Micro Focus Security ArcSight Logger for Azure

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

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 Azure

Micro Focus Logger 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 for Azure

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. Type Micro Focus Logger in the search box.
3. Select the latest version of Logger from the search results and click **Get It Now**.
4. A message window will be displayed. Click **Continue**.
5. In the Azure Portal, click **Create**.
6. Under the **Basics** tab, enter the following details about the virtual machine: **Subscription**, **resource group**, **virtual machine name**, **region**, **image**, **size**, **username**, **password** or **SSH public key**.

   Note: Username must be entered as "centos". Recommended size for Logger instance should be at least B4ms.

7. To continue editing the other tabs, click **Next**. Otherwise, click **Review + Create**.
8. After all inputs have been validated, a message will be displayed. Click **Create** to start the virtual machine deployment.
9. Once the VM is ready, connect to it via SSH as **centos** user. Make sure to use the password or SSH key previously added in step 6.
10. To connect, restart or see more detailed information about your VM, click the **Go to Resource** button.

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**.
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: Azure Portal
   - Username: Admin
   - Password: Logger for Azure will request a password change after the first login.
6. Enable the port 9000 following these steps:
   - Go to the VM Overview in Azure. In **Settings**, select **Networking**.
   - Click **Add inbound port rule**.
   - In the **Destination port ranges**, type **9000**. To later identify the port added, update the **Name** field.
   - Click **Add**.
7. Update the license key of the Logger for Azure instance.

> **Note:** After the license is uploaded, 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 at the Micro Focus Community.

.

You can also reach the MF 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 Azure 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!