Fortanix®

Integration Guide

USING FORTANIX DSM WITH SUMO LOGIC (SIEM) INTEGRATION GUIDE FOR LINUX SERVER

VERSION 1.0

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION 2
2.0 TERMINOLOGY REFERENCES 2
3.0 DOWNLOAD AND INSTALL SUMO LOGIC COLLECTOR IN LINUX 2
3.1 System Requirements 2
3.2 Download the Collector 2
3.3 Generate Access Keys 3
3.4 Install the Connector 4
3.5 Configure Syslog Server 6
3.5.1 Configure Syslog Sever in Sumo Logic 6
3.5.2 Configure Syslog Sever in Fortanix DSM 7
3.6 View Audit Logs in Sumo Logic 8
4.0 DOCUMENT INFORMATION 10
4.1 Document Location 10
4.2 Document Updates 10
4.3 Revision History ..... Error! Bookmark not defined.

1.0 INTRODUCTION

This document describes how to integrate **Fortanix Data Security Manager (DSM)** with **Sumo Logic (SIEM)** on Linux Server.

2.0 TERMINOLOGY REFERENCES

- **DSM – Data Security Manager**

Data Security Manager is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

- **Sumo Logic**

Sumo Logic is a security information and event management (SIEM) solution that provides security analysts with enhanced visibility across the enterprise to thoroughly understand the impact and context of an attack. Sumo Logic offers streamlined workflows that automatically triage alerts to maximize security analyst efficiency and focus.

3.0 DOWNLOAD AND INSTALL SUMO LOGIC COLLECTOR IN LINUX

3.1 SYSTEM REQUIREMENTS

System requirements for Linux:

- Linux, major distributions 64-bit, or any generic Unix capable of running Java 1.8
- Single core, 512MB RAM
- 8GB disk space
- Package installers require TLS 1.2 or higher

3.2 DOWNLOAD THE COLLECTOR

Download the collector in one of the following ways:

- In Sumo Logic, select **Manage Data -> Collection -> Collection**. Click **Add Collector**, click **Installed Collector**, and then click the link for the collector to begin the download.
- Open a browser and enter the static URL for your pod. The collector begins to download. *See Download a Collector from a Static URL for a list of URLs for your deployment pod.*

Fortanix recommends using the collector manually by downloading the `.sh` installation file corresponding to your endpoint. For example, for downloading the collector for Linux 64 `bit`, use

the link:

https://collectors.in.sumologic.com/rest/download/linux/64

Run the following command:

```
ubuntu@sumologictest:~$ sudo wget
https://collectors.in.sumologic.com/rest/download/linux/64
--2022-05-11 05:22:09--
https://collectors.in.sumologic.com/rest/download/linux/64
Resolving collectors.in.sumologic.com
(collectors.in.sumologic.com)... 13.126.102.227, 65.2.26.137,
65.1.116.61, ...
Connecting to collectors.in.sumologic.com
(collectors.in.sumologic.com)|13.126.102.227|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 84905788 (81M) [application/octet-stream]
Saving to: '64.1'

64.1
100%[=============================================================
==========>]  80.97M  93.5MB/s    in 0.9s

      2022-05-11 05:22:11 (93.5 MB/s) - '64.1' saved
      [84905788/84905788]
```

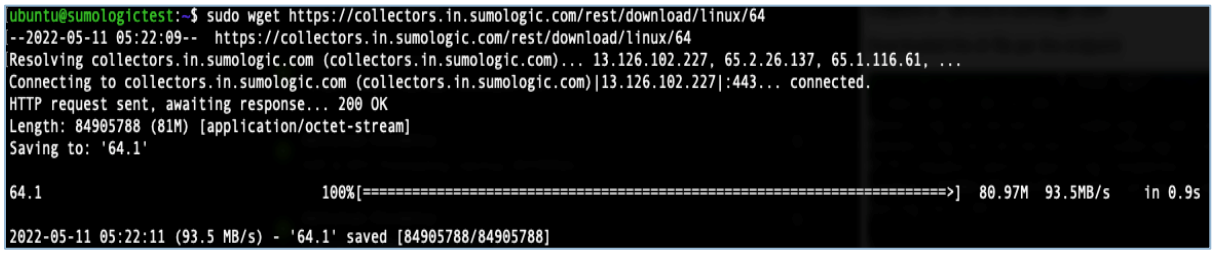

FIGURE 1: DOWNLOADING THE CONNECTOR ON LINUX 64 BIT SERVER

3.3 GENERATE ACCESS KEYS

To generate access keys:

