Hewlett Packard
Enterprise

HPE Security ArcSight Investigate

Software Version: 2.00

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://community.saas.hpe.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 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://community.saas.hpe.com/t5/ArcSight/ct-p/arcsight

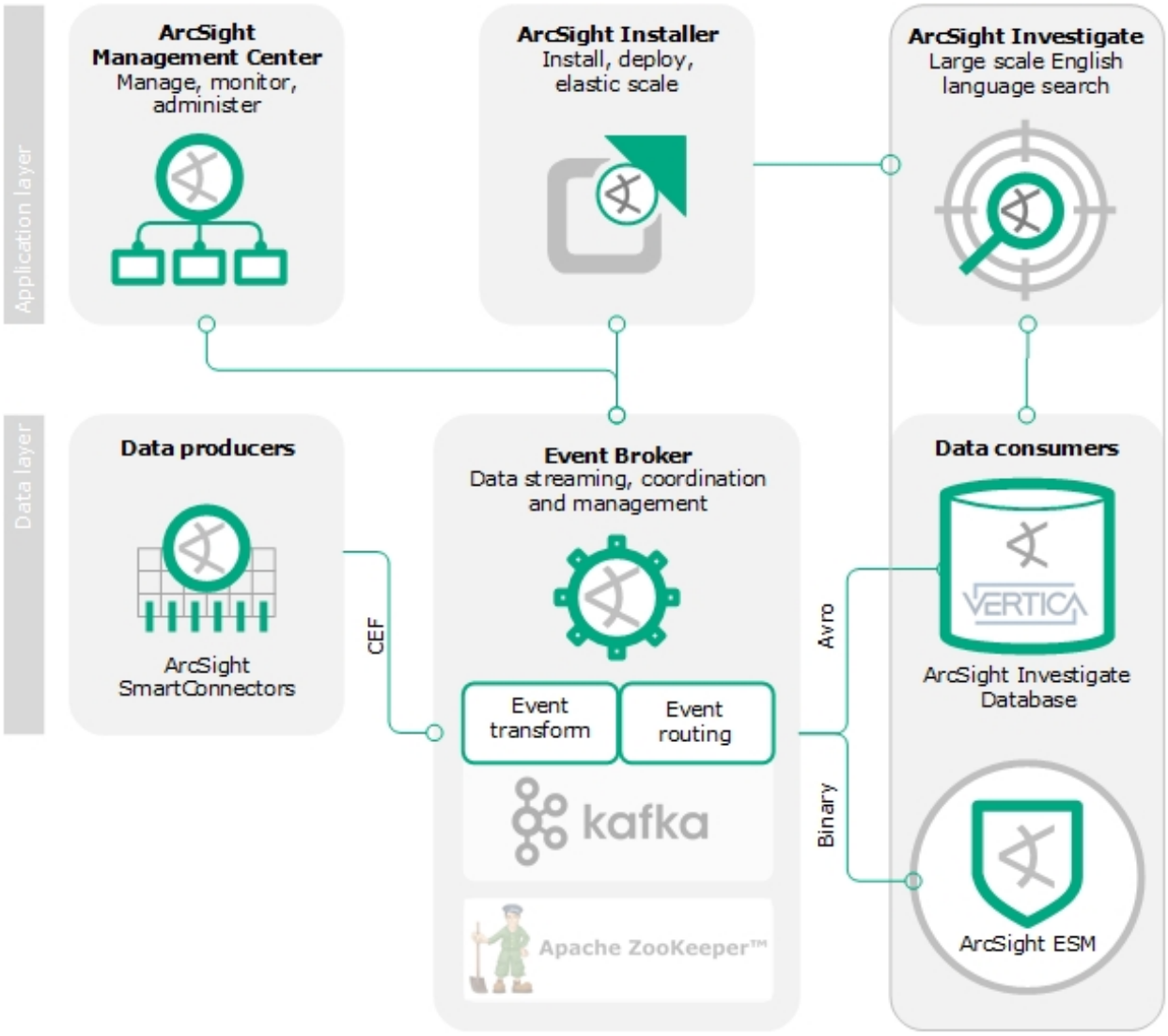
Revision History

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

Contents

Chapter 1: About ArcSight Investigate

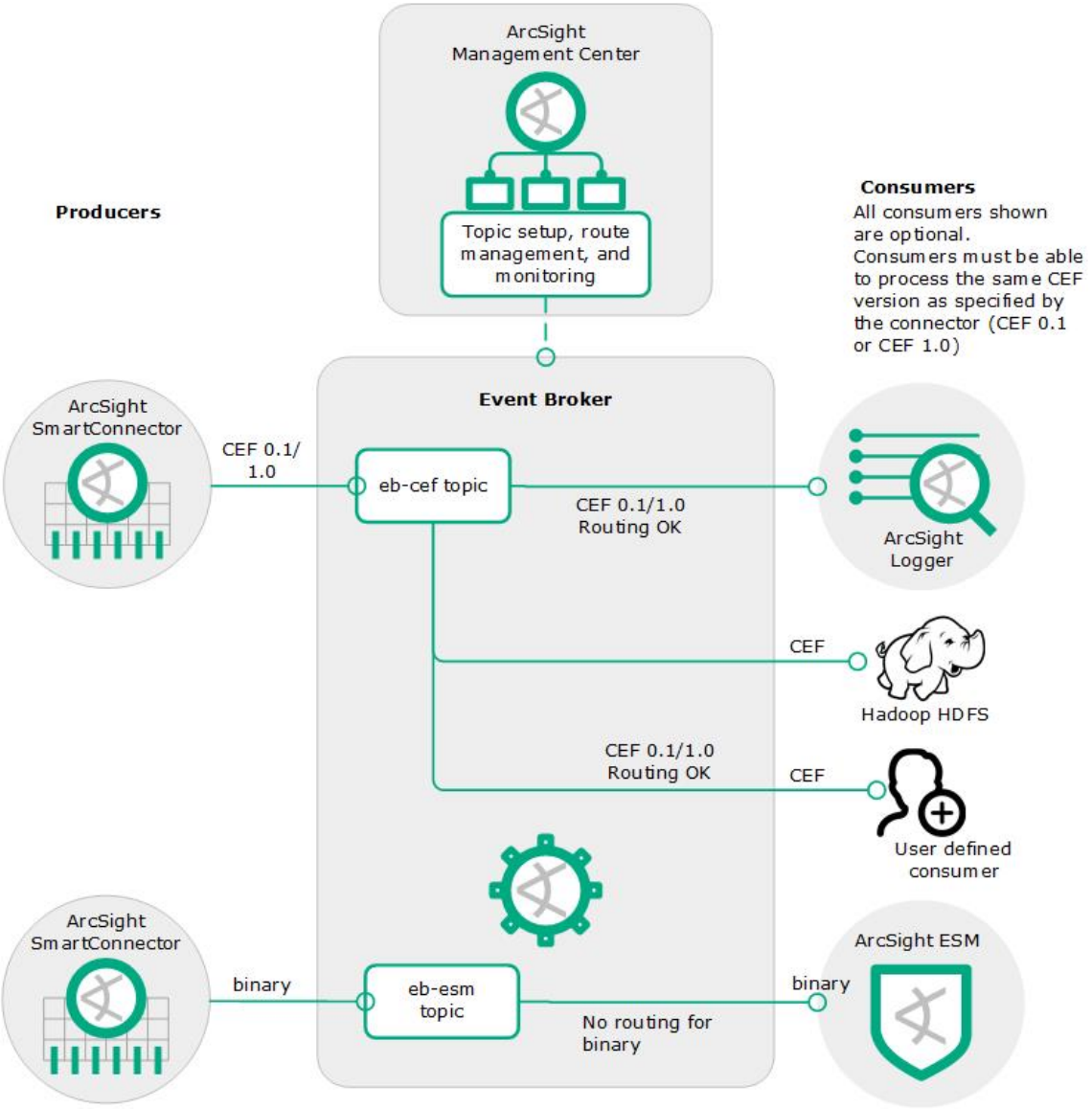
ArcSight Investigate is a high-capacity data management and analysis engine that enables you to search, analyze, and visualize machine-generated data gathered from web sites, applications, sensors, and devices that comprise your monitored network. Investigate indexes the events from your data source so you can view and search on them. You can use the English-like search language to generate results from which to create reports and visualizations.



