Micro Focus ArcSight Event Broker Deployment on Kafka

Software Version: 2.20

Deployment Guide

Document Release Date: Aug 6, 2018
Software Release Date: March 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

Chapter 1: Overview

About Event Broker

Event Broker is a high performance message bus and data ingestion application for ArcSight security events that utilizes Kafka and Micro Focus technology for deployment and management of applications. It can queue, transform, and route security events to ArcSight and third party software. Event Broker allows products such as Logger, ESM and ArcSight Investigate to receive the event stream as it comes, while smoothing event spikes.

Event Broker ingests, enriches, normalizes, and then routes data to connections between existing data lakes, analytics platforms, and other security technologies and the multiple systems within the Security Operations Center (SOC). It can seamlessly broker data from any source and to any destination that is able to consume the supported message formats.

The Event Broker product is available in two different deployment forms. Choose one that supports your specific needs:

- Event Broker: Docker container-based deployment package which utilizes Kubernetes, containerized Kafka, containerized Zookeeper, a Kafka management application, plus support for all Event Broker features. See the Event Broker Deployment Guide for information about how to install Event Broker using this deployment package.
- Event Broker Deployment on Kafka (EB-DoK): File-based deployment package that supports a subset of Event Broker features, and does not come with Kafka, Zookeeper, or the Event Broker Manager built-in. This package is intended to be used in environments where a customer wants to deploy Event Broker onto an existing Kafka cluster. This document describes how to install Event Broker Deployment on Kafka deployment package.

Product Compatibility

The following product versions are intended to be deployed together.

Event Broker Deployment on Kafka	2.20
ArcSight Investigate	2.10
ArcSight SmartConnector	7.80
ArcSight Management Center	2.80
ESM	7.0, 6.11.0

About Event Broker Deployment on Kafka

The Event Broker Deployment on Kafka (EB-DoK) deployment package is intended for environments where that have an existing installation of Kafka and Zookeeper, and customers want to install Event Broker into that environment.

The EB-DoK deployment package provides only the software components needed to run Event Broker. It does not include Kafka, Zookeeper, or Event Broker Manager which manages the Kafka brokers. EB-DoK is not a container-based deployment, but as a set of systemd managed services, one for each software component, that communicate with Kafka and Zookeeper systems and with each other. Each installed instance of EB-DoK includes the following software components (and service name):

- Schema Registry (arst-sr): Used to define the structure of messages for CEF to AVRO transformation and for the Routing Stream processor.
- Web Service (arst-ws): Provides management, monitoring, and metrics capabilities to ArcMC. Is also responsible for creating the Event Broker DoK topics in Kafka when you first install EB-DoK.
- Routing Stream Processor (arst-route): Routes CEF events to defined topics based on rules that characterize which subset of events should be routed.
- C2AV Stream Processor (arst-c2av): transforms messages from CEF to AVRO and is used in the Investigate data pipeline.

Feature Comparison Event Broker Deployment on Kafka and Event Broker

Certain features that are available in Event Broker are not available in Event Broker Deployment on Kafka. The following table summarizes the differences.

Capability	Event Broker	Event Broker Deployment on Kafka
CEF Event Routing	Supported	Supported
Management and Monitoring through ArcMC	Supported	Limited Support. • Operating System metrics are not collected. • ArcMC connects to one instance of EB-DoK at time. If that instance fails, you manually connect ArcMC to another running instance if you have a highly available deployment topology.
Connectors in Event Broker	Supported	Not Supported

Capability	Event Broker	Event Broker Deployment on Kafka
Event Broker Manager	Supported	Not Supported
Container-based deployment	Supported	Not Supported
Auto restart of failed modules	Supported via the native ability of docker containers to restart automatically.	Not supported. Services must be monitored, managed, and restarted by the customer.
Security Modes	FIPS Supported TLS Supported Client Authentication Supported	TLS is used for communication between services on an installed EB-DoK instance. TLS is not supported for communication between EB-Dok services and Kafka or Zookeeper. FIPS not supported Client Authentication not supported

Summary of the Deployment Steps

About

The high level deployment process for Event Broker Deployment on Kafka (EBDoK) is summarized in this section.

