Configure and Verify Syslog on UCS Intersight Managed Mode

Contents

[ntroduction
Prerequisites
Requirements
Components Used
Background Information
<u>Configure</u>
Fabric Interconnects
Servers
<u>Verify</u>
<u>Froubleshoot</u>
Related Information

Introduction

This document describes the process to setup and verify the Syslog protocol on Intersight Managed Mode UCS Domains.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Unified Computing System (UCS) Servers
- Intersight Managed Mode (IMM)
- Networking basic concepts
- Syslog protocol

Components Used

The information in this document is based on these software versions:

- Intersight software as a service (SaaS)
- Cisco UCS 6536 Fabric Interconnect, firmware 4.3(5.240032)
- Rack Server C220 M5, firmware 4.3(2.240090)
- Alma Linux 9

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Syslog policies are applicable for Fabric Interconnects and Servers. They allow for configuration of local and remote logging.

Configure

- 1. Navigate to **Policies > Create new policy**.
- 2. Choose Syslog, then click Start.

 ← Policies Select Policy Type 				
Filters	Q, Search			
Platform Type All UCS Server UCS Domain UCS Chassis HyperFlex Cluster Kubernetes Cluster	 Backup Configuration BIOS Boot Order Certificate Management Container Runtime Device Connector DNS, NTP and Timezone Drive Security Ethernet Adapter Ethernet Network 	 Fibre Channel QoS Firmware Flow Control HTTP Proxy HTTP Proxy Policy IMC Access IPMI Over LAN ISCSI Adapter ISCSI Adapter ISCSI Static Target Kubernetes Version LAN Connectivity LDAP Link Aggregation Link Control 	 Network CiDR Network Configuration Network Connectivity Node IP Ranges Node OS Configuration NTP Persistent Memory Port Power Replication Network Configuration SAN Connectivity Scrub SD Card Security Serial Over LAN 	 SSH Storage Configuration Switch Control Systog System QoS Thermal Trusted Certificate Authorities vcenter Virtual Machine Infra Config Virtual Machine Infra Virtual Machine Infra Config Virtual Machine Infra State Config State Config Virtual Machine Infra Config Virtual Machine Infra Virtual Machine Infra Config State Config Config State Config State Con
	Cancel			Start

Policy selection

3. Choose the Organization and choose a name, then click Next.

Policies > Syslog Create	
 General Policy Details 	General Add a name, description, and tag for the policy. Organization* default-org Mame* MMM-Systog-Policy Set Tags Enter a tag in the key-value format. Description 0 / 1024
<	Cancel

Configure organization and name

4. Choose the desired minimum severity to report for Local Logging. Severity levels can be referenced on RFC 5424.

$\lim \underline{\mathbf{K}} \subset \underline{\mathbf{J}} + $		
Policies > Syslog Create		
 General Policy Details 	Policy Details Add policy details. Local Logging — File	All Platforms UCS Server (Standalone) UCS Server (FI-Attached) UCS Domain
	Minimum Severity to Report © Debug ~ Warning Re Emergency Alert Critical Error Notice Informational Debug	Enable Enable
<	Cancel	Back

Choose the minumum severity to report for Local Logging

5. Choose the desired minimum severity to report for Remote Logging, and the required settings. These are the remote server(s) IP address or hostname, the port number, and the port protocol (TCP or UDP).

Note: This example uses the default setting UDP port 514. While the port number can be changed, **this only applies to Servers**. Fabric Interconnects use the default port 514 by design.

Policies > Syslog Create						
🧭 General	Policy Details Add policy details.					
Policy Details	Local Logging	<u>м</u>	Platforms UCS	Server (Standalone) UC	S Server (FI-Attached)	UCS Domain
	🛨 File					
	Remote Logging					
	- Syslog Server 1					Enable
	Hostname/IP Address* ()	Port* ()	Prot	tocol * ①		
	142.0.2.2	514	1- 65535			
	Minimum Severity To Report * () Debug ~					
	- Sysiog Server 2				0) Enable
	Hostname/IP Address* () 0.0.0.0 ()	Port* () 514	Prot	tocol * ① DP		
			1-65535			
<	Cancel				Back	Create

Configure Remote Logging parameters

6. Click Create.

7. Assign the Policy to the desired devices.

Fabric Interconnects

- 1. Navigate to the Domain Profile, click Edit, then click Next until step 4 UCS Domain Configuration.
- 2. Under **Management > Syslog**, choose the desired Syslog Policy.