Component	Description
ArcSight Investigate	High-capacity data management, search, and analysis web application.
ArcSight Installer	A web application for deploying and configuring the ArcSight Investigate components, including Investigate and Event Broker. The components are managed in a Kubernetes cluster. The master node hosts the ArcSight Installer web application and the Investigate web application, and the worker nodes host the Event Broker.
Investigate Vertica database	The ArcSight Investigate analytic database powered by Vertica provides high-capacity data storage and retrieval for rapid search response at high throughput. Vertica is installed separately.
ArcSight SmartConnectors	SmartConnectors collect and normalize event data from nodes on your network. Connectors normalize event data in two ways: normalizing values (such as severity, priority, and time zone) into a common format, and normalizing the data structure into a common schema. SmartConnectors can then filter and aggregate events to reduce the volume of events sent to the system. ArcSight SmartConnectors, installed and maintained separately, are producers that publish data to Event Broker. You can subscribe to data managed by Event Broker with Investigate, ADP Logger, ArcSight ESM, Apache HDFS, or your own third-party consumer.
Event Broker	ArcSight Event Broker centralizes event processing, enabling you to take advantage of scalable, high-throughput, multi-broker clusters for publishing and subscribing to event data. Event Broker coordinates and manages data streams, which enables your ArcSight environment to scale, and opens up ArcSight events to third-party data solutions.
ArcMC	HPE ArcSight Management Center (ArcMC) is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring efficiently and cost-effectively. ArcMC provides run-time management of Event Broker topics. ArcMC is sold as part of the ArcSight Deployment Platform (ADP).

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. and ArcSight Investigate.



- 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 Investigate, ArcSight ESM, Apache Hadoop, or your own consumer.

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

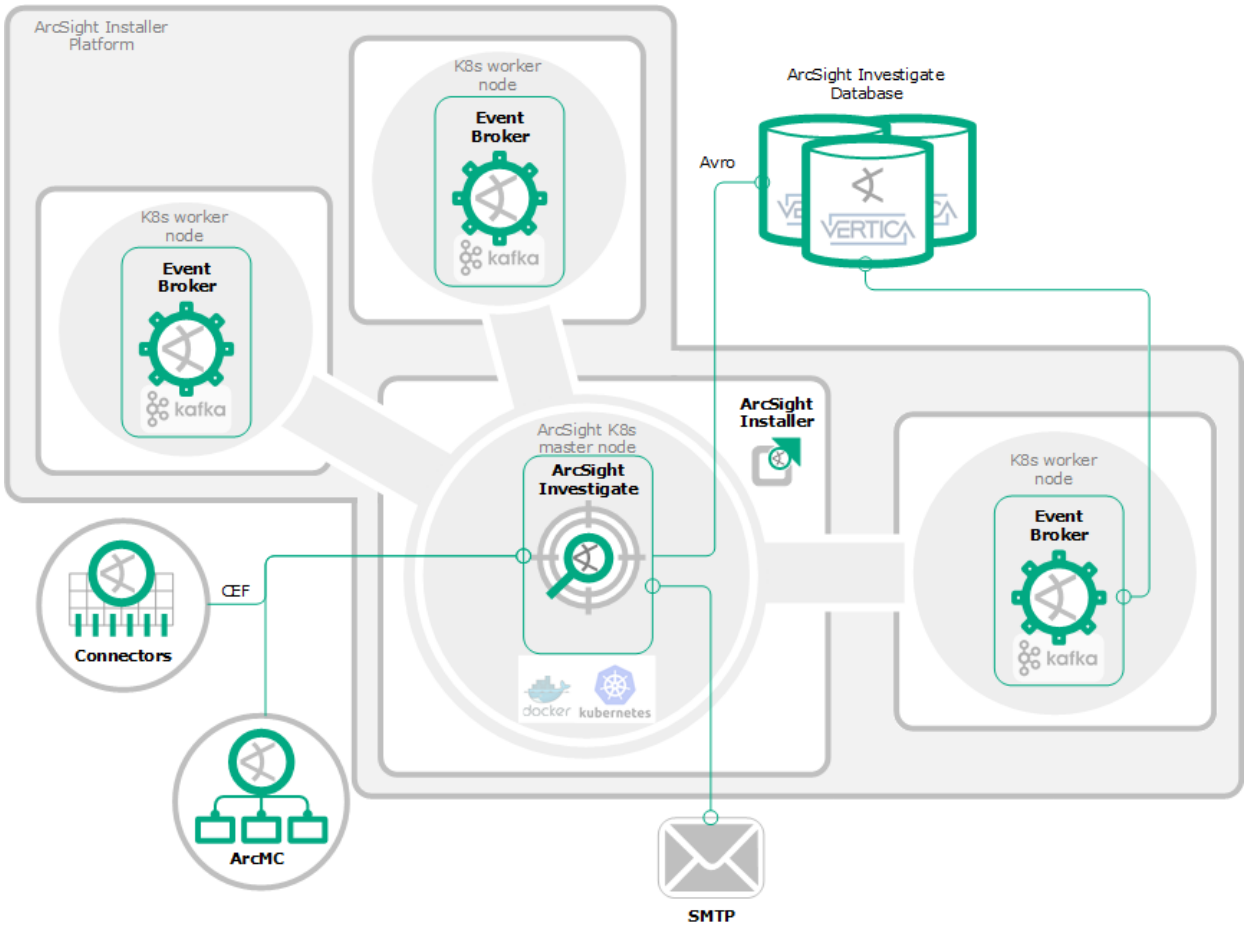
  Event Broker supports both CEF 0.1 and 1.0.

  - 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.
- Event Broker's c2av stream processor converts CEF-formatted event data in the eb-cef topic to Avro format and sends the Avro formatted event data to eb-internal-avro topic.
- ArcSight ESM can be configured as an Event Broker consumer, and can send query parameters to ArcSight Investigate via https.
  - The SmartConnector supporting this scenario has to be set up to dual-feed to both the eb-cef topic consumed by the ArcSight Investigate Vertica database and the eb-esm topic that is consumed by ESM.
  - This ensures that the exact same data generated from the connector is stored in both the Investigate database and the ESM database so that the queries sent by ESM to Investigate will produce consistent results in ArcSight Investigate.

