UCS Intersightマネージドモードのsyslogの設定 と確認

内容	
<u>はじめに</u>	
前提条件	
<u>要件</u>	
<u>使用するコンポーネント</u>	
<u>背景説明</u>	
<u>設定</u>	
Fabric Interconnect	
<u>+-//</u>	
<u>確認</u>	
<u>トラブルシュート</u>	
<u>関連情報</u>	

はじめに

このドキュメントでは、Intersight Managed Mode UCSドメインでSyslogプロトコルをセットア ップして確認するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Unified Computing System(UCS)サーバ
- Intersightマネージドモード(IMM)
- ネットワーキングの基本概念
- Syslogプロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Intersight Software as a Service(SaaS)
- Cisco UCS 6536ファブリックインターコネクト、ファームウェア4.3(5.240032)
- ラックサーバC220 M5、ファームウェア4.3(2.240090)
- ・アルマLinux 9

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

Syslogポリシーは、ファブリックインターコネクトとサーバに適用できます。ローカルロギング とリモートロギングを設定できます。

設定

- 1. Policies > Create new policyの順に移動します。
- 2. Syslogを選択し、Startをクリックします。

 ← 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 Control Ethernet Network Croup Ethernet Network Croup Ethernet QoS External FC Storage External ISCSI Storage Cancel	 Fibre Channel QoS Firmware Flow Control HTTP Proxy HTTP Proxy Policy IMC Access IPMI Over LAN ISCSI Adapter ISCSI Boot 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 Storage Configuration Switch Control System QoS Thermal Trusted Certificate Authorities vcenter Virtual KVM Virtual Machine Instance Type Virtual Media VLAN VSAN

ポリシーの選択

3. 組織を選択して名前を選択し、Nextをクリックします。

Create	
General	General
2 Policy Details	Add a name, description, and tag for the policy.
	Organization "
	Name*
	IMM-Sysiog-Policy
	Set Tags
	Enter a tag in the key-value format.
	Description
	Description
	0 / 1024
<	Cancel

4. ローカルロギングに対してレポートする最小重大度を選択します。重大度は、<u>RFC 5424</u>で 参照できます。

Policies > Syslog		
Create		
General	Policy Details Add policy details	
Policy Details		
	Local Logging	
	- File	
	Minimum Severity to Benort*	
	Debug ^	
	Warning	
	Re Emergency	
	Alert	
	Critical	
	Error	
	Notice	
	Informational	
	Debug	
	Cancel Back Create	J

ローカルロギングで報告する重大度の最小値を選択します

5. リモートロギングに対してレポートする最小重大度と必要な設定を選択します。これらは、 リモートサーバのIPアドレスまたはホスト名、ポート番号、およびポートプロトコル (TCPまたはUDP)です。

◇ 注:この例では、デフォルト設定のUDPポート514を使用しています。ポート番号は 変更できますが、これはサーバだけに適用されます。ファブリックインターコネクト

組織と名前の設定



Policies > Systog Create			
General	Policy Details Add policy details.		
Policy Details	Local Logging	All Platforms	UCS Server (Standalone) UCS Server (FI-Attached) UCS Domain
	🛨 File		
	Remote Logging		
	— Syslog Server 1		Enable
	Hostname/IP Address * ①	Port* ①	Protocol* ()
	92.0.2.2 (8)	514 A	UDP ·
	Minimum Severity To Report * ①		
	Debug ~		
	- Syslog Server 2		C Enable
	Hostname/IP Address * ①	Port* ①	Protocol * ()
	0.0.0.0 🛞	514	UDP ~
<	Cancel		Back

リモートロギングパラメータの設定

- 6. [Create] をクリックします。
- 7. 目的のデバイスにポリシーを割り当てます。

Fabric Interconnect

- 1. Domain Profileに移動して、Editをクリックし、ステップ4 UCS Domain Configurationまで Nextをクリックします。
- 2. Management > Syslogで、目的のSyslogポリシーを選択します。

Edit UCS Domain Profiles	M-6536)	
General	UCS Domain Configuration Select the compute and management policies to be associated with the Fabric Interconnect.	
UCS Domain Assignment	Show Attached Policies (4)	
VLAN & VSAN Configuration	∧ Management 2 of 6 Policies Configured	
Ports Configuration		
UCS Domain Configuration	NTP	Select Policy
6 Summary	Syslog	🗎 🖉 👁 O IMM-Syslog
	Network Connectivity	Select Policy
	SNMP	Select Policy
	LDAP	🖹 ⊘ © ● LDAP-IMM
	Certificate Management	
	V Network 2 of 2 Policies Configured	
<	Close	Back

ファブリックインターコネクトドメインプロファイルのsyslogポリシーを選択します

3. Next、Deployの順にクリックします。このポリシーの導入によって中断が発生することは ありません。

サーバ

- 1. Server Profileに移動し、Editをクリックしてから、ステップ4 Management ConfigurationまでNextに進みます。
- 2. Syslog Policyを選択します。

