Micro Focus Security ArcSight Logger for AWS

Software Version: 7.1

Setup Guide

Document Release Date: July, 2020
Software Release Date: July, 2020

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

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

Setting Up ArcSight Security Logger for AWS

Logger for AWS is available as an Amazon Machine Image (AMI) on the AWS Marketplace. It contains an operating system with Logger 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 Logger for AWS

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

1. Log in to the AWS Marketplace site with your existing AWS account credentials.
2. Type **ArcSight Logger** in the AWS search box and select the latest Logger version.
3. On the pricing tab, select **m4.2xlarge** as the EC2 instance type to verify the price and click **Continue to Subscribe**.
4. A new page will be displayed. Click **Accept Terms**.

   Note: The **Continue to Configuration** button will be grayed out while the subscription is processed.

5. Once the process is completed, click **Continue to Configuration** and then **Continue to Launch**.
6. A new page will be displayed. Make sure the **EC2 instance type** is m4.2xlarge.
7. In **Subnet Settings**, select a subnet to auto-assign public IPv4 address.

   Note: To verify if the subnet selected is enabled, go to VPC Dashboard> Subnets . Look for the subnets with **Auto-assign public IPv4 address** in "Yes".

8. Select or create a **Security Group**. To create a new security group, click **Create New Based On Seller**.
9. Click **Launch**. The following message will be displayed: *Congratulations! An instance of this software is successfully deployed on EC2*.
10. To review the list of instances, click the **EC2 Console** hyperlink in the page.

    Note: Save the AMI ID value for the instance created. This identifier will allow you to track your instance once you open the instances list.

11. Make sure the instance is running before **Configuring Logger for AWS**.

Configuring Logger for AWS

Perform the following steps to set a new password for the admin account, and then update the license key.

1. Locate the public or private IP address assigned to the Logger for AWS EC2 instance. Then, `ssh -i <private_key> <user>@<aws-assigned-address> .`

Note: Default user should be **centos**.

2. Using sudo access, change the user to **arcsight**.

3. Start the application by running the following command:
`/opt/arcsight/current/arcsight/logger/bin/loggerd start`

4. Execute the `head -1 /var/log/boot.log` to view the initial admin password or go to the first line of `/var/log/boot.log`.

Note: Actual `var/log/boot.log` file name is time stamped and will look like `/var/log/boot.log -20190221`.

5. Set a new password for the admin account at: https://<awsassigned- ip-orhostname>:9000/

- Username: admin
- Password: Logger for AWS will request a password change after the first login.

6. Enable the port 9000 following these steps:

- On **Services > EC2 > Running Instances**, select your VM and click the **Security group** name.
- A new page is displayed. Click the **Inbound** tab.
- Click **Edit** and then **Add Rule**.
- Add the following details:

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	9000	Custom : 0.0.0.0/0	* Add a description

* Description is an optional field.

- Click **Save**.

7. Update the license key of the Logger for AWS instance.

Note: After you upload the license, manually reboot the software. Select the **arcsight** user and run the following command to start Logger:

```
/opt/arcsight/current/arcsight/logger/bin/loggerd start.
```

Setting an AWS Destination using S3FS for mounting

S3FS enables you to mount an Amazon S3 bucket as a local filesystem and mount on Logger for storing. Follow the steps described below.

Step 1: Create an AWS bucket

1. Sign in to the AWS Management Console.
2. Select the Amazon S3 console.
3. Select the create bucket option and add the specific details: **Name**, **Region**, and **Settings**.
4. Select create bucket.

Step 2: Download and configure S3FS

The S3FS syncs the folder content with the AWS Bucket. S3FS can be installed in a machine or the Logger (Software). Make sure to follow the steps below.

1. Install S3FS on the machine you want to mount.

   For a S3FS pre-installation on RHEL and CentOS 7 or newer, run the following command:

   ```
   sudo yum install epel-release
   sudo yum install s3fs-fuse
   ```

2. Create a file for your credentials. Update the credentials path if needed (default is `/etc/passwd-s3fs`).
3. Set your password credential using the following format.

   ```
   accessKeyId:secretAccessKey
   ```

4. Save the file and change the permissions.

   ```
   sudo chmod 600 [credentials path]
   sudo chmod 640 [credentials path]
   ```

5. Create a folder for mounting.
6. Create the mount.

Step 3: Configure Logger

Once `/opt/s3fsMount/` is synced with the AWS S3 Bucket, you need to add a NFS mount to enable Logger storing archives in that folder.

For Logger Appliance, it is required to add a NFS mount based on the S3FS mount. For further details on how to add a remote file system, see *Managing a Remote File System* available at Logger Administration Guide.

On Logger Software, see *Archive Storage Settings* available at Logger Administration Guide for instructions on how to set up an archive storage.

Next Steps

Send logs to Micro Focus ArcSight Logger and search for events.

1. The ArcSight Logger instance has 2 Syslog SmartConnectors on UDP Receiver 8514 and TCP Receiver 8515. Configure your devices and applications to send Syslog events to the IP or Hostname of the ArcSight Logger instance.
2. Use ArcSight Logger to search for events.
3. If needed, deploy more SmartConnectors by launching the ArcMC image from the Marketplace.

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 Setup Guide (Logger for AWS 7.1)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!