ArcSight Investigate deployment architecture

ArcSight Investigate is installed using Docker containers managed by Kubernetes and deployed from the ArcSight Installer application. The default deployment consists of a Kubernetes master node, and three Kubernetes (K8) worker nodes: three worker nodes for ArcSight Event Broker, and one Kubernetes master node for Investigate.



Deployment component	Host	Functional contents
ArcSight Installer Platform	Install the platform on the master node and each work node.	ArcSight Installer application
Kubernetes master node	1 VM or physical server	• Kubernetes master node • Investigate • ArcSight Installer application
Kubernetes worker nodes	3 VMs or physical servers	• 3 Event Broker nodes
Vertica database	3 physical servers	• 3 ArcSight Investigate Vertica database instances

Deployment component	Host	Functional contents
ArcSightSmartConnectors	Stand-alone or part of ArcMC	Normalizes event data from network devices and formats as CEF.
ArcSight Management Console	Separate installation	Provides run-time management of Event Broker topics.
SMTP server	Separate installation	Provides the ability for ArcSight Investigate to send notification messages to users.

Deployment overview

Before you can deploy ArcSight Investigate deployment you must first deploy the ArcSight Installer, Event Broker, and the Vertica database.

Note: ArcSight recommends installing and running these components in a test environment before putting them into production.

These components will require configuration after you install Investigate.

1. Complete the Installation Requirements.
   a. Ensure that Event Broker and Investigate each have a dedicated servers.

      If other applications are running on the same server as Event Broker and Investigate, there will be a significant performance penalty and potential problems.
   b. Ensure that your file system type is ext4.
   c. Disable SELinux.

      See "Disabling SELinux" on page 14.
   d. Enable the firewall if it is not enabled.
   e. Increase per-user process limits.

      See "Increasing per-user process limits" on page 14.
   f. Ensure the Network Time Protocol (NTP) is configured.

      The chrony daemon, `chronyd`, is used to do this configuration.

      See "Configuring NTP using chrony on all of the hosts in the cluster" on page 15.
   g. Comment out proxy data in the `/etc/profile.d/proxy.sh` file on all nodes, if this file is being used.
   h. Add any required proxy information in the `~/.bashrc` file, on all nodes.

      See "Configuring proxy settings" on page 17.
   i. Generate an SSH certificate on the master node in order to allow connections to the worker

nodes.
See "Generating a key pair on the master node for worker nodes" on page 16.

2. Install the ArcSight Installer Platform.

   See "Installing the ArcSight Installer " on page 18.

   a. Install the ArcSight Installer.
   b. Add worker nodes.
   c. Label the master and worker nodes.

      See "Labeling nodes" on page 19
   d. Login to the ArcSight Installer (UI page) and change the password.
      - Enter the default credentials admin/cloud. After the first successful login, you are required to change the admin password.
      - From the ArcSight Installer (UI page), you can see that **Node Management** in the left navigation.
   e. Ensure that three worker nodes are up and running.

      From the Node Management page of the ArcSight Installer (UI page), check that three worker nodes are running and all have the status of `READY` (see "Managing nodes" on page 19).

3. Do any necessary pre-deployment configuring.

   To pre-configure Investigate default properties go to `/opt/arcsight/installer/arcsight-installer.properties` before starting deployment and update the values accordingly. See "Adjusting ArcSight Installer properties" on page 20

4. Obtain the images of the products you want to install.
   a. Obtain the Event Broker image.
      - For online retrieval, see "Obtaining ArcSight Investigate and Event Broker images (online)" on page 23.
      - For offline retrieval, see "Obtaining ArcSight Investigate and Event Broker images (offline)" on page 24.
   b. Obtain the Investigate image.
      - For online retrieval, see "Obtaining ArcSight Investigate and Event Broker images (online)" on page 23.
      - For offline retrieval, see "Obtaining ArcSight Investigate and Event Broker images (offline)" on page 24.

5. Deploy Event Broker.

   See "Obtaining ArcSight Investigate and Event Broker images (online)" on page 23.

6. Deploy Investigate.

   See "Deploying ArcSight Investigate and Event Broker images" on page 25.

7. Ensure that the Event Broker and Investigate images have completed deployment.

   ```
   $kubectl get pods --all-namespaces
   ```

See "Deploying ArcSight Investigate and Event Broker images" on page 25.

8. Install the Vertica database.

   See "Installing the ArcSight Investigate Vertica database" on page 28.

9. Configure Event Broker.

   See "Configuring Event Broker" on page 26.

10. Configure the Investigate, including the Investigate Vertica database, SMTP server.).
    - See "Configure ArcSight Investigate and components" on page 32

11. Uninstall Investigate.

    See "Uninstall ArcSight Investigate" on page 38

Planning your deployment

Before deploying, ensure that you have the latest version of this document, available for download from the ArcSight Product Documentation Community on Protect 724.

TLS planning

The various components in the ArcSight Investigate system interact using encrypted communication implemented using TLS 1.2 protocol.

TLS implementation requires digital certificates. Before you begin the installation process, you must decide on the type of certificate you prefer to use:

- Kubernetes self-signed certificate. Kubernetes includes the capability to generate self-signed certificates. By default, the Kubernetes installation process generates certificates for the Kubernetes cluster, but you can instruct otherwise during the installation process. You can also generate a Kubernetes certificate for other components in the system, which require a certificate, like the ArcSight Investigate Vertica database. For more information on generating a Kubernetes certificate, see Generate signed certificates for consumers.
- A valid digital certificate signed by a certificate authority (CA). Depending on your organization's security policy, you might be required to use a certificate from a trusted CA. In this case, make sure that you have a root certificate file and a private key file. Copy these files to the designated Kubernetes master node.

Note: The certificates cannot be reconfigured after installation.

If you are planning on enabling FIPS mode, make sure the certificate generated meets the FIPS criteria.

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.

Set up encryption modes before installing and configuring Investigate and Event Broker

Before installing Investigate and 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 ArcSight Investigate 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 ArcSight Investigate 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*

Product	Preparations needed	Open ports	Supported encryption modes	Guidance documentation
ArcSight ESM (optional)	ArcSight ESM can be installed and running prior to installing ArcSight Investigate and Event Broker. ESM ingests events faster than Investigate does. (Investigate Scheduler ingests events at 22K per second while ESM ingests events at 30K per second.) You can leave the ingestion rate asynchronous, or you can equalize them by setting the ESM ingestion rate to a lower rate at the connector so that Investigate and ESM ingest rates are closer. This will reduce the likelihood of a lag in search results on Investigate launched from ESM.	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*

Chapter 2: ArcSight Investigate support matrix

Supported operating systems

Version	Component	Operating system
2.0	ArcSight Investigate	RHEL 7.3 64-bit* RHEL 7.4 64-bit CentOS 7.3 64-bit* CentOS 7.4 64-bit * Linux kernel version 3.10.0-514.26.2.el7.x86_64 (or above)
	ArcSight Investigate Vertica 8.1.1-3 database	RHEL 7.3 and CentOS 7.3

Supported browsers

Browser	Version
Microsoft Edge	Version available at the time of release.
Microsoft Internet Explorer	Version available at the time of release.
Google Chrome	Version available at the time of release.
Mozilla Firefox	Version available at the time of release.

