Hewlett Packard
Enterprise

HPE Security ArcSight Event Broker

Setup Guide

January, 2018

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements: https://community.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/support-contact-information
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://community.saas.hpe.com/t5/ArcSight/ct-p/arcsight

Contents

Setting Up ArcSight Event Broker

ArcSight Event Broker is available as an Amazon Machine Image (AMI) on AWS Marketplace. Each AMI contains a CentOs 7.4 operating system with ArcSight Event Broker for an AWS pre-installed software. You can launch an instance of this AMI to create an Elastic Compute Cloud (EC2) on AWS.

Types of Supported Instances

Sizing an EC2 involves estimating the hardware for an optimal ArcSight Event Broker platform.

It is recommended to use Event Broker with the instances that meet the following minimum requirements:

Product	Install Type	AWS Type	vCPUs	Memory(GiB)
Event Broker 2.10	Single node	m4.2xlarge	8	32 GiB

Note: Event Broker supports only a single node configuration. Clusters of multiple nodes are not supported on AWS.

Launching ArcSight Event Broker

1. From the left menu go to AWS Marketplace, search for ArcSight Event Broker 2.10 - CentOS 7.4 .

2. Filter by General Purpose and select m4.2xlarge.

3. From Configure Instance Details, modify all corresponding items to align the instance to your needs.

3.1 Go to **Advanced Details.** The EC2 has a pre-installed software of Event Broker.

To complete the installation, add the following code in the User data field:

Code
#!/usr/bin/env bash bash /opt/execute.sh > /opt/execute.log

To keep track of the installation process you can ssh to the AWS instance when it is running and execute the following command:

```
tail -f /opt/execute.log
```

Note: Make sure the right network, subnet and IPs are selected.

4. You may not need to modify any setting in **Add Storage**. If you choose to increase storage volume capacity, follow the Amazon procedure to extend EBS volume once the instance is launched. Refer to the AWS User Guide and search "expanding the storage space of an EBS volume on Linux."

5. Go to **Tag Instance**, click value and enter a name for the instance.

6. From **Configure Security Group**, add any custom rules required for your environment and open the following ports:

Inbound

Type	Use	Protocol	Port Range	Source	IP
SSH		TCP	22	My IP	0.0.0.0/0
HTTPS		TCP	443	My IP	0.0.0.0/0
HTTPS		TCP	443	My IP	::/0
HTTP		TCP	80	My IP	0.0.0.0/0
HTTP		TCP	80	My IP	::/0
Custom TCP		TCP	5443	My IP	0.0.0.0/0
Custom TCP		TCP	5443	My IP	::/0
Custom TCP		TCP	9092	My IP	::/0
Custom TCP		TCP	9092	My IP	0.0.0.0/0
ICMP	Installer	Echo Reply	N/A	My IP	0.0.0.0/0
ICMP	Installer	Traceroute	N/A	My IP	0.0.0.0/0
Custom TCP	ArcMC	TCP	38080	My IP	0.0.0.0/0
Custom TCP	ArcMC	TCP	9000	My IP	0.0.0.0/0
Custom TCP	ArcSight SmartConnectors	TCP	9093	My IP	0.0.0.0/0
Custom TCP		TCP	39092	My IP	::/0
Custom TCP		TCP	39092	My IP	0.0.0.0/0

Outbound

Type	Protocol	Port Range	Destination
All traffic	All	All	0.0.0.0/0

7. From **Review and Launch**, correct any settings (if required), by clicking Previous and go back to the proper screen for editing. If they are correct, click Launch.

8. Go to **Create a new key pair** and click **Download Key Pair**. The key pair is required for connecting to the instance remotely. More details can be found in AWS User Guide.

9. Click **Launch Instances**. Launching Event Broker AWS EC2 takes around 20 minutes. The progress can be monitored by accessing EC2's dashboard and clicking the Instances link on the left panel. Once the instance is running, you can continue with the configuration of ArcSight Event Broker for AWS.

Configuring ArcSight Event Broker

Once ArcSight Event Broker is deployed, you can configure the product from the Configuration page of the Installer. After changing a product setting, ArcSight Event Broker restarts.

Note: Wait until restart completes before logging in to ArcSight Event Broker

Logging in to the Installer Page

The installer page is available once the ArcSight Event Broker EC2 instance is launched completely, go to https://<master-ip>:5443 .

To finish the installation and configure your ArcSight Event Broker, you must change the admin password.

1. Log in to the ArcSight Installer (UI page) and change the password.

1.1 Enter the default credentials admin/cloud. After the first successful login,

you are required to change the admin password.

Deploying ArcSight Event Broker Images

ArcSight Event Broker is located in the deployment page with an initial status OFF.

1. Log in to https://<master-ip>:5443 and navigate to deployment page.

2. 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.

3. To check the deployment status:

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

    When deployment is completed, all pods should be in the running state.

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

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

Establishing the System Admin

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

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 credentials for the system admin.

Configuring Event Broker

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

1. Open https://<master-ip>:5443

2. From ArcSight Installer > Left navigation > Configuration, select ArcSight Event Broker.

4. Select Replicas.

5. Click + next to Transforming String Processor and click Save . The number will change from 0 to 1.

Troubleshooting ArcSight Event Broker on AWS

Associating your Instance with an Elastic IP.

If a persistent public IP address is required to be associated to and from instances , Amazon recommends using an Elastic IP address instead of a standard EC2-VPC

IP address. For more details, refer to AWS Elastic IP documentation .

Additional Information

For additional information on the use and operation of ArcSight Event Broker, see the HPE ArcSight product documentation, available from the HPE ArcSight support community at https://www.protect724.hpe.com

You can also reach HPE ArcSight Software Support at:
https://softwaresupport.hpe.com

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 Setup Guide (Event Broker)

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!