Fortanix[®]

User Guide

CONFIDENTIAL COMPUTING MANAGER – INTEGRATION WITH EXTERNAL LOGGING SYSTEMS

VERSION 2.0



TABLE OF CONTENTS

1.0		2
2.0	AUDIT LOGGING IN CONFIDENTIAL COMPUTING MANAGER	3
2.1	Log Management	3
2.2	Sending Audit Logs to Splunk	4
2.3	Sending Audit Logs to Azure Log Analytics	7
2.3.1	1 References	10
2.4	Sending Audit Logs to Syslog	10
3.0	APPENDIX	12
4.0	DOCUMENT INFORMATION	14
4.1	Document Location	14
4.2	Document Updates	14



1.0 INTRODUCTION

This article describes how to integrate Fortanix Confidential Computing Manager (CCM) with

External logging systems.

Fortanix CCM automatically maintains an internal audit log of system operations from different applications and services, and actions related to accounts, users and sessions. The following events are logged:

- App Created
- App Updated
- App Updation Failed
- App Deleted
- App Certificate Downloaded
- App Creation Failed
- Node Enrolled
- Node Attested
- Node Attestation Failed
- Node Enrollment Failed
- Node Deactivated
- Node Certificate Downloaded
- Approve Domain
- Decline Domain
- Approve Image
- Decline Image
- Create Image
- Delete Image
- Image Conversion Succeeded
- Image Conversion Failed
- Certificate Requested by Application
- Create Registry
- Delete Registry
- Update Registry
- Node Reconnected



- Node Disconnected
- Configuration Creation

You can configure Fortanix CCM to send these audit log entries to an external logging system. In this article you will learn how to send Fortanix CCM audit logs to the following external logging systems:

- Splunk
- Azure Log Analytics
- Syslog Server

2.0 AUDIT LOGGING IN CONFIDENTIAL COMPUTING MANAGER

NOTE: Only an Account Administrator can set up integration with external logging systems.

2.1 LOG MANAGEMENT

Currently, Fortanix CCM supports the following logging systems:

- Splunk
- Azure Log Analytics
- Syslog

NOTE: Only an **Account Administrator** in Fortanix CCM can set up integration with external logging systems like **Splunk**, **Azure Log Analytics**, and **Syslog**.

To integrate with the above logging systems, click the **Settings** menu item in the CCM UI left navigation bar, and then click the **Log Management** menu item. It will give you three options for integration: Splunk, Azure Log Analytics, and Syslog. It is possible to have more than one



integration active at the same time. Logs will be pushed from Fortanix CCM to all logging facilities that are configured.

111	CONFIDENTIAL	Permo v	🗘 🛞 Fortanix User 🗸
ч.	MANAGER	product / Entripy / Lag management	
Ø	© [®] Settings	Settings	
U	Authentication	Account ID: 5c1ebd86-9e00-45c3-9e77-2341914107a5 🗋	
88	Log Management	Log Management	
Æ		All account events are permanently being stored in CCM. You can collect logs using custom log management integrations.	
 0 8		CCM Audit Logs	
8		Custom Log Management Integrations	
₽ 		> Splunk	
0		Azure Log Analytics	
		Syslog Add Integration	

FIGURE 1: LOG MANAGEMENT

2.2 SENDING AUDIT LOGS TO SPLUNK

You can configure Fortanix CCM to send audit log entries to a Splunk server using the <u>HTTP Event</u> <u>Collector</u> (HEC).

To configure logging events to Splunk,

- 1. Click the **Settings** \rightarrow **Log Management** menu item from the CCM UI left navigation bar.
- In the Custom Log Management Integrations section, click the ADD INREGRATION button for Splunk.

	CONFIDENTIAL	Demo v	Q @	D
. I I.	MANAGER	produce / Settings / Log mesuperies		
Ø		Settings		
en	Authentication	Account ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5	D	
88 24	Log Management	Log Management All account events are permanently being stored in CCM. You can collect logs using custom log management integrations.		
		CCM Audit Logs		
•		Custom Log Management Integrations		
@ 		> Splunk		
		Azure Log Analytics		
		Syslog		

FIGURE 2: ADD SPLUNK INTEGRATION

Fortanix

- 3. Configuring a Splunk integration requires the following information:
 - a. Enter the IP Address or the hostname of your Splunk server.
 - Select Enable HTTPS to communicate with the Splunk server over HTTPS (recommended) and also select the Enable SSL checkbox in the Splunk Global Settings. *Refer to the Appendix for the screenshot.*

