Konfiguration und Überprüfung von Syslog im verwalteten UCS Intersight-Modus

Inhalt

Einleitung
/oraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Fabric Interconnects
Server
Überprüfung
Fehlerbehebung
Zugehörige Informationen

Einleitung

In diesem Dokument wird der Prozess zur Einrichtung und Überprüfung des Syslog-Protokolls für Intersight Managed Mode-UCS-Domänen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Unified Computing System (UCS)-Server
- Intersight Managed Mode (IMM)
- Grundlegende Netzwerkkonzepte
- Syslog Protokoll

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- 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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Syslog-Richtlinien gelten für Fabric Interconnects und Server. Sie ermöglichen die Konfiguration der lokalen und Remote-Protokollierung.

Konfigurieren

- 1. Navigieren Sie zu Policies > Create new policy (Richtlinien > Neue Richtlinie erstellen).
- 2. Wählen Sie Syslog aus, und klicken Sie dann auf Start.

← Policies Select Policy Type				
Filters	۹, Search			
Filters Platform Type All UCS Server UCS Domain UCS Chassis HyperFlex Cluster Kubernetes Cluster	Search Backup Configuration BIOS Boot Order Certificate Management Container Runtime Device Connector DNS, NTP and Timezone Drive Security Ethernet Adapter Ethernet Network Control Ethernet Network Group Ethernet Network Group Ethernet QoS External FC Storage External ISCSI Storage	 Fibre Channel QoS Firmware Flow Control HTTP Proxy HTTP Proxy Policy IMC Access IPMI Over LAN 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 Socub SD Card Serial Over LAN 	 SSH Storage Storage Configuration Switch Control Switch Control System QoS Thermal Trusted Certificate Authorities vCenter Virtual KVM Virtual Machine Infra Config Virtual Machine Instance Type Virtual Media VIAN
	Cancel			Start

Richtlinienauswahl

3. Wählen Sie die Organisation aus, und wählen Sie einen Namen, und klicken Sie dann auf Weiter.

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

Organisation und Namen konfigurieren

4. Wählen Sie den gewünschten minimalen Schweregrad für die lokale Protokollierung aus. Auf RFC 5424 kann auf Schweregrade verwiesen werden.

Policies > Syslog Create	
General Policy Details	Policy Details Add policy details. XII Platforms UCS Server (Standalone) UCS Server (Fi-Attached) UCS Domain
	Local Logging
	- File
	Minimum Severity to Report* © Debug Re Emergency Alert Critical Error Notice Informational Debug
	Cancel Back Create

Wählen Sie den Mindestschweregrad für die lokale Protokollierung aus.

5. Wählen Sie den gewünschten minimalen Schweregrad für die Remote-Protokollierung und die erforderlichen Einstellungen aus. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-Servers bzw. der Remote-Server, die Portnummer und das Port-Protokoll (TCP oder UDP).

Anmerkung: In diesem Beispiel wird die Standardeinstellung für UDP-Port 514

verwendet. Die Portnummer kann zwar geändert werden, gilt jedoch nur für Server. Fabric Interconnects verwenden den Standardport 514.

Create					
General	Policy Details				
-	Add policy details.				
2 Policy Details		All Platforms	UCS Server (Standalone) UCS Server (FI-Attached) UCS Domain		
	Local Logging				
	🛨 File				
	Remote Logging				
	- Syslog Server 1		Enable		
	Hostname/IP Address* ①	Port* ①	Protocol * ①		
	[192.0.2.2)	514	UDP ~		
		1 - 65535			
	Minimum Severity To Report * ①				
	Debug ~				
	Syslog Server 2		Enable		
	Hostname/IP Address • ①	Port* ①	Protocol* ①		
	0.0.0.0	514	UDP ~		
		1 - 65535			
<	Cancel		Back		

Remote-Protokollierungsparameter konfigurieren

- 6. Klicken Sie auf Erstellen.
- 7. Weisen Sie die Richtlinie den gewünschten Geräten zu.

Fabric Interconnects

- 1. Navigieren Sie zum Domänenprofil, klicken Sie auf Bearbeiten, und klicken Sie dann bis zu Schritt 4 UCS-Domänenkonfiguration auf Weiter.
- 2. Wählen Sie unter Management > Syslog die gewünschte Syslog-Richtlinie aus.