Procedure

1. Make sure you have a fully functional Kafka and Zookeeper deployment before you start this process. Kafka brokers in the cluster must be able to accept connection requests, a producer must be able to publish a message to a topic, and consumers must be able to read from that same topic.
2. Plan your Deployment Topology. See "Plan the Deployment Topology" on the next page.
3. Set up the host machines needed for Event Broker DoK and ArcMC, and collect the information needed during the installation process. See "Installation Prerequisites" on page 9.
4. Download and install the Event Broker DoK installation package. See "Download and Install Event Broker Deployment on Kafka" on page 12.
5. Configure the Event Broker DoK services. See "Configure the Event Broker Services" on page 12.
6. Install your customer license to ensure continued functionality and event flow. See "Install Your Customer License" on page 17 for more information.
7. Install ArcMC to connect to Event Broker DoK. See "Connect ArcMC to Event Broker DoK" on page 17 for more information.

Start the Event Broker DoK services. See "Start the Event Broker DoK services" on page 14.

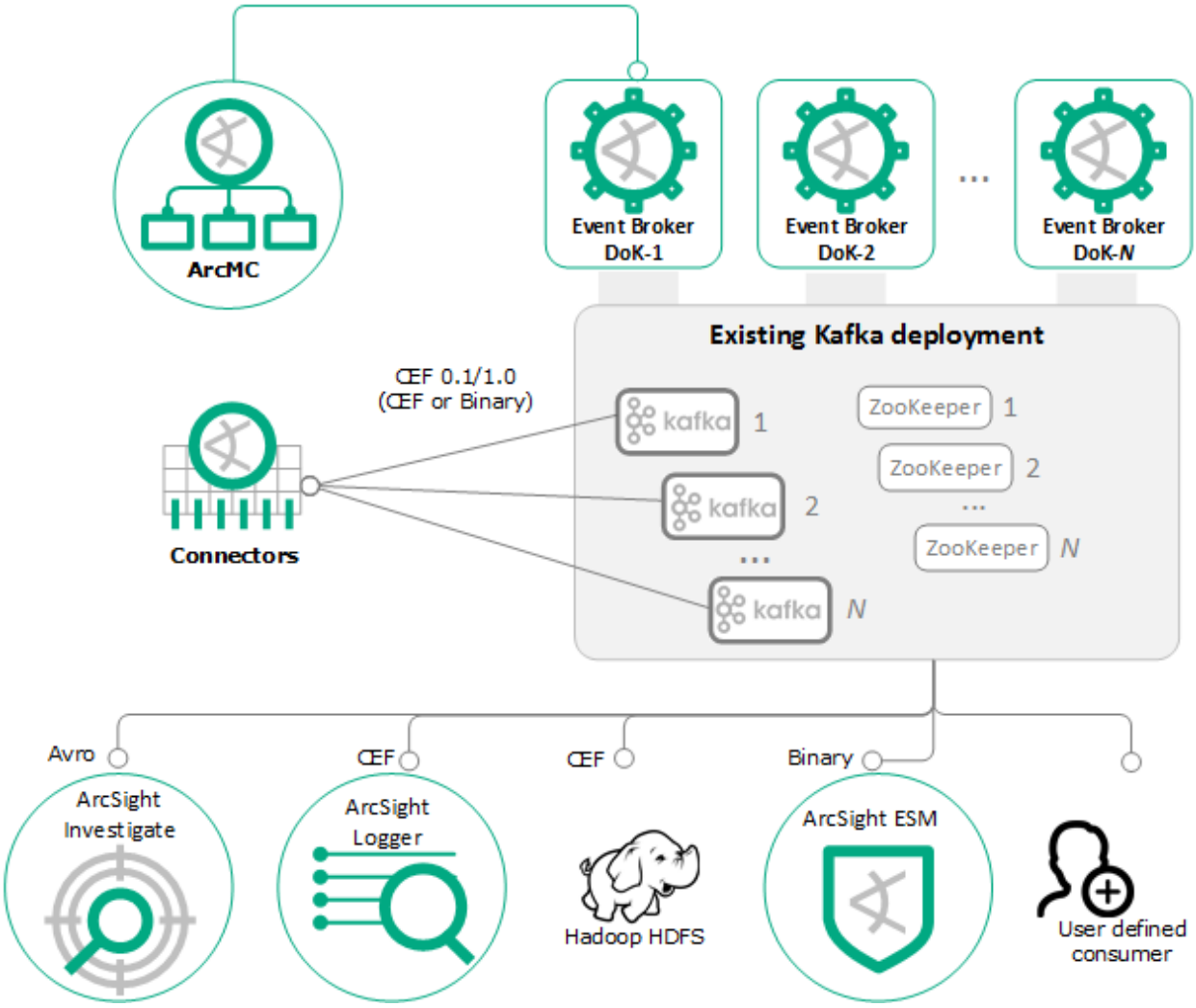
8. Ensure the Event Broker services are running and are healthy. See "Check the status of the Event Broker DoK services" on page 16
9. Set up SmartConnectors to publish events to Event Broker DoK.
10. As needed, set up ESM, Logger, and Investigate to consume events from Event Broker DoK.