Supported product compatibility

Product	Version
ArcSight Event Broker	2.1
ArcSight SmartConnector	7.5 and later
ArcMC	2.7
ArcSight Logger	6.5
ArcSight ESM	6.11

Chapter 3: Prerequisites for installation

- Ensure that Event Broker and Investigate have a dedicated server.

  If other applications are running on the same server as Event Broker and Investigate, there will be a performance penalty and potential problems.
- Ensure that your file system type is ext4.

System requirements

This information provides general sizing guidelines based on a default setup. For tailored sizing recommendations for a production environment, contact ArcSight Customer Support.

Provision the servers (or VMs) that you are using for the deployment with the following. For supported platforms and operating systems, see the ArcSight Investigate Support Matrix.

Component	Nodes	Resources needed	Needed ports
ArcSight Investigate + Event Broker	1 master 3 worker	• One CPU with 24 cores • 32 GB RAM • 8 TB disk space • Linux kernel version 3.10.0-514.26.2 (or above) • Java (OpenJDK) 1.8.0_121 or higher • Method for obtaining Docker containers, either via Internet (or proxy) or other internal method • 10 GigE network	Kubernetes: 2379, 2380, 4001, 4194, 5000, 5443, 8080, 8088, 8200, 8285, 8443, 10248-10252, 10255, 30001 Network File System (NFS): 111, 2049, 20048, 37189 For required Event Broker ports, see "System requirements" in the *HPE Security ArcSight Data Platform Event Broker Deployment Guide*. Investigate: 5443, 21085, 30001
Investigate Vertica database	3	**Important:** The Vertica database must be installed on the same sub-network as the Investigate master and worker nodes. • 2 CPUs with 24 cores • 128 GB RAM • 8TB disk space • 10 GigE network minimum (dual recommended) Recommendation: Install Vertica on a dedicated physical server, for example HPE Proliant G9 or similar Virtual environment: HPE Vertica performs better on a physical server than in a virtualized environment because of the overhead and resource constraints imposed by the virtualization software. See HPE Vertica Analytics Platform Version 8.1.x Documentation for more information.	5433
Vertica scheduler			
ArcMC (part of ADP)	1	• One CPU quad-core • 16 GB RAM • 50 GB of free disk space For ArcMC deployment details, see the *ArcMC Administrator's Guide*.	
SmartConnectors (part of ADP)	1	SmartConnector version 7.5 (can be stand-alone or managed by ArcMC) For ArcSightSmartConnector deployment details, see the *SmartConnector User's Guide*.	

Default heap size

Following are the heap memory usage settings for Event Broker modules at the JDK level. These levels are not configurable.

Module Name	Default heap sizes
Schema Registry	1 GB
Kafka	4 GB
Kafka Manager	1 GB
c2av stream processor	2 GB
Routing stream processor	2 GB
Web Service	2 GB

Disabling SELinux

About

Disable Security-Enhanced Linux (SELunix) .

Procedure

1. Configure `SELINUX=disabled` in the `/etc/selinux/config file.`
2. Reboot your system.
3. Confirm that the `sestatus` command returns `Disabled.`

Increasing per-user process limits

Procedure

1. Do the following on every Vertica and Kubernetes 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 Kubernetes master and worker nodes, and Vertica nodes.

   Nodes can be rebooted in any order.

4. Verify that all nodes are up and running by running the following command.
   `ulimit -a`

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
- **Investigate:** 5443,21085,30001

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

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
   ```

Generating a key pair on the master node for worker nodes

About

In a master and worker node deployment, generate a key pair on the master node and then copy the public key to each worker node. This enables password-less SSH access from the master server to all the other worker node servers in the cluster. Do this before you install the ArcSight Installer, and before you install and setup Kubernetes.

The following is an example of enabling password-less SSH. For additional examples, see http://www.linuxproblem.org/art_9.html

Note: Generate the key pair as a root user or sudo user.

Procedure

1. Run the `ssh-keygen` command on the master server.

   Example:

   ```
   ssh-keygen -q -t rsa
   ```
2. Copy the key from the master node to the worker node using the worker node's IP address.

   Example:

   ```
   ssh-copy-id -i ~/.ssh/id_rsa.pub root@11.111.111.111
   ```
   The system displays the key fingerprint and requests to authenticate with the node server.
3. Enter the worker node credentials as required.

   The operation is successful when the system displays the following message:

   ```
   Number of key(s) added: 1
   ```
4. To verify that the key was successfully installed on the worker node, run the following command from master to the worker node to verify that it can successfully log into the worker node.

   ```
   ssh 'root@11.111.111.111'
   ```
5. Repeat steps 2 through 4 for every worker node.

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>"
```

Chapter 4: Install ArcSight Investigate and Event Broker

The ArcSight Installer is used to install ArcSight Investigate and Event Broker. Before running the ArcSight Installer, verify that you have set up the receiving systems according to guidelines in Investigate and Event Broker prerequisites. Multi-master installation is not supported.

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

This user guidance provides instructions for installing online using the Docker Hub repository, or offline by downloading a tar file from an FTP site and replicating a local Docker Hub on the master node system.

Installing the ArcSight Installer

About

The ArcSight Installer will enable the deployment of ArcSight products, such as Event Broker and ArcSight Investigate.

Prerequisites

1. Update `/opt/arcsight/installer/arcsight-installer.properties` (see "Adjusting ArcSight Installer properties" on page 20).
2. Obtain an Investigate Docker Hub 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 Investigate license and privileges on Docker Hub.
      - You now have access to your Docker Investigate 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 (sudo to root)

Procedure

1. Login in to the master node.
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.

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

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

Labeling nodes

Procedure

SSH to the master node and label all nodes.

- `kubectl label --overwrite node {masternode_ip} investigate=yes`
- `kubectl label --overwrite node {workernode1_ip} kafka=yes zk=yes`
- `kubectl label --overwrite node {workernode2_ip} kafka=yes zk=yes`
- `kubectl label --overwrite node {workernode3_ip} kafka=yes zk=yes`

For Kafka and Zookeeper, ensure that the number of the nodes you labeled correspond to `eb-kafka-count and eb-zookeeper-count` properties from the `/opt/arcsight/installer/arcsight-installer.properties` file. Default number is three.

Managing nodes

About

Once you add a master and three worker nodes, you can view their status in the Node Management page. The labels you assigned to the nodes are also viewable from this page.

