Hewlett Packard
Enterprise

HPE Security ArcSight Event Broker

Software Version: 2.11

Deployment Guide

February 9, 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

Revision History

Date	Description
February 9, 2018	Initial release of this document.

Contents

Chapter 1: Overview

This document describes how to deploy ArcSight Event Broker using the ArcSight Installer.

About ArcSight Event Broker

ArcSight Event Broker centralizes event processing and enables topic sorting and event routing, which helps you to scale your ArcSight environment, and opens ArcSight event data to third-party solutions. It enables you to take advantage of scalable, highly available, multi-broker clusters for publishing and subscribing to event data. Event Broker integrates with ArcSight connectors, Logger, ESM, and ArcSight Investigate; can be managed and monitored by ArcMC; and is foundational for using ArcSight ADP products.

- The ArcSight Data Platform Event Broker provides a packaged version of Apache Kafka. After you install and configure an Event Broker Kafka broker or cluster of broker nodes, you can use ADP SmartConnectors to publish data, and subscribe to that data with ADP Logger, ArcSight ESM, Apache Hadoop, or your own consumer.

  Event Broker manages the distribution of events in topics to which consumers can subscribe.

  Event Broker supports both CEF 0.1 and 1.0.

  - CEF 0.1 is the legacy ArcSight CEF version that supports IPv4 IP addresses available with SmartConnector version 7.4 and earlier.
  - CEF 1.0, available with SmartConnector version 7.5 and later, supports IPv4 and IPv6 addresses. (Note, however, that although it supports IPv6 event content, Event Broker does not support installation on IPv6 systems.)
- There are two Event Broker default topics you can configure your destinations to connect to: eb-cef and eb-esm. The eb-cef topic accepts CEF text, and the eb-esm accepts binary security events, which is the format consumed by ESM. In addition, you can create new custom topics to which your SmartConnectors can connect.
- ArcSight ESM can be configured as an Event Broker consumer.

Deployment Process Outline

The complete process of deploying Event Broker includes these steps:

1. **Preparation.** Prepare and provision your network and dedicated hosts.
2. **Install the ArcSight Installer.** The ArcSight Installer is the platform used to install other ArcSight products.

3. **Deploy Event Broker.** You can deploy Event Broker either by an online deployment, where you download the product images from the online Docker Hub, or an offline deployment, where you download the product images from your private Docker registry.

Each of these steps is explained in the following sections.

Chapter 2: Deployment Planning and Prerequisites

This section discusses the following preparatory steps to take before deployment.

System Requirements

Installation of the ArcSight Installer platform has the following system requirements.

- **Disk Space:** Required disk space for the master node and each worker node is as follows:

Partition	Master Node	Worker Node	Notes
`/opt`	200 GB	150 GB	Installation in `/opt` is required.
`/var`	10 GB	10 GB	
`/root`	N/A	10 GB	

- **Operating System:** Supported operating systems are discussed in the ADP Support Matrix, available from Protect724.
- SELinux must be disabled.
- The file system type must be ext4.
- The admin needs to have root permissions. All commands in the installer process must run as a user with root privileges. (Event Broker may not be installed by a non-root user.)
- The following packages need to be installed using `rpm/yum` on the master and all workers:

  ```
  yum install -y unzip nfs-utils libseccomp libtool-ltdl
  ```
- Java 8 JRE must be present on the master node (version 1.8 update 131 or later).

Network Preparation

To prepare your network for the deployment process, take the following steps.

- **FQDN:** Ensure that each master and worker node is configured with an FQDN (fully-qualified domain name), and is in the same subnet.

NAT Environments: Event Broker uses the host system FQDN for Kafka `advertised.host.name`. If FQDN resolves in the NAT environment, then producers and consumers will function correctly. If there are network-specific issues resolving FQDN through NAT, then DNS will need to be updated, or update the `advertised.host.name` in the Kafka pod.