← UCS Domain Profiles Edit UCS Domain Profile (IN)	1M-6536)	
General UCS Domain Assignment US No NO 2 - Figure 1-	UCS Domain Configuration Select the compute and management policies to be associated with the Fabric Interconnect. Show Attached Policies (4)	
VLAN & VSAN Configuration	Anagement 2 of 6 Policies Configured	
UCS Domain Configuration	лтр	Select Policy
6 Summary	Syslog	🖹 🖉 👁 O IMM-Syslog
	Network Connectivity	Select Policy
	SNMP	Select Policy
	LDAP	ඕ ♂ @ ● LDAP-IMM
	Certificate Management	
	V Network 2 of 2 Policies Configured	
<	Close	Back

Choose the syslog policy on a Fabric Interconnect Domain Profile

3. Click Next, then Deploy. The deployment of this policy is not disruptive.

Servers

- 1. Navigate to the Server Profile, click Edit, then go Next until step 4 Management Configuration.
- 2. Choose the Syslog Policy.

← UCS Server Profiles	CSC-C220M5-IMM)	
General	Management Configuration Create or select existing Management policies that you want to associate with this profile.	
Server Assignment	Certificate Management	
Compute Configuration	IMC Access	IMC-CSeries
Management Configuration	IPMI Over LAN	● ipmi_testing
5 Storage Configuration	Local User	● ipmi_user 👔
6 Network Configuration	Serial Over LAN	
7 Summary	SNMP	
	Syslog	× © / IMM-Syslog
<	Close	Back

Choose the syslog policy on a Server Service Profile

3. Continue until the last step and **Deploy**.

Verify

At this point, Syslog messages must be logged on the Syslog remote server(s). For this example, the Syslog server was deployed on a Linux server with the rsyslog library.

Note: Verification of the Syslog messages logging can differ depending based on the remote Syslog server in use.

Confirm that the Fabric Interconnects Syslog messages were logged on the remote server:

```
[root@alma jormarqu]# tail /var/log/remote/msg/192.0.2.3/_.log
Jan 16 15:09:19 192.0.2.3 : 2025 Jan 16 20:11:57 UTC: %VSHD-5-VSHD_Syslog_CONFIG_I: Configured from vty
Jan 16 15:09:23 192.0.2.3 : 2025 Jan 16 20:12:01 UTC: %VSHD-5-VSHD_Syslog_CONFIG_I: Configured from vty
```

Confirm that the Servers Syslog messages were logged on the remote server:

```
[root@alma jormarqu]# tail /var/log/remote/msg/192.0.2.5/AUDIT.log
Jan 16 20:16:10 192.0.2.5 AUDIT[2257]: KVM Port port change triggered with value "2068" by User:(null)
Jan 16 20:16:18 192.0.2.5 AUDIT[2257]: Communication Services(ipmi over lan:enabled,ipmi privilege leve
Jan 16 20:16:23 192.0.2.5 AUDIT[2257]: Local User Management (strong password policy :disabled) by User
Jan 16 20:16:23 192.0.2.5 AUDIT[2257]: Password Expiration Parameters (password_history:5,password_expi
Jan 16 20:16:26 192.0.2.5 AUDIT[2257]: Local Syslog Severity changed to "Debug" by User:(null) from Int
Jan 16 20:16:27 192.0.2.5 AUDIT[2257]: Secured Remote Syslog with(serverId =1, secure_enabled =0) by Us
```

Troubleshoot

A packet capture can be performed on the Fabric Interconnects to confirm if the Syslog packets were forwarded correctly. Change the minimum severity to report to **debug**. Ensure Syslog reports as much information as possible.

From the command line interface, start a packet capture on the management port and filter by port 514 (Syslog port):

<#root>
FI-6536-A# connect nxos
FI-6536-A(nx-os)# ethanalyzer
local interface mgmt
 capture-filter "
port 514
" limit-captured-frames 0
Capturing on mgmt0

In this example, a server port on Fabric Interconnect A was flapped to generate Syslog traffic.