1. On the user interface (UI) click **Profile → Preferences → Add Access Key**.

FIGURE 2: ADD ACCESS KEY

2. Enter a name for the key and click **Create Key**.

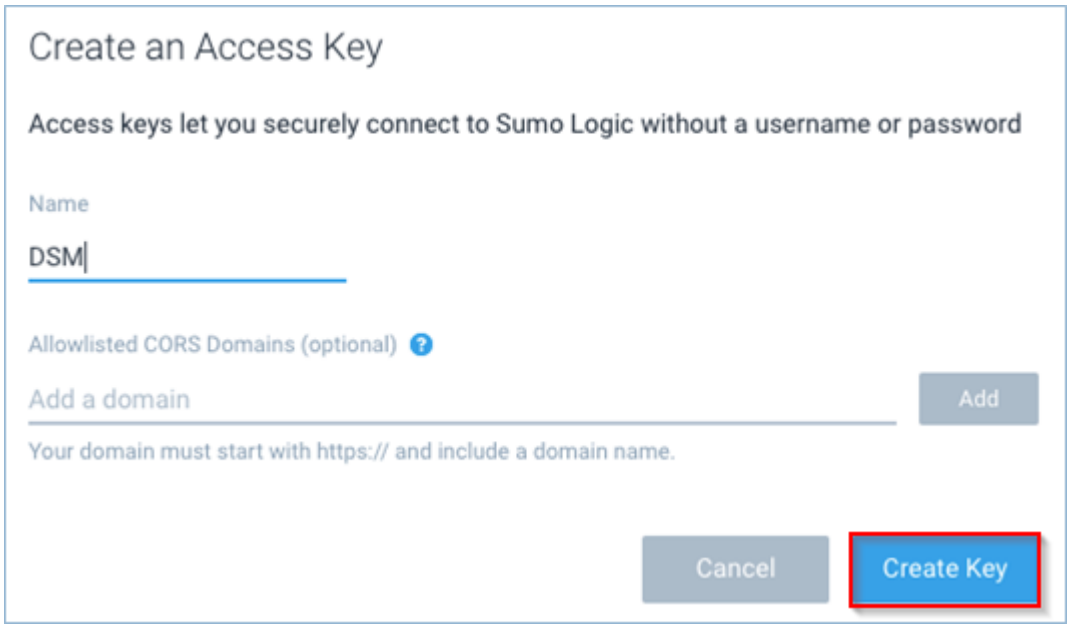

FIGURE 3: CREATE ACCESS KEY

For more details, refer to the article Access Keys.

3.4 INSTALL THE CONNECTOR

You can choose one of the following methods to install the Collector:

- *UI installer* (This method does not support all advanced settings)
- *Command-line installer*
- *RPM/Debian package*
- *Binary package*

The easiest and fastest way to install the connector is by using the command displayed below and replacing the values of `accesskey` and `accessid`.

```
ubuntu@sumologictest:~$ sudo ./SumoCollector.sh -q -
Vsumo.accessid=suVzuyDcEwXy6u -
Vsumo.accesskey=Kjpta1Obvs5SZMSYoyxYrAKNBTTtrgtPdSTLNXRyRZYS4zyzGcw
ZaBOauyQfmbih
Unpacking JRE ...
Starting Installer ...
2022-05-11 05:25:14,118 main WARN The bufferSize is set to 8192 but
bufferedIo is false: false
Uninstalling previous version
Extracting files...
Finishing installation...
```

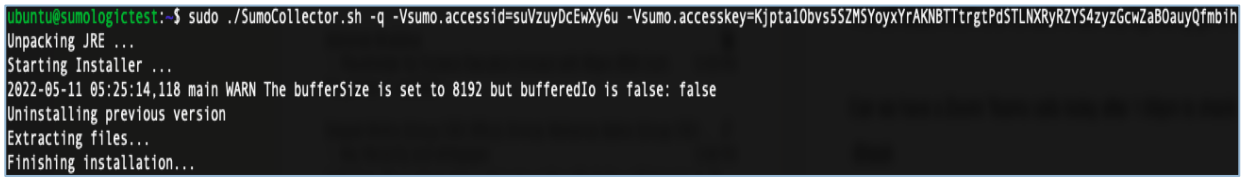

FIGURE 4: INSTALL THE CONNECTOR ON LINUX

To learn more about installing a collector on Linux, refer to the article Install a Collector on Linux.