- **DNS Resolution:** Ensure host name resolution through DNS across all systems, including correct forward and reverse DNS lookups. Host name resolution may not be performed through `etc/hosts`. (Although it supports IPv6 event content, Event Broker does not support installation on IPv6-only networks.)
- **Internet Access for Online Deployment:** If you are performing an online deployment, enable internet access in order to download the product container images.
- **Proxy Environment (if needed):** If your organization's network has a proxy, define the proxy environment variable on all servers. Define these variables for each user, and not system-wide.

Systems with NIC teaming/bonding are not supported for installation of Event Broker.

Event Broker Node Provisioning (master and workers)

The Event Broker cluster may have one master and two (or more) worker nodes. Multi-master installation is not supported at this time.

More information on Event Broker system sizing requirements can be found in the Event Broker Administrator's Guide.

Prepare Master Node

For your master node, provision a dedicated host which meets the system requirements.

Note: The NFS server on the master node cannot be used for any purposes other than the ArcSight Installer, or ArcSight applications deployed on the cluster using the ArcSight Installer. *An NFS server on an external server is not supported.*

Prepare Worker Nodes

For your worker nodes, provision two or more dedicated hosts which meet the system requirements.

Enabling SSH

In order to enable the master node to communicate with worker nodes over SSH, generate a key pair on the master node and copy the public key to each worker node. Run the following command on the master node to generate the key pair:

```
ssh-keygen -t rsa
```

Run the following command on master node to copy the generated public key to every worker node you prepared:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub root@<worker_fqdn_or_ip>
```

SSH access only needs to be enabled for installation (or upgrade). If required by your security policy, you can disable SSH access after installation or upgrade operations are complete.

Increasing per-user process limits

1. Do the following on every master and worker node.

   Open the file `/etc/security/limits.d/20-nproc.conf`.

   If you do not already have a `/etc/security/limits.d/20-nproc.conf` file, create one (and the `limits.d` directory, if necessary).
2. Add the lines below, including the leading asterisks.

   ```
   * soft nproc 10240
   * hard nproc 10240
   * soft nofile 65536
   * hard nofile 65536
   * soft core unlimited
   * hard core unlimited
   ```
3. Reboot all master and worker nodes. Nodes can be rebooted in any order.
4. Verify that all nodes are up and running by running the following command.
   `ulimit -a`

Prepare Logical Volumes for Cluster Nodes (Optional)

Follow the steps below on each cluster node to ensure that you have enough logical volumes for the ArcSight Installer platform installation. You can choose any volume group name, logical volume name and disk location address for your installation, according to your system.

Note: This is an optional step.

Prepare a physical disk for the Kubernetes cluster nodes. The physical host of your system must meet the system requirements.

1. Create a volume group by running the following command:

```
vgcreate [volume group name] [logical volume name]
```

For example: `vgcreate core-platform /dev/sdb`

2. Create a logical volume for the ArcSight Installer installation by running the following command:

```
lvcreate -l 100%FREE -n [logical volume name] [volume group name]
```

For example,to utilize 100% of the volume group:

```
lvcreate -l 100%FREE -n mylv core-platform
```

3. Activate the volume group by running the following command:

```
vgchange -ay [volume group name]
```

For example:

```
vgchange -ay core-platform
```

4. Format the file system by running the following command:

```
mkfs.ext4 [logical volume path]
```

For example: `mkfs.ext3 /dev/core-platform/mylv`

5. Mount the volumes under the folder in which you will install the ArcSight Installer by running the following command:

```
mount [logical volume path] [platform installation folder]
```

For example:

