Integration Guide

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

VERSION 1.0





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	7
4.0	DOCUMENT INFORMATION	9
4.1	Document Location	9
4.2	Document Updates	9

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* <u>Download a Collector from a Static URL</u> 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
======>] 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:



USING FORTANIX DSM WITH SUMO LOGIC (SIEM) INTEGRATION GUIDE

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

_						
м	y Profile					
	Organization ID:	0000000000DDEF				
	Password:	Change Password				
	Roles:	Administrator				
м	y Security Settin	ngs				
	2-Step Verificatio	in is currently disabled.				
	Enable 2-Ste	p Verification				
м	v Access Kevs					
	,,.					I Add Assess Key
						+ Add Access Key
	LABEL		ACCESS ID	CREATED	STATUS	
	DSM		suVzuyDcEwXy6u	10/05/2022	Active	
	v Preferences					

FIGURE 2: ADD ACCESS KEY

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

Create an Access Key	
Access keys let you securely connect to Sumo Logic without a username of	or password
Name	
DSM	
Allowlisted CORS Domains (optional) 🕜	
Add a domain	Add
Your domain must start with https:// and include a domain name.	
Cancel	Create Key

FIGURE 3: CREATE ACCESS KEY

For more details, refer to the article <u>Access Keys</u>.

3.4 INSTALL THE CONNECTOR

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

- <u>Ul installer</u> (This method does not support all advanced settings)
- <u>Command-line installer</u>
- <u>RPM/Debian package</u>
- 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.

Fortanix

USING FORTANIX DSM WITH SUMO LOGIC (SIEM) INTEGRATION GUIDE

```
ubuntu@sumologictest:~$ sudo ./SumoCollector.sh -q -
Vsumo.accessid=suVzuyDcEwXy6u -
Vsumo.accesskey=KjptalObvs5SZMSYoyxYrAKNBTTtrgtPdSTLNXRyRZYS4zyzGcw
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...
```





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** \rightarrow **Collection**.

0 * 🖻 🖢	Collection Status Ingest Budgets	Archive				
Recently Opened By Me v	Q Search for collectors and sources by name	ne or sourceCategory				Seturo Wizard, Upprade Collectors Add Collector Access Keys Tokens
PINNED SEARCHES	Show: All Collectors 🗸 S	ihow up to: 10 collectors	V Expand: All None			C ≪ < Page: 1 of 1 > ≫
U SourceCategory - Fortanix	Name	Health Type	Status Source Category	Sources Last Hour	Messages	
Innamed	▼ sumologictest	Healthy Installed		1 None		Add Edit Delete 🕕
RECENTLY RUN SEARCHES	Custom App	Healthy	Fortanix			Edit Delete
_sourceCategory="Fortanix" and _c	Systog					
_sourceCategory="Fortanix" and _c						
_sourceCategory="Fortanix" and _c						
_sourceCategory="Fortanix" and _c						
_sourceCategory="Fortanix" and _c						
_sourceCategory="Fortanit" and _c						
App Catalog						
Manage Data						
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**.

Collection Statu	s Ingest Budgets Archi	ive							
Collectors and Sour	es > Edit Source: Custom App								
Source Type	Syslog								
Name*	Syslog Server								
	Maximum name length is 128 characters								
Description									
Protocol	TCP V	Port* 514							
Source Category	Fortanix								
	Category metadata to use later for query data is queried using the '_sourceCatego	Category metadata to use later for querying, e.g. prod/web/apache/access . This data is queried using the '_sourceCategory' key name.							
Fields	+Add Field								
 Advanced Onti 	ons for Logs								
+ Autoneeu opti	0101012090								
Enable Timestamp	 Extract timestamp information from log file entries 								
Parsing									
Time Zone	Use time zone from log file. If none is detected use:								
	(UTC) Etc/UTC ~								
	Ignore time zone from log file and ins	stead use:							
	Use Collector Default	· · · · · · · · · · · · · · · · · · ·							
Timestamp Format	 Automatically detect the format) Specify a format							
Processing Ru	les for Logs	What are Processing Rules?							
		Cancel Save							

FIGURE 6: CONFIGURE THE SYSLOG SERVER ON SUMO LOGIC

USING FORTANIX DSM WITH SUMO LOGIC (SIEM) INTEGRATION GUIDE

- 3.5.2 CONFIGURE SYSLOG SEVER IN FORTANIX DSM
- 1. Log in to "https:// <fortanix_dsm_url>"
- 2. Click Settings → Log Managements.
- 3. Click Syslog.