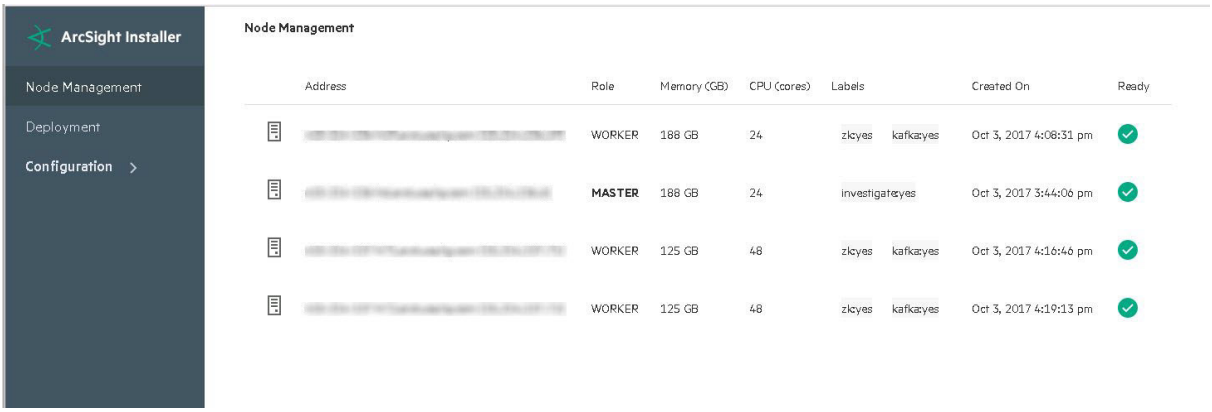
Other node information, such as address, memory, CPU and date create are viewable from the Node Management page.

Procedure

Location: ArcSight Installer > left navigation > Node Management > Node Management page

1. Login to the ArcSight Installer (UI page) and change the password.
   - Enter the default credentials admin/cloud. After the first successful login, you are required to change the admin password.
   - From the ArcSight Installer (UI page), you can see that **Node Management** in the left navigation.

2. Go to the Node Management page and check that three worker nodes are running and all have the status of READY (see "Managing nodes" on the previous page).



Adjusting ArcSight Installer properties

The arcsight-installer.properties file controls several important settings for your Event Broker installation. Those settings are detailed here. Before deploying Kubernetes, edit the properties file, `/opt/arcsight/installer/arcsight-installer.properties`, as needed for your environment.

You will need to adjust the properties set if you are deploying in FIPS mode, or adding more worker nodes to the default configuration.

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.

Note: To change optional property values, remove the comment operator (#) and then make the desired change.

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	

Setting	Notes
#eb-init-noOfTopicPartitions=6	Default value. Will only affect newly created topics. (Add new partitions to existing topics with the Event Broker Manager.) By making the number of partitions a multiple of the Vertica nodes, the copy commands are evenly distributed among the Vertica nodes. The default is 6, because there are 3 vertica nodes.
## 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. Very small, will definitely require customer adjustment. Requires calculation on customer behalf. Deletion will occur when EB hits either the duration or retention bytes, whichever comes first.
## 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. Requires calculation on customer behalf. 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.
##The replication factor for the offsets topic #eb-init-kafkaOffsetsTopicReplicationFactor=3	
## Kafka inter-broker protocol version	
#inter-broker-protocol-version=0.11.0.0	Only to be used during upgrades.

Setting	Notes
## 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 labelled 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 labelled as zk=yes in K8s. 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.
#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	If reverse DNS is not set up correctly, can be blank. Hostname verification for Kafka to Kafka connections.
## The number of stream threads	
#stream-num-threads=6	Do not change unless performance issue.
##truncate fields in c2av	
#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.

Setting	Notes
# 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	
## 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	
## Host path directory for AutoPass license data file persistence # eb-autopass-path=/opt/arcsight/k8s-hostpath-volume/eb/autopass	Path to valid Event Broker License

Obtaining ArcSight Investigate and Event Broker images (online)

About

Download the Investigate images and Event Broker images.

Procedure

1. Obtain Investigate.
   a. Download Investigate images.
      ```
      cd /opt/arcsight/kubernetes/scripts
      ./downloadimages.sh --suite investigate -r docker -o arcsightsecurity
      ```
   b. Pick the 2.00 version.
   c. Upload the images to the local Docker registry.
      ```
      ./uploadimages.sh --suite investigate
      ```
2. Obtain Event Broker.
   a. Download Event Broker images.
      ```
      cd /opt/arcsight/kubernetes/scripts
      ./downloadimages.sh --suite eventbroker -r docker -o arcsightsecurity
      ```
   b. Pick the 2.10 version.
   c. Upload the images to the local Docker registry.
      ```
      ./uploadimages.sh --suite eventbroker
      ```

Obtaining ArcSight Investigate and Event Broker images (offline)

About

Obtain the Investigate and Event Broker images tar files from the ArcSight FTP server.

Procedure

Investigate

1. Download the `arcsight-investigate-*.tar` file.
2. Place the `arcsight-investigate-*.tar` file in `master:<offline install directory>`.
3. Upload Investigate images.
   ```
   cd <offline install directory>
   tar xvf arcsight-investigate-*.tar
   ```
   All Investigate related images will be stored in the `./investigate` directory.
   ```
   cd/opt/arcsight/kubernetes/scripts
   ./uploadimages.sh -s investigate -d <offline install
   directory>/investigate
   ```

Event Broker

1. Download the `arcsight-eventbroker-*.tar` file.
2. Place the `arcsight-eventbroker-*.tar` file in `master:<offline install directory>`.

3. Upload Event bBroker images.

   ```
   cd <offline install directory>
   tar xvf arcsight-eventbroker-*.tar
   ```

   All Event Broker related images will be stored in the `./eventbroker` directory.

   ```
   cd/opt/arcsight/kubernetes/scripts
   ./uploadimages.sh -s eventbroker -d <offline install
   directory>/eventbroker
   ```

ArcSight Installer tasks

From the ArcSight Installer UI, you can check the status of the master and worker nodes, deploy the Investigate and Event Broker images, and configure Investigate and Event Broker.

Deploying ArcSight Investigate and Event Broker images

About

Products ready for deployment, Investigate and ArcSight Event Broker, are located in the Deployment page with an initial status of **OFF**.

Procedure

Location: ArcSight Installer > left navigation > Deployment > Deployment page

1. Click **Deploy** for ArcSight Investigate, then click 2.00.

   A green circle containing a check mark appears. This indicates that the deployment is in progress.

   Click **Deploy** for ArcSight Event Broker. Then click 2.10.

