



Hewlett Packard
Enterprise

HPE Security ArcSight ESM for AWS

Software Version: 6.9.1

Setup Guide

April 26, 2017

Legal Notices

Warranty

The only warranties for HPE 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. HPE 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 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 HPE 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

© Copyright 2017 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

Support

Contact Information

| | |
|------------------------------|--|
| Phone | A list of phone numbers is available on the HPE ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list |
| Support Web Site | https://softwaresupport.hpe.com |
| Protect 724 Community | https://www.protect724.hpe.com |

Contents

| | |
|--|---|
| Setting Up ESM for AWS | 4 |
| Launching an Instance of ESM for AWS | 4 |
| Configuring ESM for AWS | 4 |
| Additional Information | 5 |
| Send Documentation Feedback | 6 |

Setting Up ESM for AWS

This document explains how to set up HPE ESM for AWS.

ESM for AWS is available as an Amazon Machine Image (AMI) on the AWS Marketplace. It contains an operating system with ESM for AWS software pre-installed. You can launch an instance of this AMI to create a virtual machine (Elastic Cloud 2 instance) on the AWS cloud.

Launching an Instance of ESM for AWS

This procedure assumes that you already have Amazon Web Services account.

1. Browse to the [AWS Marketplace](#) and login with your existing AWS account credentials.
2. In the AWS Marketplace section search for "ESM". Then, click **Select**.
3. On the next screen, in the **Filter by** field, select "Memory optimized" and "r3.2xlarge".
4. Click **Next: Configure Instance Details**. Skip this procedure, as there is no need to modify any setting on the Instance Details screen.
5. Click **Next: Add Storage**. There is no need to modify any setting on the **Add Storage** screen. If you choose to increase the capacity of secondary storage (EBS volume), follow the Amazon procedure to extend the EBS volume once the instance is launched. Refer to the AWS User's Guide topic on expanding the storage space of an EBS volume on Linux.
6. Click **Next: Tag Instance**. Then, in **Value**, enter a name for the instance.
7. Click **Next: Configure Security Group**. Then add any custom rules required for your environment.
8. Open port 8443 to access the ESM for AWS web interface.
9. Click **Review and Launch**. Review the configuration selections. Correct any incorrect settings by clicking **Previous** to return to the proper screen for editing. When the settings are correct, click **Launch**.
10. Create a new key pair and click **Download Key Pair**. Follow the instructions on screen to download the key pair. (The key pair is required for connecting to the instance remotely.)
11. Click **Launch Instances**. The ESM for AWS EC2 instance should be ready in few minutes. You can monitor the progress by visiting the EC2 dashboard and clicking the **Instances** link on the left panel.

Once the instance is in a running state, you can continue with the configuration of ESM for AWS.

Configuring ESM for AWS

Prior to configuration, make sure you have the following two items available:

- **ArcSight License file path**
- **Static IP Address (Elastic IP):** To obtain a static IP address, under the **Network & Security** section on the left panel, click **Elastic IPs**, and then click **Allocate New Address**. Note down the IP address created.

Use the following steps to configure ESM:

1. Connect to the EC2 console using the key file downloaded during instance creation. There are different ways of connecting to EC2 instances. Refer to the AWS User's Guide topic on connecting to your Linux instance. Once you are connected to the EC2 instance, ArcSight ESM configuration setup starts automatically.
2. Type in the time zone information and press Enter. The ESM First Boot Wizard starts. For more information, refer to the ESM Installation Guide, "Chapter 2: Installing on an Appliance." When prompted about the "Manager Host name", enter the static IP address you obtained at the beginning of this procedure.

Next Steps

Send logs to HPE ArcSight ESM and search for events.

1. The ArcSight ESM Instance has 2 Syslog SmartConnectors listening on UDP 514 and 515. Configure your devices and applications to send syslog events to the IP or hostname of the ArcSight ESM instance.
2. Use the ArcSight Command Center or the ArcSight ESM Console to view events.
3. If needed, deploy more SmartConnectors by launching the ESM AMI.

Additional Information

For additional information on the use and operation of ESM for AWS, see the HPE ArcSight product documentation, available from HPE ArcSight Product Documentation:

<https://www.protect724.hpe.com/community/arcsight/productdocs>.

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

Note: For environmental issues related to the Amazon cloud infrastructure, please contact Amazon AWS support at <https://aws.amazon.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 (ESM for AWS 6.9.1)

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!