```
# mount /dev/core-platform/mylv /opt/arcsight/kubernetes
```

Configuring the Firewall

The following firewall ports need to be open for the correct installation and operation of Event Broker.

- **Web Installer:** 5443 on the Master node.
- **Kubernetes:** 2379,2380,3000,4001,4194,5000,5443,8080,8088,8200,8285,8443,10248-10252,10255
- **NFS:** 111,2049,20048,37189
- **Event Broker:** 2181, 9092, 9093, 39092,39093,32181

- **CEB:** (alpha feature only, not for production) 39001-39010
- **CAdvisor:** 4194

Avoiding Possible Conflicts with Network Ranges

The ArcSight Installer configures firewall settings during setup (assuming `firewalld.service` is up and running) on both Kubernetes master and worker nodes.

The Installer will use the following network ranges by defaults:

- 172.16.0.0/16: Subnetwork of 65,536 addresses for operation of Kubernetes pods with containers running in them. Each pod will operate with /24 subnetwork from the following range.
- 172.30.78.0/24: Subnetwork of 256 addresses for operation of Kubernetes services, including internal Kubernetes DNS service, located on pod 172.30.78.78.

For best results, make sure your network is conflict-free with the /16 and /24 ranges of addresses. If those are occupied or inaccessible due to network configuration, make sure to utilize another range by making corresponding changes to `POD_CIDR, SERVICE_CIDR` and `DNS_SVC_IP` parameters in the `arcsight-installer-master.sh` script before executing it.

Proxy settings

Configure the `http_proxy, https_proxy`, and `no_proxy` environmental variables on your system for each user.

> Note: Ensure no proxy settings are specified in `/etc/profile.d/proxy.sh` or any other files in this folder.

Network Time Protocol Requirements

`chrony` is a versatile implementation of the Network Time Protocol (NTP) and keeps the system clock of each cluster node in sync. A network time server must be available. `chrony` is installed by default on some versions of RHEL/CentOS. Verify `chrony` configuration by using the command:

