Hewlett Packard
Enterprise

HPE Security ADP Event Broker

Software Version: 2.10

Deployment Guide

October 19, 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

Revision History

Date	Description
October 19, 2017	Initial release of this document.

Contents

Overview

This document describes how to install the ArcSight Installer platform and use it to deploy ArcSight products, such as Event Broker .

Installation Types

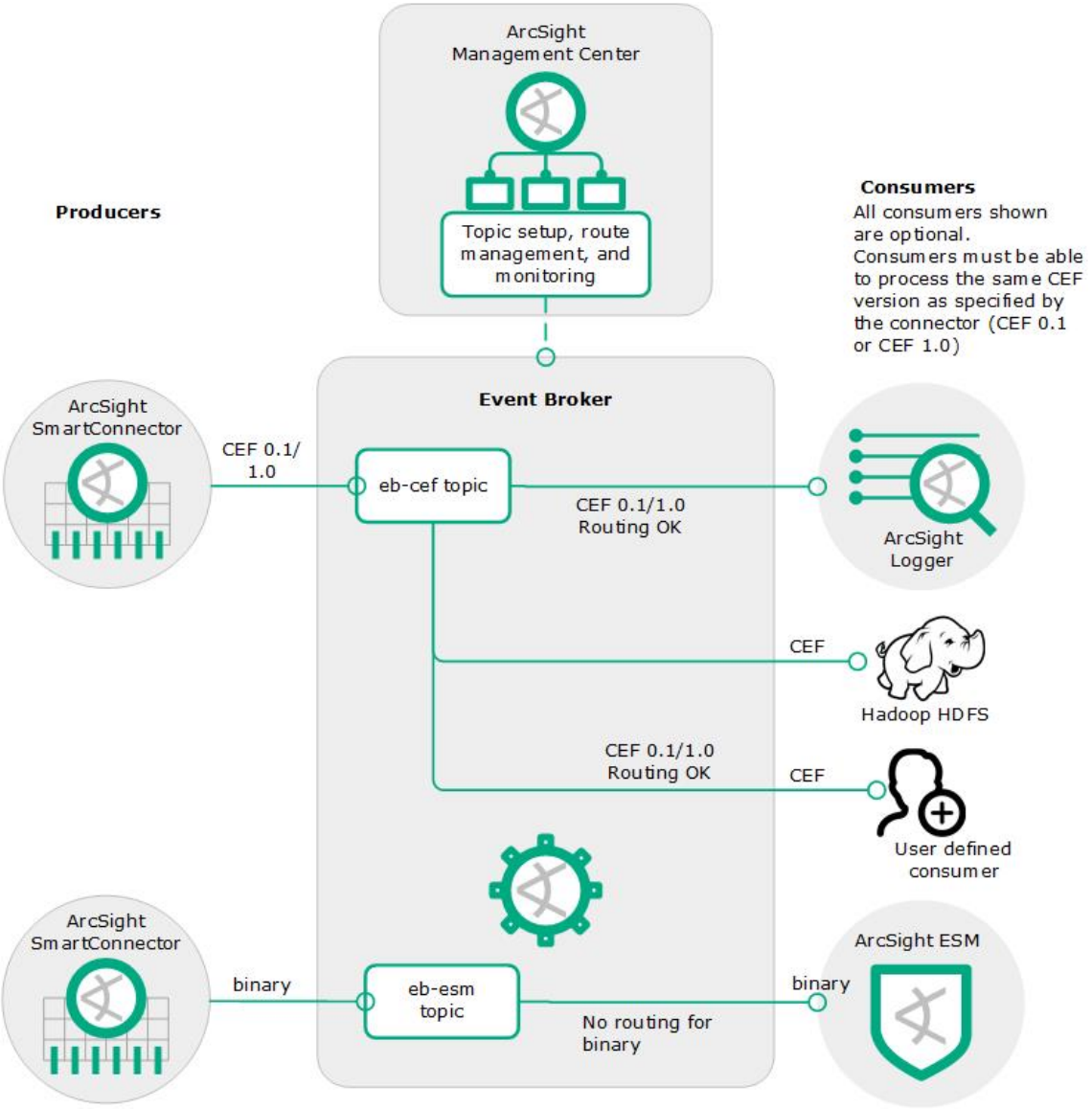
Installation of ArcSight products can be performed in two ways.

- An standard (online) installation assumes that you have a connection to the Internet and the online Docker hub. You can activate your own Docker hub account.
- An *offline* installation presumes you will download the product images from your private Docker registry.

Some instructions in this document will apply to one or the other installation type, and will be marked as such.

About ArcSight Event Broker

ArcSightEvent 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. The ADP Event Broker integrates with ArcSight connectors, Logger, and ESM, 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 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 destination s 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.