Plan the Deployment Topology

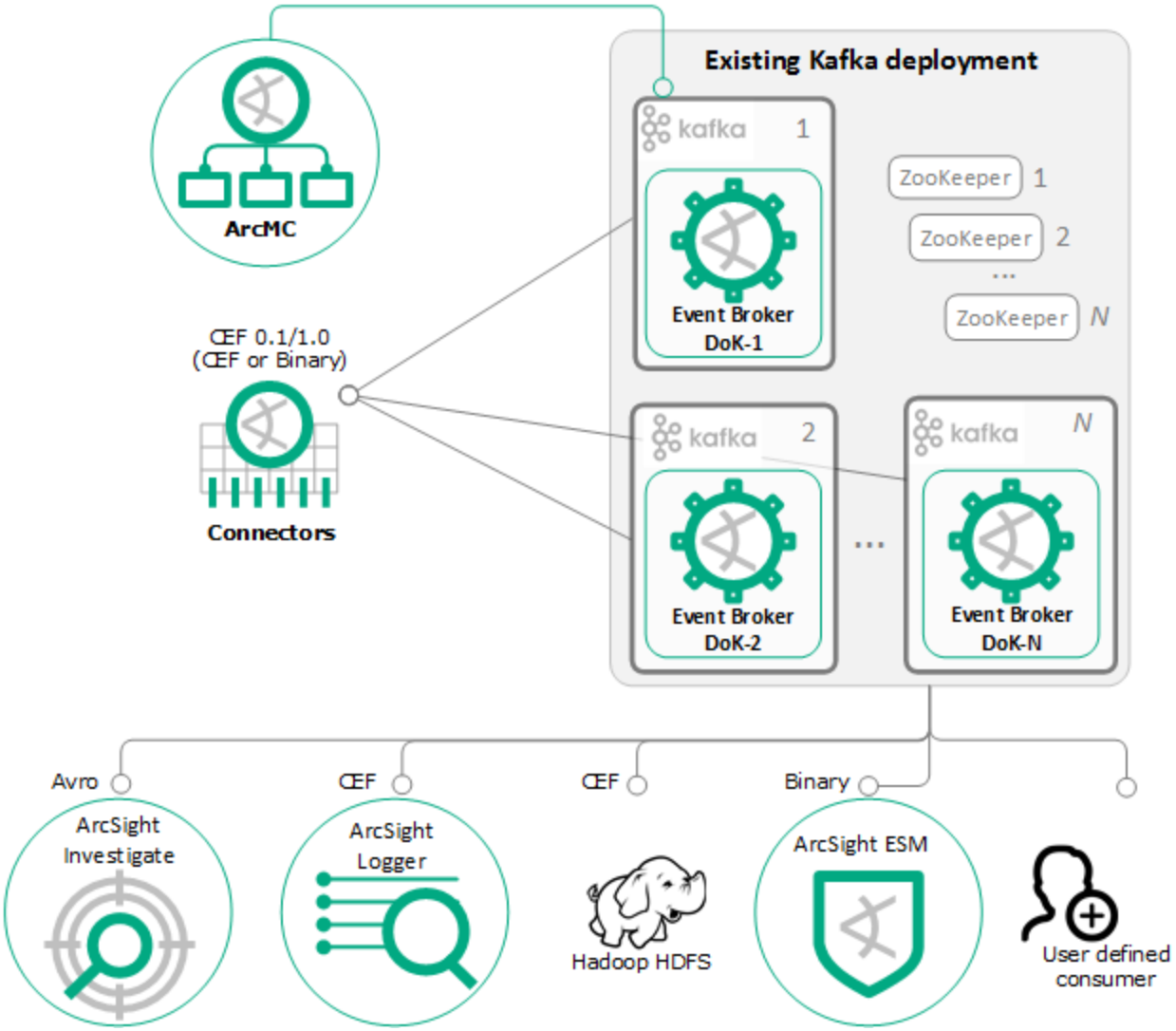
You can deploy one instance of EB-DoK or multiple instances of EB-DoK, each on a separate systems. To support a highly-available deployment topology, install at least three EB-DoK instances each on a separate server. Each EB-DoK instance can run on a dedicated system, or it can run on the same system where Kafka is installed.