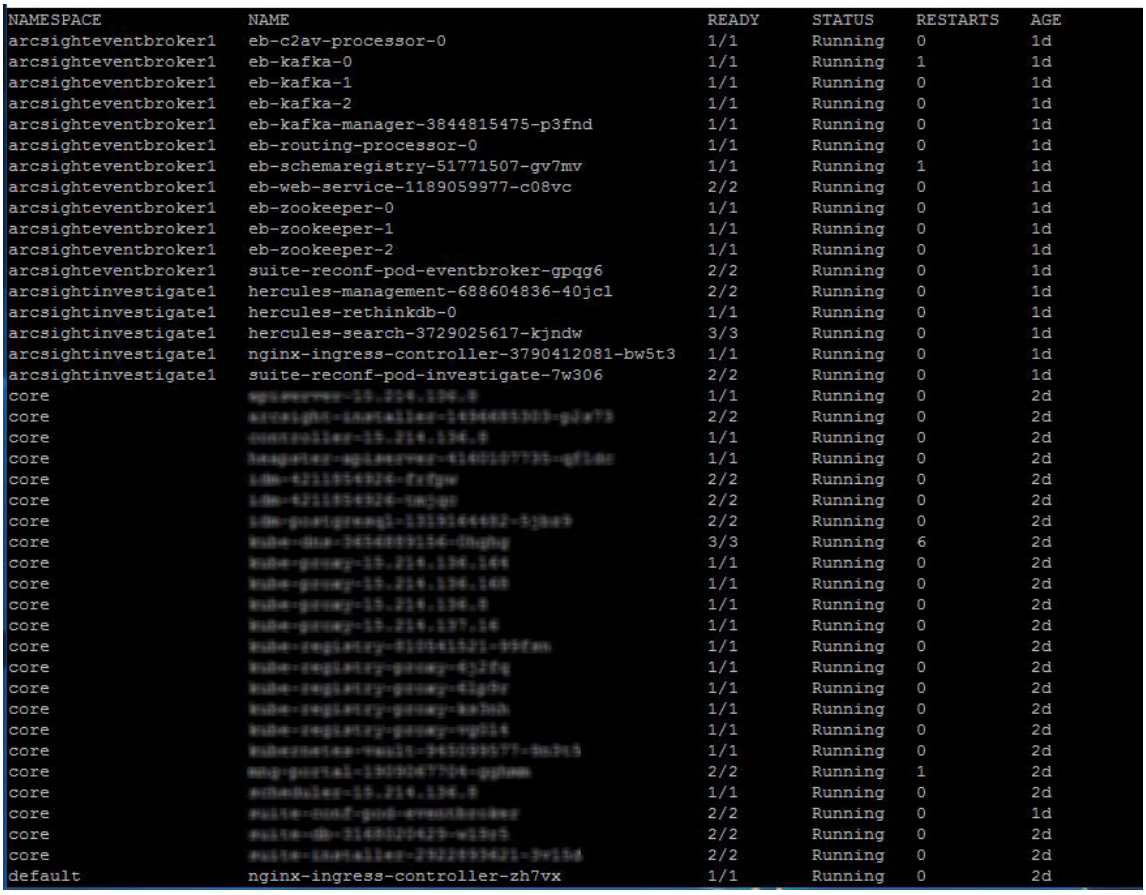
   A green circle containing a check mark appears. This indicates that deployment is in progress.

2. To check the deployment status:

   a. Run `$kubectl get pods --all-namespaces` on the master node.

      When deployment is complete, all pods should be in the running state, as shown in the example below.

      Note: It may take 2-5 minutes for all pods to start running.



NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
arcsighteventbroker1	eb-c2av-processor-0	1/1	Running	0	1d
arcsighteventbroker1	eb-kafka-0	1/1	Running	1	1d
arcsighteventbroker1	eb-kafka-1	1/1	Running	0	1d
arcsighteventbroker1	eb-kafka-2	1/1	Running	0	1d
arcsighteventbroker1	eb-kafka-manager-3844815475-p3fnd	1/1	Running	0	1d
arcsighteventbroker1	eb-routing-processor-0	1/1	Running	0	1d
arcsighteventbroker1	eb-schemaregistry-51771507-gv7mv	1/1	Running	1	1d
arcsighteventbroker1	eb-web-service-1189059977-c08vc	2/2	Running	0	1d
arcsighteventbroker1	eb-zookeeper-0	1/1	Running	0	1d
arcsighteventbroker1	eb-zookeeper-1	1/1	Running	0	1d
arcsighteventbroker1	eb-zookeeper-2	1/1	Running	0	1d
arcsighteventbroker1	suite-reconf-pod-eventbroker-gpqg6	2/2	Running	0	1d
arcsightinvestigate1	hercules-management-688604836-40jc1	2/2	Running	0	1d
arcsightinvestigate1	hercules-rethinkdb-0	1/1	Running	0	1d
arcsightinvestigate1	hercules-search-3729025617-kjndw	3/3	Running	0	1d
arcsightinvestigate1	nginx-ingress-controller-3790412081-bw5t3	1/1	Running	0	1d
arcsightinvestigate1	suite-reconf-pod-investigate-7w306	2/2	Running	0	1d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	2/2	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	2/2	Running	0	2d
core	[redacted]	2/2	Running	0	2d
core	[redacted]	2/2	Running	0	2d
core	[redacted]	3/3	Running	6	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	2/2	Running	1	2d
core	[redacted]	1/1	Running	0	2d
core	[redacted]	2/2	Running	0	1d
core	[redacted]	2/2	Running	0	2d
core	[redacted]	2/2	Running	0	2d
default	nginx-ingress-controller-zh7vx	1/1	Running	0	2d

3. To remove a product and all its containers from Kubernetes, click **Undeploy**.

Configuring Event Broker

About

Once you deploy Event Broker, you can then configure the product from the Configuration page of the Installer.

Procedure

Location: ArcSight Installer > left navigation > Configuration

- To configure ArcSight Event Broker
  a. Select **Event Broker**.
  b. Select Replicas.
  c. Click **+** next to Transforming String Processor and click **Save**. The number will change from 0 to 1.

Chapter 5: Install Vertica

Requirements for provisioning the Vertica server

- No LVM partition
- Partition type: ext4
- Minimum 2 GB swap space
- RHEL 7.3 or CentOS 7.3 only

Prerequisites for Installing Vertica

- Review the system requirements for ArcSight Investigate Vertica Database.
- Increase default user process limit by following the instructions in "Increasing per-user process limits" on page 14

Generating the SSH key pair

About

Generate a key pair on node 1 and then copy the public key to all nodes, including node 1. This enables password-less SSH access from the node 1 server to all the other node servers in the cluster.

Procedure

1. On the node 1 server, run the `ssh-keygen` command.

   Example:

   ```
   ssh-keygen -q -t rsa
   ```
2. Copy the key from node 1 to all nodes, including node 1, using the node IP address.

   Example:

   ```
   ssh-copy-id -i ~/.ssh/id_rsa.pub root@11.111.111.111
   ```
   The system displays the key fingerprint and requests to authenticate with the node server.
3. Enter the required credentials of the nodes.

   The operation is successful when the system displays the following message:

   ```
   Number of key(s) added: 1
   ```
4. To verify that the key was successfully installed on the node, run the following command from node 1 to the target node to verify that it can successfully log into the node.

```
ssh 'root@11.111.111.111'
```

5. Repeat steps 1 through 4 for all nodes.

Setting security-enhanced Linux (SELinux) to permissive

About

This procedure is needed for the Vertica host only.

Procedure

1. Set SELinux to permissive.
   a. SElinux status is enabled by default. To check status, check the file `/etc/sysconfig/selinux`:

      ```
      vi /etc/sysconfig/selinux <command>
      ```

   b. If `SELinux=enforcing`, then change to `SELinux=permissive`.
   c. Save and exit the file.
   d. Reboot the server.

Disabling the firewall

About

This procedure is needed for the Vertica host only.

Procedure

1. Disable firewall on the Vertica system.
   a. To check firewall status, run the following command on the operating system as a root:

      ```
      systemctl list-unit-files | grep firewall
      ```

   b. If return status is “firewalld.service enabled”, then run the following command:

      ```
      systemctl stop firewalld
      ```

      ```
      systemctl disable firewalld
      ```

Installing the ArcSight Investigate Vertica database

Procedure

Prerequisite

Generate a key pair on the Vertica cluster node 1 (see "Install Vertica" on page 27).