```
chronyc tracking
```

If `chrony` is not installed on your system, install it with the following procedure.

1. `yum install chrony`
2. Start `chronyd` to start and enable the chrony daemon.

   ```
   systemctl start chronyd
   systemctl enable chronyd
   ```
3. Verify that `chrony` is operating correctly.

   ```
   chronyc tracking
   ```

Plan encryption modes

Before installing Event Broker, determine the encryption mode you want to use to encrypt communications between ArcSight components. Set up the other ArcSight components with the encryption mode you intend to use before connecting them to the Event Broker. The security mode of systems connected to Event Broker (Consumers, Producers, ArcMC) must be the same as the security mode set for Event Broker. Changing encryption modes after Event Broker has been deployed will require system down time. If you do need to change the security mode after Event Broker deployment, see the *Event Broker Administrator's Guide*.

Product	Preparations needed	Open ports	Supported encryption modes	Guidance documentation
ArcMC	Install ArcMC before and Event Broker installation.	38080	• TLS • FIPS • ClientAuth	*ArcMC Administrator's Guide*
ArcSight SmartConnectors	ArcSight SmartConnectors and ArcMC onboard connectors can be installed and running prior to installing and Event Broker. FIPS mode setup is not supported between Connector version 7.5 and Event Broker. TLS and ClientAuth are the only encryption methods supported between SmartConnector version 7.5 and Event Broker.	9093	• TLS • FIPS • ClientAuth	*SmartConnector User Guide* *ArcMC Administrator's Guide*
ArcSight ESM (optional)	ArcSight ESM can be installed and running prior to installing and Event Broker.	9093	• TLS • FIPS • ClientAuth	*ESM Installation Guide* *ESM Administrator's Guide*
ArcSight Logger (optional)	ArcSight Logger can be installed and running prior to installing Event Broker.	9093	• TLS • FIPS • ClientAuth	*Logger Administrator's Guide*

Activating your Docker Hub Account (Online Deployment Only)

Docker Hub is cloud-based registry service which can store manually pushed images, including ArcSight Event Broker product images.

To complete an online deployment, you must use or create a valid company Docker ID (hub.docker.com) to grant you instant and secure cloud access to Event Broker software. If you do not have an existing Docker account, please follow the steps below to register a Docker ID.

Note: If you plan to perform an offline deployment, you will download images from the ArcSight software entitlement site, and this step is not necessary.

1. Go to https://hub.docker.com
2. Create a Docker ID, enter your company email address, and create a password.
3. Click **Sign Up.**
4. Click the **Confirm Your Email** link in the email you received from Docker to confirm your Docker ID account.
5. Go to https://hub.docker.com to verify that you can log into Docker Hub.
6. After login, click your Docker ID on the top right of the page. Click **Settings** and take a screenshot to include your Docker ID and the linked email address.

Please email your corresponding regional contact below with your registered Docker ID as well as the screenshot for us to enable your Docker Account. Based on your region and existing entitlements, contact your licensing team to enable your Docker ID:

- For the Americas region, contact dockersupport.ams@hpe.com
- For the APJ region, contact dockersupport.apj@hpe.com
- For the EMEA region, contact dockersupport.emea@hpe.com

Chapter 3: Installing the ArcSight Installer and Deploying Event Broker

Once your planning is complete and prerequisites are met, you are ready to install the ArcSight Installer and then deploy Event Broker. The following topics are discussed in this section.

Installing the ArcSight Installer

The ArcSight Installer enables the deployment of ArcSight products, such as Event Broker.

1. Log in in to the master node as the root user (`sudo` to root).
2. Download the installation zip file from the ArcSight software entitlements site.
3. Unzip the installation zip file to a secure location on the master node.
4. Change into the directory created.

   ```
   cd arcsight-installer-<version>
   ```
5. Install the platform on the master node.

   ```
   ./arcsight-installer-master.sh --REGISTRY_ORGNAME=arcsightsecurity
   ```
6. Install the platform on each worker node with the following commands:

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

   ```
   ./arcsight-intaller-worker.sh -w <Worker-Node_IPv4>
   ```

   where `<Worker-Node_IPv4>` is the distinct IPv4 address of the worker node.

You may now perform either an online deployment or an offline deployment.

Deploying ArcSight Event Broker (Online Deployment)

Once the ArcSight Installer is installed, you are ready to deploy ArcSight products supported by the installer, such as Event Broker.

Follow these steps to perform an online deployment, where you will be downloading the product images from Docker. Ensure you have activated your Docker account before proceeding.

Log in and Change Password

1. Browse to the master node at `https://<master_node_fqdn_or_ip>:5443.`
2. Enter the default credentials *admin/cloud*. After the first successful login, you will be forced to change the admin password to a non-default value.
3. On the **Node Management** page, make sure that one or more workers is up and running. All of the nodes should have status *READY*

Edit `arcsight-installer.properties` (Optional)

If you need to pre-configure some product's features before starting deployment (such as FIPS or Client Authentication) open `/opt/arcsight/installer/arcsight-installer.properties` in a text editor, and update and edit the values accordingly. See "arcsight-installer.properties" on page 22 for more information.

Label Nodes

You will need to label each node for its functionality. Perform node labeling from the master node.

1. To label a node for Kafka, run `kubectl label --overwrite node {node_ip} kafka=yes`
2. To label a node for Zookeeper, run `kubectl label --overwrite node {node_ip} zk=yes`

Make sure that the number of the Kafka and ZooKeeper nodes you labeled correspond to the eb-kafka-count and eb-zookeeper-count properties from /opt/arcsight/installer/arcsight-installer.properties. These must be an odd number; the default value is 3. Verify that labels were applied correctly on the **Node Management** page `https://{master_fqdn_or_ip}:5443/nodeManagement`

Note: If the `kubectl` command is returning a refused or time-out connection, make sure proxy is unset before repeating the command.

Download Product Images from Docker

You can now download the Event Broker product images for deployment from Docker. To download Event Broker, run the following:

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