6 LICS Domain Profiles		
Edit UCS Domain Profile (IM	M-6536)	
General General UCS Domain Assignment	UCS Domain Configuration Select the compute and management policies to be associated with the Fabric Interconnect. Show Attached Policies (4)	
VLAN & VSAN Configuration Ports Configuration	A Management 2 of 6 Policies Configured	
5 UCS Domain Configuration	NTP	Select Policy
6 Summary	Syslog	🖻 🖉 👁 O IMM-Syslog
	Network Connectivity	Select Policy
	SNMP	Select Policy
	LDAP	
	Certificate Management	🗎 🛛 🖉 🗍 👁 📔 MM-LDAPS-Cert
	V Network 2 of 2 Policies Configured	
<	Close	Back

Auswahl der Syslog-Richtlinie in einem Fabric Interconnect-Domänenprofil

3. Klicken Sie auf Weiter und dann auf Bereitstellen. Die Bereitstellung dieser Richtlinie erfolgt unterbrechungsfrei.

Server

- 1. Navigieren Sie zum Serverprofil, klicken Sie auf Bearbeiten, und gehen Sie dann bis zu Schritt 4 Verwaltungskonfiguration zu Weiter.
- 2. Wählen Sie die Syslog-Richtlinie aus.

CUCS Server Profiles	SC-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	
	vysky Virtual KVM	KVM_IMM
<	Close	Back

Auswahl der Syslog-Richtlinie in einem Server-Serviceprofil

3. Fahren Sie bis zum letzten Schritt fort, und stellen Sie bereit.

Überprüfung

An diesem Punkt müssen Syslog-Meldungen auf den Syslog-Remoteservern protokolliert werden. In diesem Beispiel wurde der Syslog-Server auf einem Linux-Server mit der rsyslog-Bibliothek bereitgestellt.

Anmerkung: Die Überprüfung der Syslog-Nachrichtenprotokollierung kann je nach verwendetem Remote-Syslog-Server unterschiedlich ausfallen.

Vergewissern Sie sich, dass die Fabric Interconnects Syslog-Meldungen auf dem Remote-Server protokolliert wurden:

[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

Vergewissern Sie sich, dass die Syslog-Meldungen des Servers auf dem Remote-Server protokolliert wurden:

[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

Fehlerbehebung

Auf den Fabric Interconnects kann eine Paketerfassung durchgeführt werden, um sicherzustellen, dass die Syslog-Pakete richtig weitergeleitet wurden. Ändern Sie den minimalen Schweregrad für den Bericht zum Debuggen. Stellen Sie sicher, dass Syslog so viele Informationen wie möglich meldet.

Starten Sie über die Kommandozeile eine Paketerfassung am Management-Port, und filtern Sie nach 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 diesem Beispiel wurde ein Server-Port an Fabric Interconnect A mit Flapping versehen, um Syslog-Datenverkehr zu generieren.

- 1. Navigieren Sie zu Fabric Interconnects > Bestand.
- 2. Klicken Sie auf das Kontrollkästchen für den gewünschten Port, öffnen Sie das Menü mit den Auslassungszeichen auf der rechten Seite, und wählen Sie Deaktivieren aus.

← Fabric Interconnects FI-6536 FI-A (@ Critical)						Actions ~
General Inventory Conn	ections UCS Domain Pro	file Topology Metrics				
Ports & Port Channels	Ports & Port Channels					
Fan Modules	Ethernet FC Etherne	t Port Channels FC Port Chann	els			
PSUs	14 TA T2 34 T4	5 × ¥6 74 ¥8 94 ¥10 114	¥12 134 ¥14 154 '	₩16 17A ₩18 19A ₩20 21A ₩22 22/	A ¥24 25A ¥26 27A ¥28 29A ¥30 31A ¥22	23 A 734 25A 736
Local Storage	ATTEX ATTEX		······································			
Traffic Mirroring (SPAN)						
					Ethernet Uplink Port Channel	Server Unconfigured
	Q Search	▼ Filters 35	results			Export
	Name	MAC : Role		Peer		<u>@</u>
	Port 1/1	Ethernet Upli	nk Port Channel M			
	Port 1/2	Ethernet Upli	nk Port Channel M			
		Server				
	Port 1/4	Unconfigured	1			Disable
	Port 1/5	Unconfigured				Reset
	Port 1/6	Unconfigured	1			
	Port 1/7	Unconfigured	1			
	Port 1/8	Unconfigured	1			

Herunterfahren einer Schnittstelle an einem Fabric Interconnect, um Syslog-Datenverkehr für Tests zu generieren

3. Die Konsole auf Fabric Interconnect muss das Syslog-Paket erfassen:

<#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. Die Meldung muss auf dem Remote-Server protokolliert werden:

