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 Logger for Azure

Micro FocusLogger is available for deployment from the Azure Marketplace. It is designed as a virtual appliance containing the required operating system and the Logger software pre-installed.

Launching an Instance of Logger

This procedure assumes that you already have an Azure portal account.

1. Log in to the Azure Marketplace site with your existing Azure credentials.
2. Click New, and then, in the search box, enter Micro Focus Logger.
3. In the search results, pick the latest version of Logger.
4. Select a Deployment Model, and then click Create.
5. Enter the basic details about the virtual machine on the next screen such as Name, User Name, SSH public key, Resource Group, Location, and so on. Then, click OK.

   Note: Username must be entered as "centos". Recommended size for Logger instance is B8ms.
6. Choose a size and click Select.
7. Optionally, edit the Settings as needed, and click OK.
8. All inputs will be validated, and if the validation is passed, click OK to continue.
9. On the next screen, accept the purchase agreement and click OK button to start the virtual machine deployment.

Once the virtual machine is ready (in the running state), connect with SSH as "centos" user and the password or SSH key provided during the deployment of the virtual machine.

Configuring Logger for Azure

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 Azure VM. Then, ssh -i <private_key> <user>@<azure-assigned-address>
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://<azureassigned-ip-or-hostname>:9000/

   Username: admin

   Password: (Note that Logger for Azure will force a password change on first login)

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

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!