NOTE: If you are using an HTTP connection, then clear the **Enable HTTPS** checkbox in the Fortanix CCM **Log Management** screen for Splunk and also clear the **Enable SSL** checkbox in the Splunk Global Settings. *Refer to the Appendix for the screenshot.*

Depending on the type of TLS certificate the Splunk server is using:

- ii. Select **Global Root CAs** if you are using a certificate that is signed by a wellknown public CA.
- Select Custom CA Certificate, if you as an enterprise want to self-sign the certificate using your own internal CA. To do this, upload the CA certificate using the UPLOAD A FILE button. When Fortanix CCM as a client connects to the Splunk server and is presented the server's certificate, it will be able to validate it using the enrolled custom CA Certificate. To generate the CA certificate, run the following command:

openssl s_client -connect <endoint/ipaddress>:port -showcerts

Where,

- ipaddress: This is the IP address of the Splunk server.
- port: This is the value of the Management port, under Server settings >General settings in the Splunk Server. *Refer to the Appendix for the* screenshot.
- iv. In case the Custom CA Certificate has a Common Name (CN) that does not match with the server in which Splunk is deployed, clear the Validate Hostname checkbox which prompts Fortanix CCM to ignore the hostname of the Splunk deployment instance. Only the certificate chain will be validated in this case.



- b. The default **Port** number is **80**. If you are running on a different port, add the applicable port number. If you enable HTTPS in *"Step a"* above, then the default port number is **443**.
- c. Add the name of the Splunk index in the Index field to submit events. The index value should be the same as the index in Splunk. *Refer to the Appendix for the screenshot*. When you push the logs to Splunk, you need to push it to a specific index. This value is sent to the Splunk server and can be set to whatever you like. This will allow distinguishing logs from different sources. For example, the logs from Fortanix CCM can be pushed to the Index source name fortanix cloud.
- d. Enter a valid **Authentication token** to authenticate to the HTTP Event Collector of your Splunk instance. The Authentication token will authenticate Fortanix CCM as a client to Splunk and allows it to push the events to Splunk. See the Splunk documentation for detail about generating HEC authentication tokens.

NOTE: For security reasons, the authentication token is not displayed in the interface when editing an existing configuration.

CONFIDENTIAL	Demo v			🛕 🛞 Fortanix User 🗸
MANAGER	praham / Settings / Log management			
	Settings			
ු [®] Settings	0		a contraction of the second	
Authentication			Account IU: 5c1ebd8b-9e00-45c0-9tc/-234191d10/a5	
Log Management	Log Management			
	> Splunk Log Management Integration	1	Enabled	
	Host			
	20.51.107.95	Splunk server		
	Enable HTTPS			
	Port			
	8088	Splunk service part number		
	Index			
	319_v1	Splunk index		
	Authentication token			
	Authensication token is hidden for security reasons. You can edit it by adding a new one.			
	SAVE CHANGES CANCEL	ŢĨ	DELETE INTEGRATION	

FIGURE 3: SPLUNK LOG MANAGEMENT INTEGRATION FORM

4. Click **SAVE CHANGES** to save the Splunk integration.

2.3 SENDING AUDIT LOGS TO AZURE LOG ANALYTICS

You can configure Fortanix CCM to send audit log entries to Azure Log Analytics in the Azure Portal to write log queries and interactively analyse the Fortanix CCM log data.

To configure logging events to the Azure Log Analytics, in the **Custom Log Management Integrations** section, click the **ADD INTEGRATION** button for Azure Log Analytics.

aigi	CONFIDENTIAL	Emo v	🛕 🔞 Fortanix User 🗸
"iP	MANAGER	prathant / Settings / Lag management	
Ø	💣 Settings	Settings	
m	Authentication	Account ID: 5c1ebd8b-9e0045c09fc7-234191d107a5 []	
5 88 8	Log Management	Log Management All account events are permanently being stored in COM. You can collect logs using custom log management integrations.	
 ® }		CCM Audit Logs	
		Custom Log Management Integrations	
\$ 		> Splunk ADD INTEGRATION	
•		Azure Log Analytics	
		Syslog ADD INTEGRATION	

FIGURE 4: ADD INTEGRATION FOR AZURE LOG ANALYTICS

- 1. Configuring an Azure Log Analytics integration requires the following information:
 - Enter the Workspace ID which is the Log Analytics workspace in the Azure portal. It is

 a GUID to identify the specific log analytics workspace in the Azure cloud. To create a
 log-analytics workspace refer to <u>https://docs.microsoft.com/en-us/azure/azure monitor/logs/quick-create-workspace</u>. To get the Workspace ID after you create a log analytics workspace:
 - i. In the log analytics workspace, click the **Agents management** tab to see the **Workspace ID**.