```
./downloadimages.sh --suite eventbroker -r docker
```

You are prompted for Docker credentials. (See "Activating your Docker Hub Account (Online Deployment Only)" on page 11 for details on how to create your Docker Hub account, if you have not already done so.)

Once the images are downloaded, run `./uploadimages.sh --suite eventbroker` to upload them to the local Docker registry.

Deployment

Browse to the **Deployment** page. The list of products should be displayed with status *OFF*

- Pick an Event Broker version to deploy and and click **Deploy**. Deployment status will be changed to *IN PROGRESS*.
- Once the product deployment is finished, the status will be changed to *DEPLOYED*. Please give the process some time to complete. This can take a few minutes. A popup window will show the list of pods, with status and memory usage. To check the pod status, click **Details**. Once all pods have status *RUNNING*, the product can be considered ready to configure and use.
- The **Undeploy** button will remove a product and all its containers from Kubernetes. (An undeployment may take a similar amount of time as a deploy, from 2-5 minutes.)

Configuration

To configure ArcSight Event Broker go to **Configuration > ArcSight Event Broker.** Change the required configuration parameters and click **Save**.

After changing a product setting, one or more containers of the product will be restarted in the cluster. Depending on which pods need to restart, there may be a brief interruption to some running applications.

Licensing

You will need to take additional steps regarding licensing Event Broker, as explained under "AutoPass Licensing" on page 18.

Deploying ArcSight Event Broker (Offline Deployment)

Once the ArcSight Installer is installed, you are ready to deploy ArcSight products supported by the installer, such as Event Broker.

Follow these steps to perform an offline deployment, where you will be downloading the product images from the ArcSight software entitlement site.

Verifying the Download: HPE provides a digital public key to enable you to verify that signed software you download from the software entitlement site is indeed from HPE and has not been manipulated in any way by a third party. Visit the following site for information and instructions: https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

Log in and Change Password

1. Browse to the master node at `https://<master_node_fqdn_or_ip>:5443.`
2. Enter the default credentials *admin/cloud*. After the first successful login, you will be forced to change the admin password to a non-default value.
3. On the **Node Management** page, make sure that one or more workers is up and running. All of the nodes should have status *READY*

Edit `arcsight-installer.properties` (Optional)

If you need to pre-configure some product's features before starting deployment (such as FIPS or Client Authentication) open `/opt/arcsight/installer/arcsight-installer.properties` in a text editor, and update and edit the values accordingly. See "arcsight-installer.properties" on page 22 for more information.

Label Nodes

You will need to label each node for its functionality. Perform node labeling from the master node.

1. To label a node for Kafka, run `kubectl label --overwrite node {node_ip} kafka=yes`
2. To label a node for Zookeeper, run `kubectl label --overwrite node {node_ip} zk=yes`

Make sure that the number of the Kafka and ZooKeeper nodes you labeled correspond to the eb-kafka-count and eb-zookeeper-count properties from /opt/arcsight/installer/arcsight-installer.properties. These must be an odd number; the default value is 3. Verify that labels were applied correctly on the **Node Management** page `https://{master_fqdn_or_ip}:5443/nodeManagement`

Note: If the `kubectl` command is returning a refused or time-out connection, make sure proxy is unset before repeating the command.

Prepare Product Images

1. Download the Event Broker tar archive `arcsight-eventbroker-XX.tar` to a secure location; for example, `/opt/arcsight/download/arcsight-eventbroker-XX.tar.`

2. Unpack the product archive

```
cd /opt/arcsight/download
```

```
tar -xvf arcsight-eventbroker-XX.tar
```

The `/opt/arcsight/download/eventbroker` folder will contain the product images. Verify the download as explained above.

Upload to the Local Registry

Once verified, upload the images to the local registry as follows:

