Micro Focus Security ArcSight Logger for AWS

Software Version:

Setup Guide

Document Release Date: May, 2019
Software Release Date: May, 2019

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 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 "ArcSight Logger". Then, click Select.

3. On the next screen, in the Filter by field, select Memory optimized and m4.2xlarge.

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 9000 to access the Logger 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 Logger 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 cancontinue with the configuration of 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' user.

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

4. Execute '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. Browse to the web UI at: https://<awsassigned- ip-orhostname>:9000/

Username: admin

Password: (Note that a password change is forced on first login)

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

7. Continue product configuration as described in the Logger for AWS documentation.

Next Steps

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

1. The ArcSight Logger 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 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 ArcSightEvent Broker, 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 (Investigate Database)

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!