Fortanix[®]

CCM WITH EXTERNAL LOGGING SYSTEMS

\equiv Microsoft Azure		℅ Search resources, services, and docs (G+/)			
Home > logAnalyticsWSDev	Home > logAnalyticsWSDev				
IogAnalyticsWSDev Log Analytics workspace	IogAnalyticsWSDev Agents management Log Analytics workspace				
Search (Ctrl+/) «	Windows servers & Linux servers	ers			
Access control (IAM)	O Windows computers of Go to logs	connected			
🔷 Tags					
Diagnose and solve problems	Download agent				
Settings	Download an agent for your operating sys You'll need the Workspace ID and Key to	stem, then install and configure it using the keys for yo install the agent.	ur workspace ID.		
A Locks	Download Windows Agent (64 bit)				
	Download Windows Agent (32 bit)				
Agents configuration	Workspace ID	17e2efbc-3e99-4645-a7f1-653ad1107674	D		
Eustom logs	Primary key	all difficults and County of Charlest 1977 Day 1788 (1997)	Lines 1910 Barland Thilling Installed Witz	Regenerate	
Computer Groups	i initially key	sources a construction of the second second second	an and the second second	negenerate	
Linked storage accounts	Secondary key	Ziv5yTcliDpEpUWwMygSM00hHosgmd8bIEyIcrW	pOTROSSREWOVSRSMertinVide.	Regenerate	
Network Isolation	Log Analytics Gateway				
General	If you have machines with no internet con	nectivity to Log Analytics workspace, download the Lo	g Analytics Gateway to act as a proxy.		
Workspace summary	Learn more about Log Analytics Gateway Download Log Analytics Gateway				
Workbooks	, ,				
🧬 Logs					
P Solutions					

FIGURE 5: WORKSPACE ID

b. The Custom Log Type is set to "fortanix_audit_v1_CL" for all event logs published to Azure Log collector from Fortanix services. This field is set in HTTP POST request header of all the logs published to the Azure log collector and therefore it is used to query logs from Fortanix services in Azure Log Analytics Workspace. For more details refer to <u>https://docs.microsoft.com/en-us/azure/azure-monitor/logs/queries</u>.

	₽ Search	esources, services, and docs (G+/)	区 66 年 10 ? 反
Home > Log Analytics workspaces > logAr	nalyticsWSDev v∣Logs & …		
P Search (Ctrl+/) «	🧬 New Query 1* 🛛 × 🕂		♡ Feedback 😂 Queries 🕞 Query explorer 🛛 🎯
Overview	P logAnalyticsWSDev Select scope	▶ Run Time range : Last 24 hours 🛛 🗟 Save ∨ 😰 Share ∨ 🕂 New	alert rule \mapsto Export 🗸 🔗 Pin to dashboard 🛛 🚟 Format query
Activity log	Tables Queries Functions ··· «	<pre>1 fortanix_audit_v1_CL where service_s contains "ccm"</pre>	
Access control (IAM)			
Tags	P Search		
Diagnose and solve problems	Filter (Group by: Category	Results Chart Columns V C Display time (UTC+00:00) V) Group columns
Settings	T Collapse all	Completed. Showing results from the last 24 hours.	(© 00:01.2 🔳 2 records
🔒 Locks	Favorites	TimeGenerated [UTC] V Computer V RawData V Message	∑ log_id_g 🖓
🥔 Agents management	You can add favorites by clicking on the 🕱 icon	✓ 8/11/2021, 11:21:26.000 AM User "jiig	ny spally@fortanix.com" created app "TestApp" 71e4c638-f7df-4030-9ac5-15b8cfc5aa2d
Agents configuration	- Applications		
Custom logs	Error and exception count	Tenantid 17e2efbc-3e99-4645-a7f1-653ad1107674	
Computer Groups	E Exceptions causion request	SourceSystem RestAPI	
Linked storage accounts	failures	TimeGenerated [UTC] 2021-08-11T11:21:26Z	
Network Isolation	III Failed operations	··· Message User "Jun a highling@fortanix.com" created app "TestA	pp"
General	E Failed requests – top 10	log_id_g 71e4c638-f7df-4030-9ac5-15b8cfc5aa2d	
 Workspace summary 	Failing dependencies	service_s ccm	
Workbooks	E Function activity over time	acct_id_g 6576dbef-c357-4cd6-8130-a533e7adc2c5	
e Logs	Function Error rate	action_type_s ADMINISTRATIVE	
Solutions	III Function results	client_ip_s 10.201.77.15	
Ilsane and estimated costs	10	object_groups_s	
Orage and estimated costs	Uperations performance	operation_s CREATE_APP	
III Propercies	Page views trend	operation result s SUCCESS	