```
cd /opt/arcsight/kubernetes/scripts
./uploadimages.sh -s eventbroker -d /opt/arcsight/download/eventbroker
```

Deployment

Browse to the **Deployment** page. The list of products should be displayed with status *OFF*

- Pick an Event Broker version to deploy and and click **Deploy**. Deployment status will be changed to *IN PROGRESS*.
- Once the product deployment is finished, the status will be changed to *DEPLOYED*. Please give the process some time to complete, which can take a few minutes. A popup window will show the list of pods, with status and memory usage. To check the pod status, click **Details**. Once all pods have status *RUNNING*, the product can be considered ready to configure and use.
- The **Undeploy** button will remove a product and all its containers from Kubernetes. (An undeployment may take a similar amount of time as a deploy, from 2-5 minutes.)

Configuration

To configure ArcSight Event Broker go to **Configuration > ArcSight Event Broker.** Change the required configuration parameters and click **Save**.

After changing a product setting, one or more containers of the product will be restarted in the cluster. Depending on which pods need to restart, there may be a brief interruption to some running applications.

Licensing

You will need to take additional steps regarding licensing Event Broker, as explained under "AutoPass Licensing" below.

AutoPass Licensing

Event Broker ships with a 30-day instant-on evaluation license, which will enable functionality for 30 days after installation. In order for Event Broker to continue working past the initial 30-day evaluation period, you will need to apply the ADP ArcMC license to Event Broker.

Note: It is **strongly** recommended that you do not use the evaluation license for production servers. Plan and apply the proper license before the 30-day evaluation period has expired.

For details on how to apply a new license file to Event Broker, see the Licensing chapter of the *Event Broker Administrator's Guide*.

Uninstallation

To uninstall Event Broker from the master node:

1. Run `/opt/arcsight/kubernetes/uninstall.sh.`
2. Enter Y and N for the prompts.
3. To optionally delete all Event Broker data, then run `rm -rf /opt/arcsight /opt/kubernetes /root/.kube /opt/arcsight/kubernetes/uninstall.sh.`
4. Reboot the node..

To uninstall Event Broker from each worker node:

1. From `opt/arcsight/kubernetes`, run `/root/arcsight-installer-worker/uninstall.sh`
2. Enter Y and N for the prompts.
3. If you wish to delete product data, then run `rm -rf /opt/arcsight root/.kube /root/arcsight-installer-worker`
4. Reboot the node..

After uninstallation, product data is still kept in the NFS folder. You can delete the product data if it is not planned for retention or future recovery. By default, this location is on the master node and the hostpath directory on the master and worker nodes. These locations are `/opt/arcsight/volumes` and `/opt/arcsight/k8s-hostpath-volume.`

Troubleshooting

This section includes material to help you troubleshoot problems or issues that may occur during the installation. Consult the Event Broker Administrator's Guide for additional detailed troubleshooting information.

Why do I see `Failed to upload .. suite features ...` failures when running `uploadimages.sh` during the installation?

If you see the failure `The suite-installer container is not running. Please make sure your suite-installer pod status is "RUNNING". Failed to upload the data of suite features."` then make sure you are running the uploadimages.sh script from the correct folder, which is `/opt/arcsight/kubernetes/scripts/`.

What kind of errors can indicate potential DNS resolution issues?

DNS resolution issues can be indicated by the schema registry not running, and the schema registry pod in crash loop status, with following error message in the Schema Registry logs

```
# kubectl logs eb-schemaregistry-1138097507-1jxbn -n arcsighteventbroker

...

org.apache.kafka.common.config.ConfigException: No resolvable bootstrap urls
given in bootstrap.servers