Once the collector is installed, it appears under **Manage → Collection**.

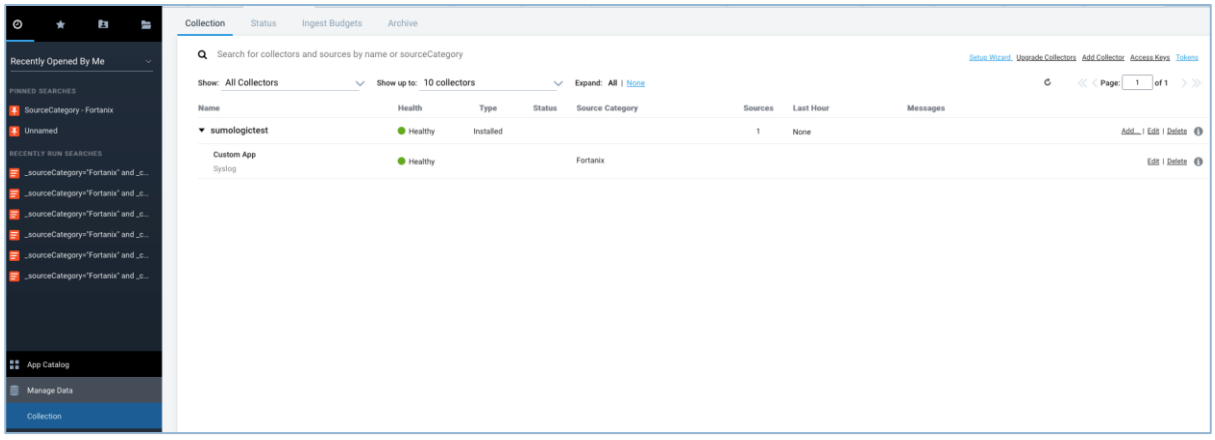

FIGURE 5: COLLECTOR APPEARS IN SUMO LOGIC

3.5 CONFIGURE SYSLOG SERVER

3.5.1 CONFIGURE SYSLOG SEVER IN SUMO LOGIC

1. Click **Manage Data → Collection**.
2. Click **Edit** next to **Syslog Server**.
3. Select **Protocol** as **TCP**, **Port** as **514**, leave the rest of the settings as default, and then click **Save**.