<#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)
```

Derselbe Test kann auf Servern ausgeführt werden:

Anmerkung: Dieses Verfahren funktioniert nur für Server mit Out-of-Band-Konfiguration in ihrer IMC-Zugriffsrichtlinie. Wenn Inband verwendet wird, führen Sie stattdessen die Paketerfassung auf dem Remote-Syslog-Server durch, oder wenden Sie sich an das TAC, um sie mit internen Debug-Befehlen durchzuführen.

(1100 0 B-+ (1		
CCS Server Profiles		
0030-0220113-11111		Actions V
General Server Inventory Connectivity	y la	
Details	Configuration IMC Access Details	
Status	General Identifiers vNICs / vHBAs General	
	All Compute Management Network Storage Name	
Name	IMC-CSeries	
UCSC-C220M5-IMM	Boot Order © MXSVLAB_BootLocal III Organization	
User Label	IMC Access Policy IMC-CSeries II default-org	
•	IPMI Over LAN ipmi_testing () Policy Details	
Target Platform	LAN Connectivity IMM-LAN-SV III In-Band Configuration	
UCS Server (FI-Attached)	Enabled	
Template Name	Local User Ipmi_user III No	
	Syslog IMM-Syslog (
Last Update	Virtual KVM KVM_IMM (
	Enabled	

Überprüfen der Konfiguration in der IMC-Zugriffsrichtlinie

In diesem Beispiel wurde der LED-Positionsgeber auf einem integrierten C220 M5-Server aktiviert. Dies erfordert keine Ausfallzeiten.

 Überprüfen Sie, welcher Fabric Interconnect Out-of-Band-Datenverkehr für Ihren Server sendet. Die Server-IP-Adresse lautet 192.0.2.5, sodass Fabric Interconnect A seinen Verwaltungsdatenverkehr weiterleitet ("sekundäre Route" bedeutet, dass Fabric Interconnect als Proxy für den Serververwaltungsdatenverkehr fungiert):

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. Starten Sie eine Paketerfassung auf dem entsprechenden Fabric Interconnect:

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

3. Navigieren Sie zu Server > Aktionen > System, und wählen Sie Locator einschalten aus:

FI-6536-1 🜘 Critical					Actions ~
Conners Inventerur, 1100 Samuer Dreffle, 1101 Tanalamu, Matrice, Cannesticitur					
General Inventory OCS Server Profile H	CL Topology Metrics Connectivity		Turn On Locator	System	>
Details	Properties			Profile	>
			Reset vKVM	VMware	>
Health O Critical	Cisco UCSC-C220-M5SX	Front R	Ear Lock Front Panel	Install Operatin	g System
			Rediscover	Upgrade Firmw	/are
Name FI-6536-1			Decommission	Launch vKVM	
User Label	Power On Locator LED Off	H	Secure Erase	Launch Tunnek	ed vKVM
			Certificate >	Start Alarm Sup	pression
UCS Server Profile	CPUs	CPU Capacity (GHz)	Reboot Management Controller	Open TAC Case	Ð
UCSC-C220M5-IMM	2 Threade	12.8		Set License Tie	н
OCS Server Profile Status	56		Reset Memory Errors	Collect Tech Su	upport Bundle
Management IP	CPU Cores	Adapters	Set Asset Tag	IPM	
	28		Set User Label		
Serial	CPU Cores Enabled	UUID	Disable Tunneled vKVM		
	Memory Canacity (CiB)		Download System Event Log		01 011
mac Address	256.0		Clear System Event Log		01
PID					
UCSC-C220-M5SX					
Vendor Cisco Systems Inc					

Aktivieren der LED-Positionsbestimmung in einem Server

4. Die Konsole auf dem Fabric Interconnect muss das erfasste Syslog-Paket anzeigen:

<#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

```
: 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. Die Syslog-Meldung muss in der Datei AUDIT.log des Remote-Servers protokolliert werden .:

```
<#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:
```

Wenn Syslog-Pakete vom UCS generiert, aber vom Syslog-Server nicht protokolliert wurden:

- 1. Bestätigen Sie, dass die Pakete mit einer Paketerfassung am Remote-Syslog-Server angekommen sind.
- 2. Überprüfen Sie die Konfiguration des Remote-Syslog-Servers (einschließlich, aber nicht beschränkt auf: konfigurierten Syslog-Port und Firewall-Einstellungen).

Zugehörige Informationen

- <u>RFC 5424 The Syslog Protocol</u>
- Intersight IMM Expert-Serie Syslog-Richtlinie
- <u>Cisco Intersight Help Center: Konfigurieren von UCS-Domänenprofilrichtlinien</u>
- <u>Cisco Intersight Help Center Serverrichtlinien konfigurieren</u>

Wenn für den Server Inband in seiner IMC-Zugriffsrichtlinie konfiguriert ist, laden Sie die CIMC-Debug-Shell, und führen Sie eine Paketerfassung für die bond0-Schnittstelle für Racks oder die bond0.x-Schnittstelle (wobei x das VLAN ist) für Blades durch.

```
[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
```

 Die Syslog-Portnummer kann auf Fabric Interconnects nicht geändert werden, sondern nur auf Servern. Dies ist vom Entwurf her und wurde dokumentiert am

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.