- 1. Navigate to **Fabric Interconnects > Inventory**.
- 2. Click the checkbox for the desired port, open the ellipsis menu on the right, and choose disable.

FI-6536 FI-A O Critical					Actions ~
General <u>Inventory</u> Con	nections UCS Domain I	Profile Topology	Metrics		
Ports & Port Channels	Ports & Port Channe	əls			
Fan Modules	Ethernet FC Ether	met Port Channels	FC Port Channels		
PSUs	14 TA TE 34 TA	5A V6 7A V8	94 VI0 114 V12 134 V14 154	<u>¥16 17A ¥18 18A ¥20 21A ¥22 23A ¥24 25A ¥26 27A ¥28 28A ¥</u>	200 31A 722 32A 734 25A 736
Local Storage	ATTELY ATTELY	-			X ATTEX ATTEX
Traffic Mirroring (SPAN)	•0 •••				
				Ethernet Uplink Po	rt Channel 🔵 Server 🌑 Unconfigured
	Q Search]	▼ Filters 35 results		🛆 Export
	Name	MAC :	Role :	Peer	@
	Port 1/1		Ethernet Uplink Port Channel M		
	Port 1/2		Ethernet Uplink Port Channel M		
			Server		
	Port 1/3 Port 1/4		Server Unconfigured		 Disable
	Port 1/3 Port 1/4 Port 1/5		Server Unconfigured Unconfigured		Disable Reset
	Port 1/3 Port 1/4 Port 1/5 Port 1/6		Server Unconfigured Unconfigured Unconfigured		Disable Reset
	Port 1/3 Port 1/4 Port 1/5 Port 1/6 Port 1/7		Server Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured		Uisable

Shut down an interface on an Fabric Interconnect to generate syslog traffic for testing

3. The console on the Fabric Interconnect must capture the Syslog packet:

<#root>

FI-6536-A(nx-os)# ethanalyzer local interface mgmt capture-filter "port 514" limit-captured-frames Capturing on mgmt0 2025-01-16 22:17:40.676560

192.0.2.3 -> 192.0.2.2

Syslog LOCAL7.NOTICE

: : 2025 Jan 16 22:17:40 UTC: %ETHPORT-5-IF_DOWN_NONE:

Interface Ethernet1/3 is down

(Transceiver Absent)

4. The message must be logged in your remote server:

<#root>

```
[root@alma jormarqu]# tail -n 1 /var/log/remote/msg/192.0.2.3/_.log
Jan 16 17:15:03
```

192.0.2.3

```
: 2025 Jan 16 22:17:40 UTC:
```

%ETHPORT-5-IF_DOWN_NONE: Interface Ethernet1/3 is down (Transceiver Absent)

The same test can be run on servers:

Note: This procedure only works for servers with out-of-band configuration on their IMC Access Policy. If Inband is in use, perform the packet capture on the remote Syslog server instead, or reach out to TAC to perform it with internal debug commands.

← UCS Server Profiles		
UCSC-C220M5-IMM		Actions ~
General Server Inventory Connectivity		
Details	Configuration =	IMC Access Details
Status © OK	General Identifiers vNICs / vHBAs	General
Name	All Compute Management Network Storage	IMC-CSeries
UCSC-C220M5-IMM	Boot Order © MXSVLAB_BootLocal @	Organization
User Label	IMC Access Policy IMC-CSeries 👔	default-org
-	IPMI Over LAN ipmi_testing 👔	Policy Details
Target Platform	LAN Connectivity IMM-LAN-SV 🕼	In-Band Configuration
Template Name	Local User ipmi_user 🕼	Enabled No
	Syslog IMM-Syslog 🕼	
Last Update	Virtual KVM KVM_IMM	Out-Of-Band Configuration
		Enabled Yes

Verify the configuration on the IMC access policy

In this example, the LED locator on a C220 M5 Integrated Server was enabled. This does not require downtime.