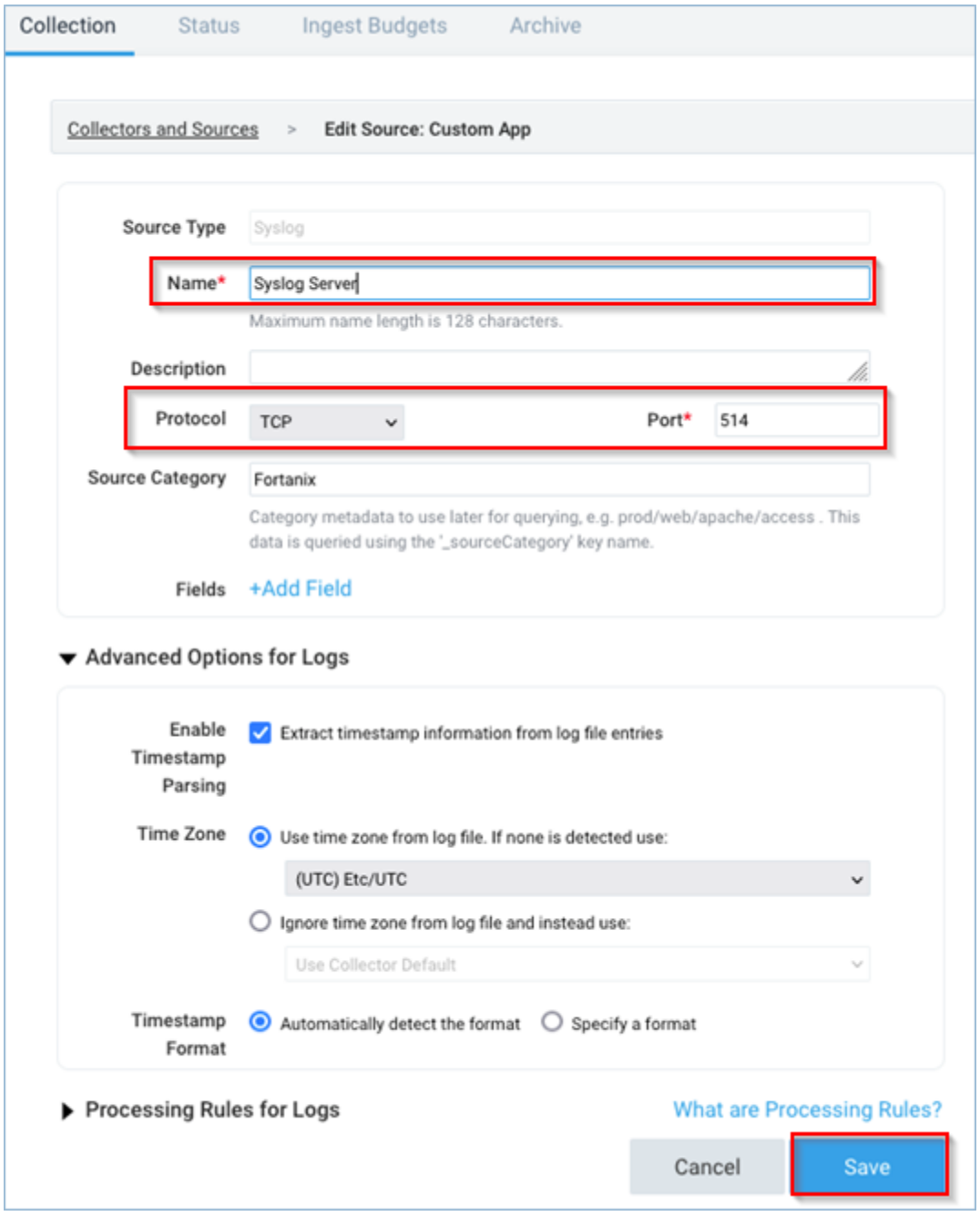

FIGURE 6: CONFIGURE THE SYSLOG SERVER ON SUMO LOGIC

3.5.2 CONFIGURE SYSLOG SEVER IN FORTANIX DSM

1. Log in to https://www.sdkms.fortanix.com
2. Click **Settings → Log Managements**.

3. Click **Syslog**.

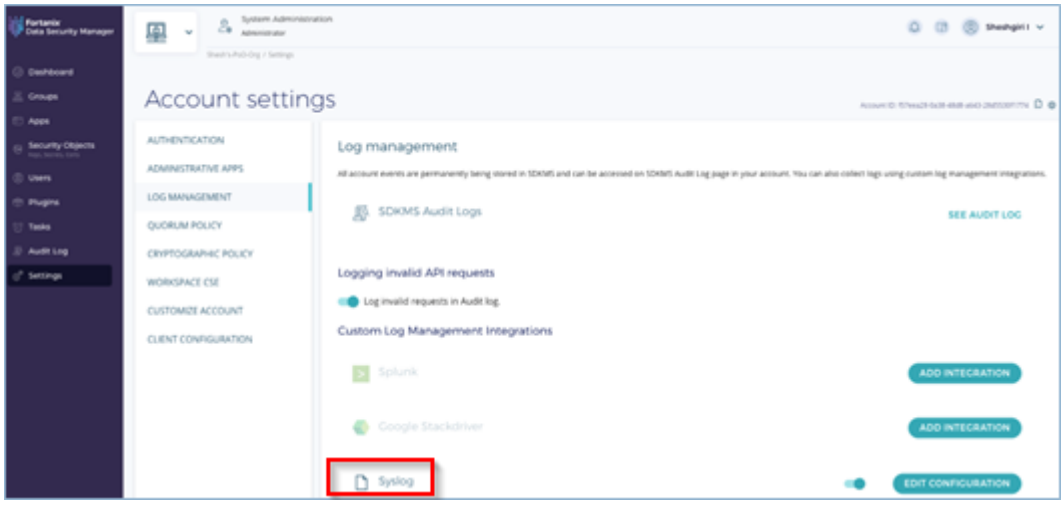

FIGURE 7: CONFIGURE THE SYSLOG SERVER IN FORTANIX DSM

4. Click **Edit Configuration** and update the **Host IP**. **Host IP** is the server where you have installed the Sumo Collector.