System requirements

Installation of the ArcSight Installer platform has the following requirements for both master and worker nodes:

- **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.
- Master and the worker nodes must be installed under the same subnet. You should note the IP or FQDN of all nodes, as these will be needed for later in the installation process.
  - Minimal disk size required for master node is 50 GB in `/opt` and 4 GB in `/var`.
  - Minimal disk size required for each worker node is 150 GB in `/opt` and 3 GB in `/root`.
- Admin needs to have root permissions. All the commands in the installer process must run under root.

Network planning

- Ensure that each node is configured with a fully qualified domain name.
- Ensure proper DNS configuration across all systems including correct forward and reverse DNS lookups.
- Enable internet access in order to download the product container images.
- If your organization's network has a proxy, define the proxy environment variable on all servers. Define these variables per user, and not system-wide.

Configuring NTP using chrony on all of the hosts in the cluster

About

Chrony is a versatile implementation of the Network Time Protocol (NTP). Chrony keeps the system clocks of each of the cluster nodes in sync with each other. A network time server must be available.

Chrony is installed by default on some versions of RHEL/CentOS. If chrony is not installed or running on your system, install it.

Verify Chrony Configuration by using the command:

```
chronyc tracking
```

If not installed, perform the following procedure.

Procedure

1. If necessary, install chrony.

   ```
   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
   ```

Firewall configuration

The following ports need to be free and available for firewall configuration.

- **Web Installer:** 5443
- **Kubernetes:** 2379,2380,3000,4001,4194,5000,5443,8080,8088,8200,8285,8443,10248-10252,10255
- **NFS:** 111,2049,20048,37189
- **Event Broker:** 2181,9092,9093,39000,39093,32181
- **CEB:** (alpha feature only, not for production) 39001-39010

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

Configuring proxy settings

About

Comment out proxy data in the `/etc/profile.d/proxy.sh` file on all nodes, if it is being used.

If you are using a proxy server in your environment, then add your proxy data to the `~/.bashrc` file.

Procedure

Update the `.bashrc` file according to the following example:

```
export http_proxy=http://<proxyserver>:8080/
```

```
export https_proxy=http://<proxyserver>:8080/

export HTTP_PROXY=http://<proxyserver>:8080/

export HTTPS_PROXY=http://<proxyserver>:8080/

export no_proxy="<master ip>,<worker-1 ip>,<worker-2 ip>,<worker-3
ip>,localhost,<domain>"

export NO_PROXY="<master ip>,<worker-1 ip>,<worker-2 ip>,<worker-3
ip>,localhost,<domain>"
```

RPM Requirements

For offline installation (only), the following packages need to be installed using rpm/yum on all systems (master and workers):

```
yum install -y unzip nfs-utils libseccomp libtool-ltdl
```

Java 8 needs to be available and accessible on all servers.

Set up encryption modes before installing and configuring Event Broker

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*

Kubernetes nodes configuration (master and workers)

A Kubernetes installation should have 1 master and 2 or more worker nodes. Multi-master installation is not supported.

Prepare Master node

For your master node, prepare an empty host which meets the system requirements as described under "System requirements" on page 6.

Note: The NFS server on the master Kubernetes node cannot be used for any purposes other than Kubernetes.

Prepare Worker nodes

For your worker nodes, prepare two or more empty hosts which meet the system requirements.

In order to let workers communicate with the master, you need to generate a key pair and copy the public key to each worker node.

Prepare the desired number of empty hosts to be used as workers, which meet the requirements as described under "System requirements" on page 6.