1. Verify which Fabric Interconnect sends out-of-band traffic for your server. The server IP is 192.0.2.5, so Fabric Interconnect A forwards its management traffic ("secondary route" means that the Fabric Interconnect acts as a proxy for the server management traffic):

```
<#root>
FI-6536-A
(nx-os)# show ip interface mgmt 0
IP Interface Status for VRF "management"(2)
mgmt0, Interface status: protocol-up/link-up/admin-up, iod: 2,
IP address: 192.0.2.3, IP subnet: 192.0.2.0/24 route-preference: 0, tag: 0
IP address:
192.0.2.5
, IP subnet: 192.0.2.0/24
secondary route-preference
: 0, tag: 0
```

2. Start a packet capture on the appropriate Fabric Interconnect:

FI-6536-A(nx-os)# ethanalyzer local interface mgmt capture-filter "port 514" limit-captured-frames Capturing on mgmt0

3. Navigate to Servers > Actions > System and choose Turn On Locator:

FI-6536-1 Ocritical					Actions 🗸
General Inventory UCS Server Profile	ICL Topology Metrics Connectivity			Power	>
	iez repercy mentee connection,		Turn On Locator	System	
Details	Properties			Profile	
			Reset vKVM	VMware	
Health	Cisco UCSC-C220-M5SX	Front Rea	Lock Front Panel	Install Operating	System
			Rediscover	Upgrade Firmwar	e
Name FI-6536-1			Decommission	Launch vKVM	
User Label	Power On Locator LED Off	- Heal	Secure Erase	Launch Tunneled	vKVM
-			Certificate >	Start Alarm Supp	ression
UCS Server Profile	CPUs	CPU Capacity (GHz)	Reboot Management Controller	Open TAC Case	
	Threads			Set License Tier	
© OK	56		Reset Memory Errors	Collect Tech Supp	port Bundle
Management IP	CPU Cores	Adapters	Set Asset Tag	I PM	
	28	1	Set User Label		
Serial	CPU Cores Enabled 28	UUID	Disable Tunneled vKVM		
Mac Address	Memory Capacity (GiB)		Download System Event Log		
•	256.0		Clear System Event Log		
PID					
UCSC-C220-M5SX					
Vendor Cisco Systems Inc					

Turn on LED locator in a Server

4. The console on the Fabric Interconnect must show the Syslog packet captured:

<#root>

```
FI-6536-A(nx-os)# ethanalyzer local interface mgmt capture-filter "port 514" limit-captured-frames
Capturing on mgmt0
2025-01-16 22:34:27.552020
```

192.0.2.5 -> 192.0.2.2

Syslog AUTH.NOTICE

: Jan 16 22:38:38 AUDIT[2257]: 192.0.2.5 CIMC Locator LED is modified to "ON" by User:(null) from Interface :redfish Remote IP:

5. The Syslog message must be logged in your remote server AUDIT.log file:

<#root>
root@alma jormarqu]# tail -n 1 /var/log/remote/msg/192.0.2.5/AUDIT.log
Jan 16 22:38:38
192.0.2.5
AUDIT[2257]:
CIMC Locator LED is modified to "ON"
by User:(null) from Interface:

If Syslog packets were generated by UCS, but the Syslog server did not log them:

- 1. Confirm that the packets arrived at the remote Syslog server with a packet capture.
- 2. Verify the configuration of your remote Syslog server (including but not limited to: configured syslog port and firewall settings).

Related Information

- <u>RFC 5424 The Syslog Protocol</u>
- Intersight IMM Expert Series Syslog Policy
- <u>Cisco Intersight Help Center Configure UCS Domain Profile Policies</u>
- <u>Cisco Intersight Help Center Configure Server Policies</u>

```
If the Server has Inband configured on its IMC Access Policy, load CIMC debug shell and perform a
packet capture on the bond0 interface for Racks, or bond0.x interface (where x is the VLAN) for Blades.
[Thu Jan 16 23:12:10 root@C220-WZP22460WCD:~]$tcpdump -i bond0 port 514 -v
tcpdump: listening on bond0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:12:39.817814 IP (tos 0x0, ttl 64, id 24151, offset 0, flags [DF], proto UDP (17), length 173)
192.168.70.25.49218 > 10.31.123.134.514: Syslog, length: 145
Facility auth (4), Severity notice (5)
Msg: Jan 16 23:12:39 C220-WZP22460WCD AUDIT[2257]: CIMC Locator LED is modified to "OFF" by User:(null
```

• The Syslog port number **cannot** be changed on Fabric Interconnects, only in Servers. This is by design and was documented on