- When you deploy in a multi-node configuration, the Stream Processor services (both CEF to AVRO and Routing) will work as a consumer group providing High Availability (HA) if one EB-DoK instance fails.
- ArcMC connects to Web Service on one of the instances. If that system fails, ArcMC will need to be manually reconfigured to connect to one of the other systems running the EB-DoK Web Service.
- You must install the ArcMC server certificate onto the EB-DoK system that ArcMC connects to. You can import certificates to all systems ahead of time to prepare for the future connections, or you can import the certificate to the individual system only at the time you connect ArcMC to that instance.
- JMX must be enabled on Kafka brokers so that monitoring data can be obtained from the brokers.

Event Broker DoK running on Dedicated Nodes



Event Broker DoK running on Kafka Nodes



Installation Prerequisites

Software and system prerequisites

Make sure that you have the following software installed on each system where EB-DoK will be installed:

Operating system	CentOS 6.9, CentOS 7.3 or RHEL 7.3, CentOS 7.4
Kafka and Zookeeper	Cloudera CDH version 5.10 with Kafka 0.11 and Zookeeper.
Java	Java 8

OpenSSL	Any version of OpenSSL is sufficient. Make sure that the openssl command can be called from the command line. OpenSSL is used to generate a certificate during installation .
Python	2.7.5

Configuration prerequisites

Make sure that you perform the following configurations :

- Open port 8080 on each system where you will install Event Broker Deployment on Kafka and where you plan to connect ArcMC. This port is used by ArcMC to communicate to Event Broker Deployment on Kafka .
- Make sure that JMX is enabled on the Kafka cluster so that the Web Service can retrieve metrics from Kafka.
- If you plan to connect ArcMC to Event Broker Deployment on Kafka so that you can manage and monitor the Event Broker, you will need a copy the ArcMC server certificate, as a *.crt file.
- The scripts that install EB-DoK, configure services, and manage services must be run as root user. Make sure you can connect to each system with this privilege.

