Fortanix[®]

Integration Guide

USING DATA SECURITY MANAGER WITH LOGRHYTHM

VERSION 1.0

DATA SECURITY MANAGER INTEGRATION WITH LOGRHYTHM

TABLE OF CONTENTS

1.0		2
2.0	CONFIGURING SYSLOG SERVER	2
3.0	INSTALL OPEN COLLECTOR	2
4.0	VALIDATE THE INSTALLATION	3
5.0	DOCUMENT INFORMATION	5
5.1	Document Location	5
5.2	Document Updates	5
5.3	Revision HistoryError! Bookmark not	defined.

Fortanix[®]

1.0 INTRODUCTION

This article describes how to integrate and use LogRhythm as a Syslog server **Fortanix Data Security Manager** (DSM).

2.0 CONFIGURING SYSLOG SERVER

1. Go to the Fortanix DSM **Account settings** page and click the **LOG MANAGEMENT** tab to configure the Syslog Server details. Enter the IP and port number of the Syslog server.

Fortanix	Acme Company			System Adr Administrator	ministration	Ĵ		🛞 User Fortanix 🗸
" III" Data Security Manager	Acme Company / Settings							
② Dashboard	Account settings							
곲 Groups	Account settings						1cd498-c685-4	4e9-b242-ff53c5ffe1ee 📙 🕲
🗁 Apps	AUTHENTICATION	Log manageme	nt					
Security Objects Keys, Secrets, Certs	ADMINISTRATIVE APPS							
® Users	LOG MANAGEMENT	Management Integratio	on					
Plugins	QUORUM POLICY	Host:	40.80.90.204		Syslog server			
한 Tasks	CRYPTOGRAPHIC POLICY		Enable TLS					
🖺 Audit Log	WORKSPACE CSE	Port (TCP):	514		Syslog service p	oort number		
ැ [®] Settings	WORKDIFACE CSE							
	CUSTOMIZE ACCOUNT	Facility:	User	~	Syslog facility			
	CLIENT CONFIGURATION							
	ADD INTEGRATION CANCEL							
		·						

FIGURE 1: CONFIGURE SYSLOG SERVER

3.0 INSTALL OPEN COLLECTOR

To install the Open Collector on the Linux host:

1. First, install Wget.

```
sudo yum install -y wget
```

2. Download the Open Collector Control Script using the following command.

wget https://raw.githubusercontent.com/logrhythm/versions/master/lrctl



DATA SECURITY MANAGER INTEGRATION WITH LOGRHYTHM

3. Change the permissions.

chmod +x lrctl

4. Initialize the Open Collector and start all the components.

```
sudo yum erase podman buildah
```

5. Install the Docker-Community Edition (CE) using the following command.

```
./lrctl init
```

If there is no Docker CE, install it from the following website:

https://docs.docker.com/engine/install/rhel/

6. Start the Metrics service.

./lrctl metrics start

7. Finally, start the Open Collector.

./lrctl open-collector start

4.0 VALIDATE THE INSTALLATION

1. Validate that the services are running using the following three commands:

```
./lrctl open-collector status
./lrctl metrics status
./lrctl <beat name> status
```

2. View the metrics in Grafana.

http://<opencollectorip>:3000

3. In Grafana, go to Open Collector, and then Open Collector Overview.



DATA SECURITY MANAGER INTEGRATION WITH LOGRHYTHM

- a. The default Open Collector Overview dashboard has three columns. Each column includes a "Messages Per Second" and a "Counters (total)" graph. The "Pipelines" and "Output" columns also have "Errors" graphs.
- b. Left column: Input a Beat is successfully sending logs to the Open Collector.
- c. Middle column: **Pipelines** the logs are matching our Microsoft Defender for Identity (MDI).
- d. Right column: **Output** the logs are successfully sent to the System Monitor Agent.

If data is flowing through the Open Collector, the graphs will be populated with data regarding total counts and the Mathematical Programming System (MPS) for various parts of the pipeline. Each graph has an information icon in the top-left corner. Point to this icon for a description of what each graph displays.





FIGURE 2: OPEN COLLECTOR OVERVIEW

Fortanix[®]

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/7570195214740-Using-Fortanix-Data-Security-Manager-with-LogRhythm

5.2 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

© 2016 – 2022 Fortanix, Inc. All Rights Reserved.

Fortanix® and DSM Applications are trademarks of Fortanix, Inc. All other trademarks are trademarked by their respective owners.

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform <u>info@fortanix.com</u> immediately.