...
```

How do I capture diagnostic data and logs?

Event Broker includes a range of diagnostic scripts in the web service container. For details on how to utilize these scripts, see Diagnostic Data and Scripts in the Event Broker Administrator's Guide.

Appendix A: arcsight-installer.properties

The arcsight-installer.properties file controls several important settings for your Event Broker installation. Those settings are detailed here.

To edit the file: open in a text editor and make changes as needed.

In order for changed settings to take effect, you will need to undeploy Event Broker and then re-deploy.

Setting	Notes
`## All Event Broker components will use FIPS-certified encryption algorithms`	
`eb-init-fips=false`	Turns FIPS on. Not recommended to change after deployment.
`## Event Broker Kafka will use TLS Client Authentication to verify client connections`	
`eb-init-client-auth=false`	Turns TLS-CA on. Not recommended to change after deployment.
`## Number of partitions for Event Broker default topics in Kafka`	
`eb-init-noOfTopicPartitions=6`	Default value. Will only affect newly created topics. (Add new partitions to existing topics with the Event Broker Manager.)
`## Replication factor for Event Broker default topics in Kafka`	
`eb-init-topicReplicationFactor=2`	Default value. Will only affect newly created topics. (Must delete old topics to change replication factor.)
`## Kafka log retention size`	
`eb-init-kafkaRetentionBytes=10737418240`	Default value per partition per topic. Deletion will occur when EB hits either the duration or retention bytes, whichever comes first.

Setting	Notes
## Kafka log retention size for the Vertica Avro topic. This is uncompressed and requires more space to hold events for the same duration.	
eb-init-kafkaRetentionBytesForVertica=10737418240	Default value per partition per topic. May require additional space than other topics because data is uncompressed. To ensure data retention is the same as other topics, this topic may need to be significantly larger than other topics, as large as a factor of 7 or more. Deletion will occur when EB hits either the duration or retention bytes, whichever comes first.
## Kafka log retention duration	
eb-init-kafkaRetentionHours=672	Based on environment. Requires calculation on customer behalf. Applies to all topics, including those created through ArcMC. Deletion will occur when EB hits either the duration or retention bytes, whichever comes first.
## Kafka inter-broker protocol version	
inter-broker-protocol-version=0.11.0.0	Only to be used during upgrades.
## The message format version the broker will use to append messages to the logs.	
log-message-format-version=0.11.0.0	Only to be used during upgrades.
## Number of Kafka brokers	
eb-kafka-count=3	Determines cluster size for Kafka. Must match number of worker nodes labeled as kafka=yes in Kubernetes. 1 node to 1 host.
eb-zookeeper-count=3	Determines cluster size. Max of 7. Must match number of worker nodes labeled as zk=yes in Kubernetes. MUST be an odd number.
## Host path to store data persistently	
eb-kafka-path=/opt/arcsight/k8s-hostpath-volume/eb/kafka	Will be created if it does not exist.

Setting	Notes
eb-zookeeper-path=/opt/arcsight/k8s-hostpath-volume/eb/zookeeper	Will be created if it does not exist.
## ArcMC hostname	
eb-arcmc-hosts=localhost:443	
## The endpoint identification algorithm to validate the server hostname using the server certificate.	
ssl-endpoint-identification-algorithm=https	Hostname verification for Kafka to Kafka connections.
## The number of stream threads	
stream-num-threads=6	Do not change unless performance issue.
## Log level for each EB container	
level=info	Support settings only.
kafka-log-level=${level}	
zookeeper-log-level=${level}	
schema-log-level=${level}	
web.service-log-level=${level}	
c2av-stream-processor-log-level=${level}	
eventbroker-routing-processor-log-level=${level}	
## Host path directory for ArcMC certificates	
arcmc-certs-path=/opt/arcsight/k8s-hostpath-volume/eb/arcmccerts	
##truncate fields in c2av	

Setting	Notes
c2av-field-truncate=false	If true, fields that are too long will be truncated to fit in the SuperSchema. See ArcMC Admin Guide for details of SuperSchema. If false (default), data in large fields will not be searchable.
##c2av config params	Optional tuneable configuration parameters for c2av stream processor.
# c2av-heartbeat-interval-ms=1000 # c2av-max-poll-interval-ms=3600000 # c2av-max-poll-records=100 # c2av-session-timeout-ms=180000 # c2av-request-timeout-ms=305000	

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 Deployment Guide (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!