FIGURE 6: CCM EVENT LOG QUERY

c. Click **ADD PRIMARY SHARED KEY** to add a shared key. Any request to the Azure Monitor HTTP Data Collector API must include an authorization header. Each event log



posted to azure log analytics workspace from the logging service is authenticated by the log monitor service in azure by validating the request and checking whether it is signed with either the primary or the secondary key for the workspace that is making the request. To get the Primary Shared Key:

 In the log analytics workspace, click the Agents management menu item to see the Primary key. The Primary key of the log-analytics workspace is referred as shared_key.

	P Search resources, services, and docs (G+r)
Home > logAnalyticsWSDev logAnalyticsWSDev LogAnalytics workspace > Search (Ctrl+/) « Activity log % Access control (IAM)	v Agents management … [■] Windows servers ▲ Linux servers ● 0 Windows computers connected Go to los
Tags Diagnose and solve problems Settings Locks Setting Agents management	Download an gent To your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent. Download Windows Agent (64 bit) Download Windows Agent (32 bit)
Agents configuration Custom logs Computer Groups Linked storage accounts Advance Isolation	Workspace ID 17e2efbc-3e99-4645-a7f1-653ad1107674 Primary key Indeficit flaxees/2gmlax4017pb/s1F122Fe1288p1FPCFLde=715Milepv1TipLintSee64/3Ffa. No Regenerate Secondary key ZIV/5g12600p1pu1MeMyg5MX884/orgmd812Epv05Vp01R0215BiseCoVR5Meemv1Aaka. No Regenerate
General Workspace summary Workbooks P Logs P Solutions	Log Analytics Gateway If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway to act as a proxy. Learn more about Log Analytics Gateway Download Log Analytics Gateway

FIGURE 7: PRIMARY SHARED KEY

CONFIDENTIAL	Demo v	💭 🛞 Fortanix User 🗸
MANAGER	prather / Settings / Log management	
	Settings	
	Settings	
Authentication	Account ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5 [])	
Log Management		
	Log Management	
	P Azure Log Management Integration	
	Workspace ID	
	Sc1ebd8b-9e00-45c0-9fc7-234191d107a5	
	Primary Shared Key	
	SAVE CHANCES CANCEL	

FIGURE 8: CONFIGURE AZURE LOG ANALYTICS

ADD PRIMARY SHARED KEY		×
Enter primary shared key		
CANCEL	SAVE	

FIGURE 9: ADD PRIMARY SHARED KEY

NOTE: For security reasons, the Primary Shared Key is not displayed in the interface when editing an existing shared key.

2. Click **SAVE CHANGES** to save the Azure Log Analytics integration.

2.3.1 REFERENCES

- Create log-analytics workspace: <u>https://docs.microsoft.com/en-us/azure/azure-</u> monitor/logs/quick-create-workspace. In the URL refer to the section: **Create a workspace**.
- Create log-analytics workspace using CLI <u>https://docs.microsoft.com/en-</u> us/azure/azure-monitor/logs/quick-create-workspace-cli. In the URL refer to the sections: Prerequisites and Create a workspace.
- Monitoring logs: <u>https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview</u>.
- Querying logs: <u>https://docs.microsoft.com/en-us/azure/azure-monitor/logs/queries</u>.

2.4 SENDING AUDIT LOGS TO SYSLOG

You can configure Fortanix CCM to send audit log entries to the Syslog server.