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>
```

Installing the ArcSight Installer

About

This platform is necessary for the ArcSight Installer to run.

Prerequisites

1. Update `/opt/arcsight/installer/arcsight-installer.properties` (see "Adjusting ArcSight Installer properties" on page 1).
2. Obtain aHub account.
   a. Create an account on Docker Hub.
   b. Send your Docker ID to the HPE personal distribution list (PDL).
      - HPE gives you the ArcSight Event Broker license and privileges on Docker Hub.
      - You now have access to your Docker account and Docker images.
      - For more information, refer to the welcome letter you received when you bought your ArcSight product.
3. Perform the installation as the root user.
4. Master and worker nodes need to be installed under the same subnet.

- Minimal disk size required for master node is 50 GB in `/opt` and 4 GB in `/var.`
- Minimal disk size required for each worker node is 150 GB in `/opt` and 3 GB in `/root.`

Procedure

1. Log into the master node as a root user.
2. Download the installation zip file.

   Unzip the installation zip file.
3. Run these commands from where you downloaded the installation zip file.
4. Change into the directory created.

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

   `./arcsight-installer-master.sh`
6. Install the platform on each worker node.

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

   Where *<Worker-Node_IPv4>* is the IPv4 address of each worker node.

Deploying ArcSight products

Once the ArcSight Platform is installed, you are ready to deploy ArcSight products supported by the installer.

1. Browse to `https://<master_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*
4. If you need to pre-configure some product's features (such as FIPS, Client Authentication) before starting deployment, open `/opt/arcsight/installer/arcsight-installer.properties` and update the values accordingly. See arcsight-installer.properties for more information.
5. **Node labeling:** You will need to label each node for its functionality.

To label a node for Kafka run `kubectl label --overwrite node {node_ip} kafka=yes`

To label a node for Zookeper run `kubectl label --overwrite node {node_ip} zk=yes`

For Kafka and Zookeper 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.

6. **Download product images:** If performing an online installation, you can now download the product images for deployment from Docker , as listed below. (If you are performing an offline installation, see Offline Download for your steps. Then proceed with step 7, below.)

- Download Event Broker

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

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

Pick a version you want to download. Once the images are downloaded run `./uploadimages.sh --suite eventbroker` to upload them to the local Docker registry.

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

- Pick a product 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 up to 2-5 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.)

8. **Configuration**: Once a product is deployed, it can be configured on the **Configuration** page. 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 interruptions to some running applications.

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

Activating your Docker Hub account

You now have the option to deploy HPE ArcSight Event Broker included in the HPE ArcSight Data Platform using container deployment and management, which allows for a new delivery and deployment model. Visit HPE Software Entitlements Portal at http://www.hpe.com/software/entitlements to download.

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

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

Offline Download

Use this installation if you do not have an Internet connection from your ArcSight Event Broker to the Docker Hub registry.

Procedure

1. From a server with an Internet connector, connect to the HPE Software Entitlements portal at http://www.hpe.com/software/entitlements and download the offline installer file.

```
<eventbroker-XX>.tar
```

2. Copy the installer TAR file to any location on the master node.

3. Push the images to your private local Docker registry, which is configured and runs on 127.0.0.1, and is accessible from all nodes.

```
./uploadimages.sh -s eventbroker -d /tmp/eventbroker
```

4. Run the following command on the master node:

```
/opt/arcsight/installer/k8s/master/pushImages.sh -f <images.tar>
```

5. Verify the integrity of the files using the Docker inspect command. Event Broker includes 7 Event Broker images. In the command below, .Id represents 'Id' field of the image, which is the unique identifier of a Docker image. Run the following commands and compare your output with what is shown. Your output should be the same.

```
 # docker inspect --format='{{.Id}}' arcsightsecurity/atlas_connector_image:
```

```
2.10.0

sha256:<TBD>

 # docker inspect --format='{{.Id}}' arcsightsecurity/atlas_kafkamanager:

2.10.0

sha256:<TBD>

# docker inspect --format='{{.Id}}' arcsightsecurity/atlas_web-service:2.10.0

sha256:<TBD>

# docker inspect --format='{{.Id}}' arcsightsecurity/atlas_sp:2.10.0

sha256:<TBD>

# docker inspect --format='{{.Id}}' arcsightsecurity/atlas_schemaregistry:

2.10.0

sha256:<TBD>

# docker inspect --format='{{.Id}}' arcsightsecurity/atlas_kafka:2.10.0

sha256:<TBD>

# docker inspect --format='{{.Id}}' arcsightsecurity/atlas_zookeeper:2.10.0

sha256: <TBD>
```

6. Continue with Step 7 of Deployment, as shown here.

Undeploying and redeploying Event Broker

About

In the event of a planned redeployment of Event Broker without a restart of the cluster node systems, be sure to do a clean undeploy of event broker.

Procedure

1. If possible please turn off all the data producers (like the connectors or any other third party producers) sending events to Kafka and wait for Kafka to process all the events.
2. Undeploy Event Broker.
3. Wait for all pods being terminated. You can check this with the following `command: kubectl get pods --namespace=arcsighteventbroker1`
4. Wait for kafka hostports being unallocated on all machines. You can check this on each machine with the following command: netstat -putna | grep LISTEN | grep "(9092|9093|9999|10000)"

5. **Optional:** Wipe out the Kafka data by running the following command on each machine: `rm -rf /opt/arcsight/k8s-hostpath-volume/eb/*`

   Caution: This step removes all existing data. Do not perform this step unless you want to remove existing data.

6. Deploy Event Broker

Uninstallation

To uninstall Event Broker from the master node:

1. `/opt/arcsight-installer-1.20.27-master/uninstall.sh.`
2. Enter Y and N for the prompts.
3. If you wish to delete data, then `rm -rf /opt/arcsight /opt/kubernetes /root/.kube /opt/arcsight-installer-1.20.27-master.`
4. Sync and reboot.

To uninstall Event Broker from each worker node:

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

After uninstall, 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.`

Upgrading to Event Broker 2.10

Currently, no upgrade is supported to Event Broker 2.10.

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 2.10)

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!