Cota Decurity Manager	a System Administratio	n 🔘 🛞 Standard V
Deshtoore Deshtoore Deshtoore Deshtoore Deshtoore Deshtoore Appen Deshtoore D		S Assure to thread have an account to D account of thread have an account of D account of thread have an account of D account of thread have account on the account events are permanently term, strength and can be account on SCHAIS Audit toggage in your account, this can all called have account on the account of the acco
a Authing C a Authing C a Settings C C	RYPTOGRAPHIC POLICY WORKSPACE CSE SUSTOMIZE ACCOUNT CLIENT CONFIGURATION	Logging invalid API requests Custom Log Management Integrations Splunk Coople Stackdriver

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.

	B DELETE INTEGRATION	
CLIENT CONFIGURATION		
CUSTOMIZE ACCOUNT	Facility: User v	Syring Sacity
WORKSPACE CSE	Port (TCP): 514	Systing service port number
CRYPTOGRAPHIC POLICY	C Enable TLS	
QUORUM POLICY	Host: 52.140.46.113	Syring server
LOG MANAGEMENT	 Systog cog management integration 	Chaute
ADMINISTRATIVE APPS	C Suring Log Management Integration	Caublad
AUTHENTICATION	Log management	
Account setting	JS	Account ID: 153/ees28-bu38-4868-a4403-2865/3001774

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.