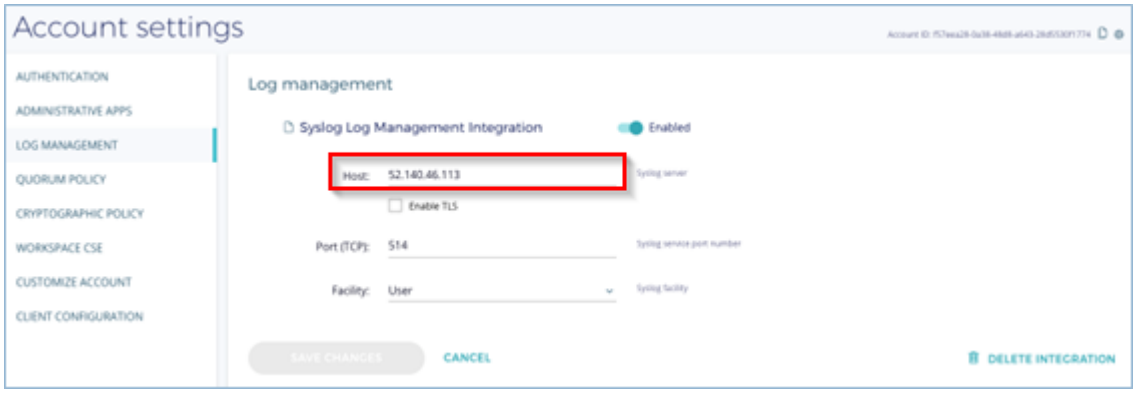

FIGURE 8: EDIT SYSLOG SERVER CONFIGURATION IN FORTANIX DSM

3.6 VIEW AUDIT LOGS IN SUMO LOGIC

Once all the above steps are completed, you can see all the audit logs in the Sumo Logic Screen.

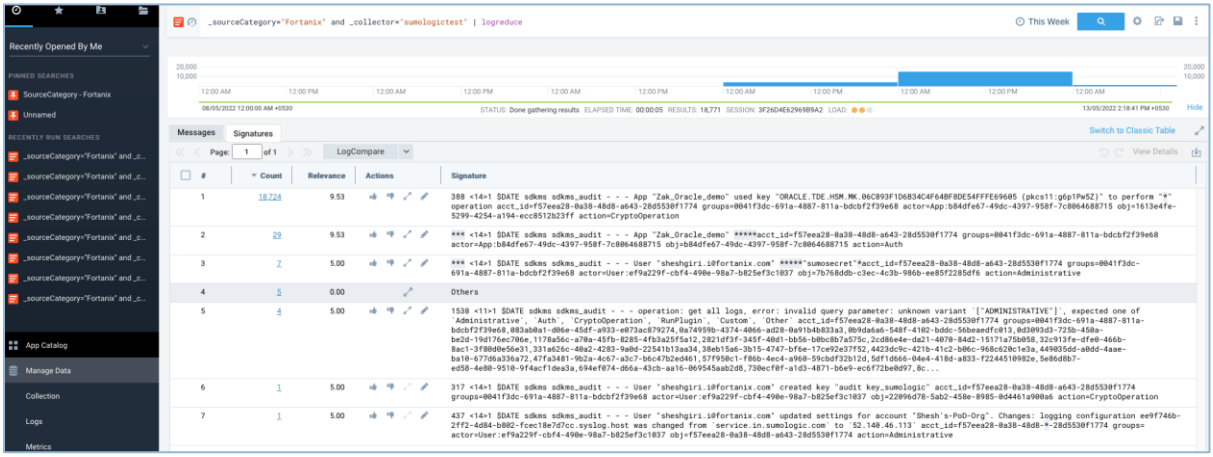

FIGURE 9: VIEW AUDIT LOGS IN SUMO LOGIC

You can further customize the data and chart by writing a query on the search bar. For example:

```
_sourceCategory="Fortanix" and _collector="sumologictest" |
logreduce
| timeslice 1h
| count by _timeslice
| order by _timeslice
```

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/6390501090452-Using-Fortanix-DSM-with-Sumo-Logic-SIEM-Integration-Guide-for-Linux-Server

4.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com