Kubernetes pods may not match the namespace listed in the documentation. This would cause commands such as kubectl logs <pod name> -n <namespace> to report that the pod can't be found. Resolution: You can get the list of all the pods with their namespaces via the command: kubectl get pods --all-namespaces -o wide. Depending on the original Event Broker version, you may see some pods with in either the eventbroker1 or arcsighteventbroker1 namespaces. If Event Broker was upgraded from version 2.0.2 to 2.11, the namespace is eventbroker1, however if Event Broker was upgraded from version 2.10 to 2.11, the namespace is arcsighteventbroker1.
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 the known Kafka defect KAFKA-4950. Work around is to restart the affected stream processor using the 'kubectl delete' command. Example if c2av stream processor is affected : kubectl delete eb-c2av-processor-927505239-xc1ol -n arcsighteventbroker1Example 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
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 2.11)

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!