Micro Focus Security ArcSight Investigate

Software Version: 2.20

Tech Note: Standalone C2AV Process

Document Release Date: June 6, 2018
Software Release Date: June 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.

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

Introduction

Investigate 2.20 can launch a stand-alone CEF-to-Avro (C2AV) Stream processor to perform data transformation. The stand-alone C2AV stream processor can be executed against an Apache Kafka 1.0 cluster run in your environment.

This tech note describes the deployment of the standalone C2AV processor.

Technical Requirements

In order to run the C2AV processor, the following is required.

- Version 2.20 or later of ArcSight Investigate.
- A source topic where CEF messages will be sent. The source topic may have any name.
- A sink topic, named `eb-internal-avro` , to which transformed Avro messages will be written by the stream processor for consumption by the Investigate Vertica scheduler process.

Deployment

The standalone C2AV process is delivered with other Investigate container images. However, unlike other Investigate container images, the standalone C2AV transform container is not deployed when Investigate launches. Instead, it must be invoked manually.

The scripts to invoke it manually can be deployed to any worker or master node in the Kubernetes cluster and then executed using the following commands.

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

# ./get-product-tools.sh

Utilities extracted to ./product_tools/investigate
```

Commands

After the technical requirements are met and product tools are extracted, you can invoke and run the C2AV standalone processor.

C2AV Launch Command

The following example assumes that the Kafka topics `eb-cef` and `eb-internal-avro` have already been created on the Kafka cluster:

```
# cd product-tools/investigate/kafka-transform

# ./launch.sh

Usage: ./launch.sh [KAFA_HOST:PORT,KAFKA_HOST:PORT][ZOOKEEPER_
HOST:PORT,ZOOKEEPER_HOST:PORT] [SOURCE TOPIC] [SINK TOPIC]

# ./launch.sh <IP Address>:9092 <IP Address>:2181 eb-cef eb-internal-avro

819e4747e5d7ec5e4b91b41fe966413f6dd76916a75f686a0a7afe02ea730b48

Container investigate_sp_16755 started
```

C2AV Status Command

Status for the stream transform application can be reviewed by running the status command:

```
# ./status.sh

NAMES                  IMAGE                                  CONTAINER ID
CREATED             STATUS

investigate_sp_16755   arcsightsecurity/standalone_sp:master   3ae9512cffe1
     3 seconds           Up 1 second
```

C2AV Stop Command

The transform tool can be stopped by running the stop command:

```
# ./stop.sh

Destroying the following Investigate Stream Processor Containers:
```

```
CONTAINER ID        IMAGE                                  COMMAND
  CREATED             STATUS              PORTS
NAMES

3ae9512cffe1        arcsightsecurity/standalone_sp:master   "/docker-
entrypoin..."   28 seconds ago      Up 26 seconds       2181/tcp, 2888/tcp,
3888/tcp   investigate_sp_16755

3ae9512cffe1

#./status.sh

NAMES                  IMAGE                                CONTAINER ID
CREATED             STATUS
```

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 Tech Note: Standalone C2AV Process (Investigate 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!