To configure logging events to the Syslog, in the **Custom Log Management Integrations** section, click the **ADD INTEGRATION** button for Syslog.



iiii	CONFIDENTIAL	Emo Konstruer	🛕 🔞 Fortanix User 🗸
- I II	MANAGER	producer / Societys / Lag management	
ß	💣 Settings	Settings	
m m	Authentication	Account ID: 5c1ebd8b-9400.45c0-96c7-234191d107a5 🗋	
94 88 F	Log Management	Log Management All account events are permanently being stored in CCM. You can collect logs using custom log management integrations.	
@ @		CCM Audit Logs	
		Custom Log Management Integrations	
@ 		> Splunk ADD INTEGRATION	
		Azure Log Analytics	
		Syslog	

FIGURE 10: ADD SYSLOG INTEGRATION

- 1. Configuring a Syslog management integration requires the following information:
 - a. Enter the Hostname or IP address of your Syslog server.
 - You can communicate with a Syslog server either over a non-secure connection or a secure connection using TLS. Depending on the type of TLS certificate that the Syslog server is using,
 - i. Select **Global Root CAs**, if you are using a certificate that is signed by a wellknown public CA.
 - ii. Select Custom CA Certificate, if you as an enterprise want to self-sign the certificate using your own internal CA. To do this, upload the CA certificate using the UPLOAD A FILE button. When Fortanix CCM as a client connects to the Syslog server and is presented with the server's certificate, it will be able to validate it using the enrolled custom CA Certificate.
 - c. The default **Port** number is TCP **514** at which the server must listen for Syslog messages. If you are running on a different port, change to the applicable port number.
 - d. When you log an event in Syslog, you can choose to log it in different facilities. This allows you to filter your log for a specific facility. The facilities appearing in the **Facility** list are well-defined facilities in the Syslog protocol. For example: User, Local0, Local1, and so on. You can configure the Fortanix CCM system to use the Local0 facility for instance. This will help in filtering logs from a particular appliance using a facility.



CCM WITH EXTERNAL LOGGING SYSTEMS

CONFIDENTIAL	Personal v	Ω	🛞 Fortanix User 🗸
MANAGER	senter/Joing/Jagenequeen Settings		
Authentication	Account D: Schedall-Accounts Counter and Account D: Schedall-Accounts Accounts (D)		
Log Management	Log Management		
	Syslog Log Management Integration		
	Host		
	1.1.1.1 Systag server		
	Enable 11.5		
	Validate host		
	Validate certificate G Global Root CAs		
	O Custom CA Centificate		
	Port		
	8088 Systag service port number		
	Local 5yring fieldy		
	SAVE CHANGES CANCEL		

FIGURE 11: SYSLOG INTEGRATION FORM

3.0 APPENDIX

Following are the Splunk Server screenshots-

• If you are using an HTTPS connection, then select the **Enable SSL** check box below in the Global Settings.

Edit Global Settings	;	×	
All Tokens	Enabled	Disabled	
Default Source Type	Select Source Type 🔻		
Default Index	fortani	x_cloud ▼	
Default Output Group	N	one 🔻	
Use Deployment Server			
Enable SSL			
HTTP Port Number ?	8088		
		Cancel Save	

FIGURE 12: ENABLE SSL

2. Port number on the Splunk server used for generating Custom CA Certificate.



General settings Server settings × General settings		
	Splunk server name *	splunk-node-test
		/home/dexter/splunk
	Management port *	8089
		Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.
	SSO Trusted IP	
		The IP address to accept trusted logins from. Only set this If you are using single sign-on (SSO) with a proxy server for authentication.

FIGURE 13: MANAGEMENT PORT NUMBER

3. The index value in the Fortanix CCM Splunk Log Management Integration form should be the same as the Default Index value.

Edit Token: fortanix	_cloud	×
Description	optional	
Source	optional	
Set Source Type	Entered sourcetype 💌	
Source Type	fortanix_audit_v1 •	
Select Allowed Indexes (optional)	Available indexes add all > Selected indexes « remove all I fortanix_cloud I fortanix_cloud I history I fortanix_cloud I main I summary	
	Select indexes that clients will be able to select from.	
Default Index	E fortanix_cloud ▼	
Output Group (optional)	None 🔻	
Enable indexer acknowledgement		
	Cancel	ave

FIGURE 14: INDEX VALUE OF THE SPLUNK SERVER

Fortanix

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/4405381586708-User-s-Guide-Logging

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 – 2021 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.

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.