Information needed before you get started

You will be prompted for information during the installation and the services set up interviews. Gather the following information ahead of time to prepare .

Information Needed	Description
Information about your Kafka Installation	You will need to know the host names and port of each system in the cluster where Kafka brokers are running. You will need the hostname and port of all systems in the cluster where Zookeeper is running.
Password for Self Signed certificate	The Event Broker Deployment on Kafka services communicate with each other securely. Self signed certificates are used for this communication. You will be prompted for a password when this certificate is generated.
Kafka JMX port	If you plan to have ArcMC manage and monitor Event Broker Deployment on Kafka, you will need to configure JMX on all Kafka brokers so that the Event Broker Web Service can retrieve metrics from the cluster. You will need to provide the port that was configured as the JMX_PORT.
Choose an Admin username and password	The Event Broker Web Service requires that admin credentials are created for communication with the Routing

Information Needed	Description
	stream processor.
Information about your ArcMC installation	You will need to know the host name and port of the system where ArcMC will be installed. You will also need to obtain the ArcMC server certificate. It must be copied to the EB-DoK system that ArcMC it will connect to.
AutoPass Customer License	Obtain your permanent license. Event Broker Deployment on Kafka provides a 90 day trial license. You will need to install your own license to continue operation past the 90 day trial. If you do not replace the license before the 90 day trial ends, then data will stop flowing through the Event Broker DoK data pipelines.

Chapter 2: Install Event Broker Deployment on Kafka

Download and Install Event Broker Deployment on Kafka

About

The following steps install the Event Broker Deployment on Kafka files to the system. If you want the high-ability of the EB-Dok cluster, you must install it on multiple systems. Repeat the following steps on each system in the cluster that will run EB-DoK. You must perform these steps as root user.

Procedure

1. Download EBDoK 2.20.0.1004 Installer from the software entitlement site to the system where you plan to install it.
2. Change to the directory where you downloaded the file.
3. Run the command:

   ```
   ./ArcSight-EBDoK-2.20.0.1004.bin
   ```

   You will see the message start with:

   ```
   Extracting the JRE from the installer archive...

   Unpacking the JRE...
   ```

   This first installation prompt provides an explanation about the installation interview that follows.
4. Read the License Agreement and Accept the Terms.
5. You will be prompted to define an Installation folder. It is recommended that you use the default folder:

   ```
   /opt/arcsight/EBDoK
   ```

6. Read and confirm information in the Pre-Installation Summary.
7. When complete you will see the following message, with additional instructions about next steps:

   ```
   Congratulations! Event Broker Deployment on Kafka has been successfully
   installed to: /opt/arcsight/EBDoK/current
   ```

   The next steps are to configure the Event Broker Deployment on Kafka services.

Configure the Event Broker Services

About

The following steps guide you through configuring Event EB-DoK Services so that it can communicate with Kafka and Zookeeper, and enable ArcMC to connect to a Web Service instance. Perform these steps on each system where you installed the Event Broker Deployment on Kafka. You must perform these steps as root user.

Procedure

1. Change to the /opt/arcsight/EBDoK/current/bin directory.

   ```
   cd /opt/arcsight/EBDoK/current/bin
   ```

2. To start the set up script, run command:

   ```
   ./setup-ebdok
   ```

3. You will be prompted for the following information:
   - Is your Kafka in TLS mode?

     Always enter N. You will be prompted to provide a user name and password. A self-signed certificate is generated for communication between the EB-DoK services. When the generation is complete, you will see the message:

     ```
     A private self signed certificate will be generated for this host system and added to the keystore.
     ```

   - Enter Kafka endpoint (host1:port1,host2:port2,...).

