



Micro Focus Security

ArcSight Logger for AWS

Software Version: 7.0

Setup Guide

Document Release Date: January, 2020

Software Release Date: January, 2020

Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

US Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the US Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 CFR. 122.12 (Computer Software) and 122.11 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the US Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 CFR. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This US Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are US registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

- Setting Up ArcSight Security Logger for AWS 5
 - Launching an Instance of Logger for AWS 5
 - Configuring Logger for AWS 6
 - Additional Information 7

- Send Documentation Feedback 8

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 `tail /var/log/boot.log` to view the initial admin password.

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.
```

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.

Additional Information

For additional information on the use and operation of ArcSight Transformation Hub, see the Micro Focus ArcSight product documentation, available from the Micro Focus ArcSight support community at [Micro Focus Community](#)

You can also reach Micro Focus ArcSight Software Support at: <https://softwaresupport.softwaregrp.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 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 7.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!