USING FORTANIX DSM WITH SUMO LOGIC (SIEM) INTEGRATION GUIDE

○ ★ Þ ≌	🗐 🕗 _sou	rceCategory="Forta	mix' and _c	collecto	r="sum	ologic	test" logreduce 📀 This 1	Veek Q	0	0	
Recently Opened By Me 🛛 🗸											
PINNED SEARCHES	20,000 10,000										20,000 10,000
🛃 SourceCategory - Fortanix	12:00 AM	M 12:00	PM	12.0	0 AM		12:00 PM 12:00 AM 12:00 PM 12:00 PM 12:00 PM 12:00 PM	12.00 AM			
🔝 Unnamed	08/05/20	322 12:00:00 AM +0530					STATUS: Done gathering results: ELAPSED TIME 00.00.05 RESULTS: 18,771 SESSION: 3F260466296989A2 LOAD: 0 0	13/05/2022	2:18:41 PM +	0530	Hide
RECENTLY RUN SEARCHES	Messages	Signatures						Switch t	o Classic	Table	12
_sourceCategory="Fortanix" and _c	<< < Page	E 1 of 1 > >	LogC	ompare	~				View	Details	¢
_sourceCategory="Fortanix" and _c		* Count	Relevance	Action	5		Signature				
🧮 _sourceCategory*"Fortanix" and _c	1	18.724	9.53	14.1	9.2	1	388 <14>1 \$DATE sdkms_sdkms_audit App "Zak_Oracle_demo" used key "ORACLE.TDE.HSM.MK.06C893F1D6B34C4F64BF8DE54FFFE69605 (pkcs1	1:g6p1Pw5Z)" to	perform	-*-	
and _c							operation acct_1d=f57eea28-0a38-4808-a643-28d5330f1774 groups=0041f3dc-691a-4887-811a-bdcbf2f39e68 actor=App:b84dfe67-49dc-4397-958 5299-4254-a194-ecc8512b23ff action=CryptoOperation	f-7c8064688715 (obj=1613	e4fe-	
_sourceCategory="Fortanix" and _c	2	<u>29</u>	9.53	14.1	• Z	1	*** <14>1 \$DATE sdkms sdkms_audit App "Zak_Oracle_demo" *****acct_id=f57eea28-8a38-48d8-a643-28d5530f1774 groups=8841f3dc-691 actor=App:b84dfe67-49dc-4397-958f-7c8864688715 obj=b84dfe67-49dc-4397-958f-7c8864688715 action=Auth	a-4887-811a-bdcl	of2f39e6	8	
_sourceCategory="Fortanix" and _c	3	Z	5.00	- 14	ŧ 2	1	*** <14>1 \$DATE sdkms sdkms_audit User 'sheshgiri.i0fortanix.com' ****** sumosecret'*acct_id=f57ees28-0838-48d8-a643-28d5530f1	774 groups=00411	f3dc-		
_sourceCategory="Fortanix" and _c											
_sourceCategory="Fortanix" and _c	4	2	0.00		1		others				
	5	4	5.00		• 2	/	1538 <11>1 \$DATE sdkms sdkms_audit operation: get all logs, error: invalid query parameter: unknown variant '["ADMINISTRATIVE 'Administrative', 'Auth', 'CryptoOperation', 'RumPlugin', 'Custom', 'Other' acct_id=f5/reea28-8a38-46d8-a543-28d5580fb747 group=804 Getbpf219686_032abd1-d666-45d7-a932-a732abc7272.0a270959-4372-4666-ad58-a951405132a.0e0dada6-f546-1102-ddc-5405-a963-451-012-ddc-1102-	"]`, expected on 1f3dc-691a-4887- 1-725b-450a-	ne of -811a-		
App Catalog							be2d-19d176ec786e,1178a56c-a78a-45fb-8285-4fb3a25f5a12,2821df3f-345f-40d1-bb56-b8bc8b7a575c,2cd86e4e-da21-4678-84d2-15171a75b858,32 8ac1-3f88d0e56e31,333a526c-48a2-4283-9a8d-22541b13as34,38eb15a6-3b15-4747-bf6e-17ce92e37f52,4423dc9c-421b-41c2-b86c-968c628c1e3a,44	c913fe-dfe8-466 9035dd-a0dd-4aa	b- 8-		
🍧 Manage Data							ba10-077dba336a72,47fa3481-9b2a-4c67-a3c7-bbc47b2e4461,57f95bc1-786b-4ec4-a968-59cbdf32b12d,5df1d666-94e4-418d-a833-f2244510982e,5e ed58-4e88-9510-9f4acf1dea3a,694ef074-d66a-43cb-aa16-069545aab2d8,730ecf0f-a1d3-4871-b6e9-ec6f72be0d97,8c	86d8b7-			
Collection	6	1	5.00		• ~	1	317 <14+1 \$DATE sdkms_sdkms_audit User "sheshgiri.i0fortanix.com" created key "audit key_sumologic" acct_id=f57eea28-0a38-484 groups=0041f3dc-691a-4887-811a-bdcbf2f39e68 actor=User:ef9a229f-cbf4-490e-98a7-b825ef3c1037 cbj=22096d78-5ab2-458e-89085-0d4461a900a	8-a643-28d5530f 5 action=Cryptol	1774 Operation	n	
Logs Metrics	7	1	5.00	-	• /	1	407 1481 BATE datas dakas audit Usar "ahahajri.idformaix.com" updated settings for account "Benkh s-PoD-Org." Changes 1a 2767-4841-886-cellafd/cz.oyalab bet mas changed form" services nu analogic.com to "2, 13.484, 4113" accidifyEnez28-ba38-48461- actor/User ef%s2297-cbf4-980-9837-b825ef3c1807 obj=f37ees28-ba38-4868-8461-8450-28653801774 action=Administrative	gging configurat -28d5530f1774 g	tion ee9 roups=	f746b-	

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:



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

© 2016 – 2023 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc. All other trademarks are the property of their respective owners.