     Provide a comma separated list of the host name and port for each system in the cluster that runs a Kafka Broker. For example:

     ```
     host1.usa.company.com:9092,host2.usa.company.com:9092,host3.usa.company.com:9092
     ```

   - Enter Zookeeper endpoint (host:port):

     Provide a comma separated list of the host name and port for each system in the cluster that runs a Zookeeper instance . For example:

     ```
     host3.usa.company.com:2181,host4.usa.company.com:2181,host5.usa.company.com:2181
     ```

   - Enter Kafka JMX port:

     Kafka JMX is used by the Web Service to retrieve metrics about the installed Kafka brokers. Enter the port that you configured when you enabled JMX on the Kafka cluster.

   - Enter Event Broker Deployment On Kafka Admin Username:
   - Enter Event Broker Deployment On Kafka Admin Password:

     Confirm password:

     NOTE: The Admin Username and Password are used for authentication during communication between the Routing Stream Processor and the Web Service. These credentials will not need to be used by a user for any other purpose.

   - Do you want to provide ArcMC host info? [Y/N]

     Select Y if you will connect ArcMC to this system, you will be prompted for ArcMC host name.

     ```
     Enter ArcMC host:
     ```

   - You will be prompted to review the information provided:

     ```
     Please review the following information regarding Kafka configuration.
     ```

- You will be prompted to start the configuration

  ```
  About to install Event Broker Deployment on Kafka services to run on boot as user root? Enter Y or N.
  ```

  It is a requirement that the services run as root user. Enter Y.

4. When the configuration is complete, you will see the message:

   ```
   Event Broker Deployment on Kafka service has been installed, you can run service using: /opt/arcsight/EBDoK/current/bin/manage-service start
   ```

5. If you plan to connect ArcMC to an Event Broker Deployment on Kafka node, continue to the section "Connect ArcMC to Event Broker DoK" on page 17. If not, continue with the section "Start the Event Broker DoK services" below.

Start the Event Broker DoK services

You can start all services at the same time or start them individually. Services must start in a specific order:

1. Schema Registry
2. Web Service
3. either the Routing Stream Processor or CEF to AVRO Stream Processor

If any dependent service fails to start, the downstream service will not start. You must run these scripts as root user.

Start all services using one command

1. Change to the /opt/arcsight/EBDoK/current/bin/ directory:

   ```
   cd /opt/arcsight/EBDoK/current/bin/
   ```

2. Run the following command to start all services:

   ```
   ./manage-service start
   ```

3. You will see a confirmation prompt:

   ```
   Event Broker Deployment on Kafka

   ========================================

   About to start Event Broker Deployment on Kafka services as user root.

   Are you sure you want to continue? (type YES)
   ```

4. After you enter YES, you will see status output as the individual services start. If a service fails to start you will see the FAILURE status , and the entire start up process will stop .

   ```
   Starting Schema Registry...

   Starting arst-sr (via systemctl):                          [  OK  ]
   ```

```
Starting Web Service...
Starting arst-ws (via systemctl):                          [  OK  ]
Starting Routing Stream Processor...
Starting arst-route (via systemctl):                       [  OK  ]
Starting CEF to AVRO Transforming Stream Processor...
Starting arst-c2av (via systemctl):                        [  OK  ]
Event Broker Deployment on Kafka services started.
```

5. Check that the services are running by running the command:

   ```
   ./manage-service status
   ```

Start one service at a time

You can start a single service using the following commands. You must execute these commands as root user.

Command	Description
`systemctl start arst-sr`	Starts the Schema Registry service.
`systemctl start arst-ws`	Starts the Web Service.
`systemctl start arst-c2av`	Starts the CEF to AVRO Stream Processor service
`systemctl start arst-route`	Starts the Routing Stream Processor service

Stop the Event Broker DoK services

About

This procedure explains how to stop the Event Broker DoK services. You can stop all services at the same time or stop them individually. You must run these commands as root user.

Procedure

Stop all services using one command

- Change to the /opt/arcsight/EBDoK/current/bin/ directory:

  ```
  cd /opt/arcsight/EBDoK/current/bin/
  ```

- Run the following command to stop all services:

  ```
  ./manage-service stop
  ```

Stop one service at a time

You can stop an individual service using the following commands.