1. On the node 1 server, create a folder for the ArcSight Investigate Vertica Database:

   `mkdir /root/install-vertica/`
2. Copy the Investigate Vertica Database scripts:

   `arcsight-investigate-vertica-scripts.<hash>.tar.gz to /root/install-vertica`

   `arcsight-investigate-vertica-scripts.<hash>.tar.gz.md5`
3. Verify that the tarball matches the MD5 checksum:

   `cd /root/install-vertica`

   `md5sum arcsight-investigate-vertica-scripts.<hash>.tar.gz`

   `cat arcsight-investigate-vertica-scripts.<hash>.tar.gz.md5`

   Both outputs should match.
4. Extract the tar file:

   `tar xvfz arcsight-investigate-vertica-scripts.<hash>.tar.gz`
5. Edit the `vertica.properties` file.

   The `hosts` and `license` properties must be updated while the other properties are optional.

Property	Value
# environment settings	
ssh_private_key	/root/.ssh/id_rsa
timezone	Your timezone according to the format in: /usr/share/zoneinfo/ of Linux systems. For example, US/Pacific, Europe/Prague, Japan. "UTC" is the default setting.
# vertica settings # please be sure not to use loop-back addresses in case cluster would need to be performed.	
hosts	A comma separated list of the Investigate Vertica Database servers in IPv4 format (1.1.1.1)
license	Download the license file from the Software Entitlements portal. Place the license file on your filesystem, and then point to this file from license parameter.
rpm	/root/install-vertica/data/vertica-8.0.1-5.x86_64.RHEL6.rpm
dba_user	<dbadmin> Encrypted value provided during Vertica installation
database	investigate
dbpassword	<dbadmin> Encrypted value provided during Vertica installation

Property	Value
ssl_enable=1	Use this option if your database supports an SSL connection
# Database users # DBadmin	
dba_user	Database administrator
dba_password	Database administrator password
# search	
search_user	Search user for ArcSIght Investigate
search_password	Search user password for ArcSIght Investigate
## Tune DB Tupple Mover (TM) to for best ingestion performance, recommended: 4 active partitions, 5 threads for TM, 6000 MB for TM 5 threads for TM, 6000 MB for TM ## Use scripts/tuning_util.sh to modify below values after installing vertica	

active_partitions=4
tm_concurrency=5
#value in MB
tm_memory=6000
	Database tuning parameters

use_p2p=1	Use this option in case your infrastructure does not support broadcast messaging or your nodes are not located on the same subnet. You should also use this option for all virtual environment installations, regardless of whether the virtual servers are on the same subnet or not.

6. Run the following command to install Vertica.

   ```
   ./vertica_installer install
   ```

   You will be promptes to set up two users, a database administrator and an investigate search user.

   After installation completes, safeguard your database admin credentials.

7. Run the following command to create the schema and database tables.

   ```
   ./vertica_installer create-schema
   ```

8. Run the following command to create a scheduler and related schema and tables.

   ```
   ./kafka_scheduler create <EB Worker Node 1 IP>:9092,<EB Worker Node 2 IP>:9092,<EB Worker Node 3 IP>:9092 number_of_partitions
   ```

Note: `number_of_partitions` default is 6. However, it should match with the number defined in Event Broker master file, `/opt/arcsight/installer/arcsight-installer.properties`:

`predeploy.eb.init.noOfTopicPartitions`

9. The Kafka Scheduler supports the following commands:

Action	Command	Description
Stop	./kafka_scheduler stop	Stops all running scheduler instances
Start	./kafka_scheduler start	Starts scheduler for all Kafka instances registered after performing a stop operation first.
Create	./kafka_scheduler create <EB Worker Node 1 IP>:9092,<EB Worker Node 2 IP>:9092,<EB Worker Node 3 IP>:9092 number_of_ partitions	Creates a new Kafka scheduler
Status	kafka_scheduler status host1:9092	Presents the status of running Kafka scheduler including count of imported/rejected messages
Delete	kafka_scheduler delete	Deletes the meta data. After doing this, immediately run the kafka_scheduler create command.

10. Run `./kafka_scheduler` status to check the Vertica status.

See Also

ArcSight Investigate deployment troubleshooting and FAQs

Chapter 6: Configure ArcSight Investigate and components

Once you deploy ArcSight Investigate, you can then configure the product from the Configuration page of the Installer. After changing a product setting, Investigate restarts. Wait until restart completes before logging into Investigate.

Establishing the system admin

About

When you log in to ArcSight Investigate for the first time, you need to create the first user in the system. This user is assigned the system admin role.

Procedure

1. Open `https://master-ip`
2. From the Welcome page, enter the name, email, and password information for the system admin and then click **Create System Admin**.
3. From the Login page, enter the credentials for the system admin.

Configuring the ArcSight Investigate Vertica database connection in the ArcSight Installer

Procedure

Location: ArcSight Installer

1. Click **Configuration > Investigate > Vertica**.
2. Enter the following information and then click **Save**:
   - Vertica host — Vertica node 1 IP
   - Vertica user name — See step 6 in "Installing the ArcSight Investigate Vertica database" on page 28.
     This is the Investigate search user name.
   - Vertica database — Investigate (hard-coded.)
   - Vertica password — See step 6 in "Installing the ArcSight Investigate Vertica database" on

page 28
This is the Investigate search user password.

Configuring the SMTP server inArcSight Installer

About

Configure access to your SMTP server in ArcSight Installer to enable users that you create in ArcSight Investigate to receive notification emails.

Procedure

Location: ArcSight Installer

1. Go to **Configuration > ArcSight Investigate** and then click the **User Management** tab.
2. In the **User Management** tab, enter the following information and then click **Save**:
   - SMTP Host
   - SMTP Port
   - SMTP User Name
   - SMTP Password
   - Sender Address

Configuring session and search settings in ArcSight Installer

About

You can configure the following properties:

- Session timeout

  When the user session ends, the user is redirected to the login screen in order to log in again. The default session timeout is 60 minutes.
- Search query timeout

  Search queries may take a long time and impact performance. You can put a limitation on the amount of time a search query runs. The default search query timeout is 60 minutes.

Procedure

Location: ArcSight Installer

1. Click **Configuration > ArcSight Investigate**.
2. From the **General** tab, do the following:
   - In the **Session timeout** field, enter the maximum time (in minutes) that you want a session to run.
   - In the **Search query timeout** field, enter the maximum time (in minutes) that you want a search query to run.
3. Click **Save**.

Configuring TLS on the ArcSight Investigate Vertica database in the Vertica server

About

The components of the ArcSight Investigate system interact using encrypted communication implemented using the Transport Layer Security (TLS) cryptographic protocol. The components managed by the ArcSight Installer are deployed with encrypted communication. This procedure provides instructions for distributing the key and certificate files on all ArcSight Investigate Vertica Database nodes and enabling TLS on the database.

Requirements

- A valid digital certificate signed by a certificate authority (CA). This includes two files:
  - Server certificate file (server.crt)
  - Root certificate file (root.crt)
- Private key file (server.key)

Note: The database does not need to be running when you distribute the key and certificate files.