Command	Description
`systemctl stop arst-sr`	Stops the Schema Registry service.
`systemctl stop arst-ws`	Stops the Web Service.
`systemctl stop arst-c2av`	Stops the CEF to AVRO Stream Processor service
`systemctl stop arst-route`	Stops the Routing Stream Processor service

<ToDo: add the output>

Check the status of the Event Broker DoK services

About

This procedure explains how to check the status of Event Broker DoK services. You must run these scripts as root user.

Procedure

View the status of all services using one command

1. Change to the /opt/arcsight/EBDoK/current/bin/ directory:

   ```
   cd /opt/arcsight/EBDoK/current/bin/
   ```

2. Run the command

   ```
   ./manage-service status
   ```

View the status of an single service

You can view the status of a single service using the following commands.

Command	Description
`systemctl arst-sr status`	View the status of the Schema Registry service.
`systemctl arst-ws status`	View the status of the Web Service.
`systemctl arst-c2av status`	View the status of the CEF to AVRO Stream Processor service
`systemctl arst-route status`	View the status of the Routing Stream Processor service

Install Your Customer License

About

Event Broker Deployment on Kafka comes packaged with a 90 day trial license. Make sure to install the license you received as part of the license activate process before the 90 day trial period ends. The check for a valid license happens during the start up process for the c2av, routing, web service, and schema registry services. All services look for the license file in the same location under the installation directory of that instance.

Procedure

After you receive your ADP ArcMC software license file:

- Rename the file to ***license.xml***
- Connect to each system that runs Event Broker Deployment on Kafka and copy the license file to the /opt/arcsight/EBDoK/current/config/autopass/ directory. This directory is created when the EB-DoK services are started for the first time. If you do not see the directory, "Start the Event Broker DoK services" on page 14 and then recheck for the directory.

  If you have installed multiple EB-DoK instances, you must copy the license file to each instance under the same installation sub-directory
- Restart the c2av, routing, web service, and schema registry services. You must restart the services each time you change the license.

Connect ArcMC to Event Broker DoK

About

ArcMC can connect to one system in a EB-DoK cluster at a time. If the system that ArcMC is connected to fails, then you will need to reconfigure ArcMC to connect to another system in the cluster.

Procedure

Import ArcMC Certificate to the Event Broker Deployment on Kafka system

- Get a copy of the ArcMC server certificate , with the extension *.crt from the system where ArcMC is running.
- Copy the ArcMC certificate file to the system where ArcMC will connect, under the /opt/arcsight/EBDoK/current/cert/webservice/ directory.

Connect ArcMC to Event Broker Deployment on Kafka

See the ArcMC Administrator Guide for instructions about how to Add a Host in ArcMC.

Chapter 3: Uninstalling the Event Broker DoK service

About

The following steps will uninstall the EB-DoK instance from the system. This process does not remove the Kafka topics created by the web service. To remove the Kafka topics, you must manually delete them. See the Apache Kafka documentation for steps about to delete topics. You must run this script as root user

Procedure

- Change to the following directory:

  ```
  cd /opt/arcsight/EBDoK/current/UninstallerData/
  ```

- Run the command:

  ```
  ./Uninstall_ArcSight_EBDoK
  ```

Chapter 4: Troubleshooting the Event Broker DoK instance

About

This section provides the mechanisms you can use to troubleshoot issues you may encounter with Event Broker Deployment on Kafka.

Procedure

There are two mechanism you can use to investigate issues.

- To check the status of services, see "Check the status of the Event Broker DoK services" on page 16.
- You can also view Event Broker DoK (EBDoK) logs under `/opt/arcsight/EBDoK/current/logs` directory.

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Deployment Guide (Event Broker Deployment on Kafka 2.20)

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!