Procedure

1. Copy the .crt and .key files to one of the ArcSight Investigate Vertica Database nodes.
2. Run the Vertica Administration Tools, as described in Using the Administration Tools in the Vertica documentation.
3. From the Main Menu, select **Configuration Menu** and click **OK**.
4. In the **Configuration Menu** screen, select **Distribute Config Files** and click **OK**.
5. In the **Select a category of files to copy** screen, select **SSL Keys** and click **OK**.
6. In the **Select database** screen, select the database on which you want to distribute the files and click **OK**.
7. In the **Select files to install** screen, modify the file path to the location to which you copied the

files and click OK.

The names of the files should be:

- server.crt
- server.key
- root.crt

8. Run the Administration Tools again.

   In the Main Menu screen, select **Connect to Database** and click **OK**.
9. When prompted, enter the database password.
10. Run the following command: `ALTER DATABASE mydb SET EnableSSL = 1;`
11. Restart the database.

Configuring Vertica SSL

About

The ArcSight Installer contains the script, `/opt/arcsight/installer/k8s/master/cert-utils.sh` which provides a tool that enables you to generate a certificate signed by the root certificate authority used by Kubernetes and all modules.

Procedure

1. Connect to the master node (where installation were run) and run `./cert-utils.sh generate-certificate vertica => script` produce `vertica.key` and `vertica.crt`

   You can change `vertica` to your host name.
2. Copy `vertica.key` and `vertica.crt` to all Vertica nodes.

   It is also needed to copy there certificate of certificate authority (default `/opt/arcsight/kuberntes/ssl/ca.crt`)
3. On each node run the `su - -c adminTools dbadmin => vertica` Administration Tool.

   Use the user specified in Vertica configuration.
   a. From the **Main Menu** in the **Administration Tools**, select **Configuration Menu**, and then click **OK**.
   b. From the **Configuration Menu**, select **Distribute Config Files** and then click **OK**.
   c. Select SSL Keys and then click **OK**.
   d. Select the database on which you want to distribute the files (the database from configuration), and then click **OK**.
   e. Add the file locations for the `vertica.crt`, `vertica.key` and `ca.crt` (certificate authority certificate) files, and then click **OK** to distribute the files.

See Also

https://my.vertica.com/docs/8.0.x/HTML/index.htm#Authoring/Security/SSL/ConfiguringSSL.htm

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

Chapter 7: Generate signed certificates for consumers

Event Broker consumers need a signed certificate from the Event Broker to establish secure communication.

There are a number of methods for generating signed certificates. Each used for different use cases:

- ArcSight Installer includes a utility for generating a signed certificate from the CA that is configured in the system (either Kubernetes or another trusted CA). You can use this utility to generate certificates for other components in the system, such as the ArcSight Investigate Vertica database.
- ArcSight Installer includes a utility for generating a signed certificate from a Certificate Signing Request (CSR) file. You can use this utility to generate certificates for client authentication, such as ESM and Logger.

Note: You can perform these procedures only after Kubernetes is installed.

Chapter 8: Uninstall ArcSight Investigate

About

Uninstalling ArcSight Investigate requires two basic steps:

- Uninstall ArcSight Installer.
- Uninstall Kubernetes.

Procedure

1. Uninstall Kubernetes.

   Run the following command on all the worker nodes and on the master server and then reboot:

   ```
   /opt/arcsight/kubernetes/uninstall.sh
   yes
   yes
   ```

   The system reboots automatically.

2. a. After the server reboots, run the following command on the master node.

      ```
      rm -rf /root/.kube /root/.docker
      ```

   b. On the worker node(s), run:

      ```
      rm -rf /root/.kube /root/arcsight-installer-worker
      ```

   Note: If you want to delete all your data as well, run the following command on all nodes.

   ```
   rm -rf /opt/arcsight /opt/kubernetes
   ```

See Also

ArcSight Investigate deployment troubleshooting and FAQs

Appendix A: ArcSight Investigate deployment troubleshooting and FAQs

Troubleshooting

Installing the ArcSight Installer Platform fails

Contact Technical Support.

Where to find the logs

To troubleshoot issues, capture the following logs. Logs are found under the pod number.

- zookeeper_container.log
- kafka_container.log
- schema-registry_container.log
- webservice_container.log

Pod starting order

After deploying Event Broker, pods are configured to start in the following order. Downstream pods will not start until the dependencies are met.

1. A quorum of zookeeper pods in the cluster must be up (2 of 3, or 3 of 5). Total number of zookeepers must be odd.
2. All Kafka pods must be up
3. Schema Registry pod must be up
4. Bootstrap Web Service, Kafka Manager
5. Transformation Stream Processor, Routing Stream Processor

Cannot query zookeeper

Symptom: when you run kubectl get pods command to get status of the pods and you see that downstream pods (see the pod star order) do not stay up and the status is a 'CrashLoop'-type error.

Conditions to look for:

- Check that zookeeper pods are running.
- If the zookeeper pod status is Pending, you may not have labeled the nodes (zk=yes). Verify that the nodes are labeled using the kubectl get nodes -L=zk command.
- Verify that you configured an odd number of zookeepers in arcsight-installer.properties predeploy.eb.zookeeper.count attribute.
- Check the zookeeper pod logs for errors using the kubectl logs <pod name>.

Common errors/warnings in Zookeeper logs

- Quorum Exceptions: Cannot elect a leader. If you see this type of error, check the check conditions above.
- Socket errors: this can occur if there are too many connections. The solution is to restart the pod using the kubectl delete <pod_name>. The pod will be recreated automatically.

SSL connection error

These are warnings that occur if there is a connection issue between Kafka and consumer or producer.

kubectl command is returning refused

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

Vertica Scheduler unable to read events from Kafka

- New set up: Vertica Kafka scheduler: Check that kafka scheduler is configured to communicate to Kafka port 39092.
- Working at first, but stopped working: Offset is not recognized: In this scenario, the kafka scheduler fails to recognize offset ids of messages that are in the topic. It can happen if the kafka scheduler unexpectedly stops reading from the topic, and then is restarted.
  Solution: execute the Kafka_scheduler delete command to delete the meta data. After doing this, immediately run the Kafka_scheduler create command to set up the scheduler.
- New set up: Check the network connection.
- New set up and existing set up: Check whether the broker is down.
- Existing set up: you did not configure all brokers that contain the topic the consumer connects to, and the brokers which are configured in that consumer are down.
- New set up: If you are encountering SSL connection related errors, check the steps that you used to import certificates to both Event Broker and consumers.

FAQs

Which pods in Kubernetes comprise the ArcSight Investigate deployment?

- Hercules pods: management, proxy, rethinkdb, search

Related topic: ArcSight Investigate and Event Broker prerequisites

Can I use my existing Event Broker v1.0 with ArcSight Investigate + Vertica?

No. ArcSight Investigate requires Event Broker 2.0. You can migrate your data from Event Broker 1.0 using the Event Broker Data Migration utility. Check with ArcSight Support about the availability of this tool.

Related topic: *Event Broker Data Migration Tech Note*.

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 (Investigate 2.00)

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!