← UCS Server Profiles Edit UCS Server Profile (UC)	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	Ø ipmi_testing
5 Storage Configuration	Local User	⊘ ipmi_user
6 Network Configuration	Serial Over LAN	
	SNMP	
(7) Summary	Syslog	× 👁 🖉 🛛 IMM-Syslog 📶
	Virtual KVM	● KVM_IMM
<	Close	Back

サーバサービスプロファイルのsyslogポリシーを選択します

3. 最後のステップまで続行し、展開します。

確認

この時点で、SyslogメッセージはSyslogリモートサーバに記録される必要があります。 この例で は、syslogサーバはsyslogライブラリを備えたLinuxサーバに展開されています。

✤ 注:Syslogメッセージのロギングの検証は、使用しているリモートSyslogサーバによって異なる場合があります。

Fabric Interconnectのsyslogメッセージがリモートサーバに記録されたことを確認します。

[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

サーバのsyslogメッセージがリモートサーバに記録されたことを確認します。

[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

トラブルシュート

Syslogパケットが正しく転送されたかどうかを確認するために、ファブリックインターコネクト でパケットキャプチャを実行できます。レポートする重大度の最小値をdebugに変更します。 Syslogが可能な限り多くの情報を報告するようにします。

コマンドラインインターフェイスから、管理ポートでパケットキャプチャを開始し、ポート 514(Syslogポート)でフィルタリングします。

<#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

この例では、Syslogトラフィックを生成するために、Fabric Interconnect Aのサーバポートがフラ ップされました。

- 1. Fabric Interconnects > Inventoryの順に移動します。
- 2. 目的のポートのチェックボックスをクリックし、右側の省略記号メニューを開いて disableを選択します。

← Fabric Interconnects FI-6536 FI-A (© critical			Actions ~
General Inventory Cor	nnections UCS Domain Profile	Topology Metrics	
Ports & Port Channels	Ports & Port Channels		
Fan Modules	Ethernet FC Ethernet Port C	Channels FC Port Channels	
PSUs	14 1A Y2 3A Y4 3A Y6	<u></u>	29 A T30 31 A T22 33 A T34 35 A T36
Local Storage			
Traffic Mirroring (SPAN)			
		@ Ethernet I k	Server Alloconfigured
			enk Port Chaimer Server Oncomgares
	Q Search	▼ Filters 35 results	🔿 Export
	Name MA	C : Role : Peer	@
	Port 1/1	Ethernet Uplink Port Channel M	
	Port 1/2	Ethernet Uplink Port Channel M	
	Port 1/3	Server -	
	Port 1/4	Unconfigured -	Disable
	Port 1/5	Unconfigured -	Reset
	Port 1/6	Unconfigured -	
	Port 1/7	Unconfigured -	
	Port 1/8	Unconfigured -	

テスト用のsyslogトラフィックを生成するためにFabric Interconnect上のインターフェイスをシャットダウンする

3. Fabric Interconnect上のコンソールでは、Syslogパケットをキャプチャする必要があります

o

<#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. メッセージは、リモートサーバにログインしている必要があります。

<#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)

同じテストをサーバでも実行できます。

◆ 注:この手順は、IMCアクセスポリシーでアウトオブバンド設定を行っているサーバでのみ 機能します。インバンドを使用している場合は、代わりにリモートsyslogサーバでパケット キャプチャを実行するか、TACに連絡して内部debugコマンドを使用して実行します。

← UCS Server Profiles		
UCSC-C220M5-IMM	Action	is V
General Server Inventory Connectivity	ı —	
Details	Configuration IIMC Access Details	
Status	General Identifiers vNICs / vHBAs General	
	All Compute Management Network Storage IMC-CSeries	
Name UCSC-C220M5-IMM	Boot Order © MXSVLAB_BootLocal @ Organization	
User Label	IMC Access Policy IMC-CSeries III default-org	
	IPMI Over LAN ipmi_testing () Policy Details	
Target Platform	LAN Connectivity IMM-LAN-SV I	
Template Name	Local User ipmi_user I Phabled No	
	Syslog IMM-Syslog D	
Last Update a few seconds ago	Virtual KVM Cut-Of-Band Configuration	
	Enabled Yes	

IMCアクセスポリシーの設定を確認します

この例では、C220 M5統合サーバのLEDロケータが有効になっています。これにはダウンタイム は必要ありません。

 サーバにアウトオブバンドトラフィックを送信するFabric Interconnectを確認します。サー バIPは192.0.2.5であるため、Fabric Interconnect Aはその管理トラフィックを転送します (「セカンダリルート」とは、Fabric Interconnectがサーバ管理トラフィックのプロキシと して動作することを意味します)。

<#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. 該当するFabric Interconnectでパケットキャプチャを開始します。

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

3. Servers > Actions > Systemの順に移動し、Turn On Locatorを選択します。

FI-6536-1 O Critical				A	ctions ~
Canaral Inventory IICS Server Profile IICI Topology Matrice Connectivity				Power	
	Topology methos connectivity		Turn On Locator	System	
Details	Properties			Profile	>
			Reset vKVM	VMware	>
Health Critical	Cisco UCSC-C220-M5SX	Front Rear	Lock Front Panel	Install Operating Sy	stem
			Rediscover	Upgrade Firmware	
Name FI-6536-1			Decommission	Launch vKVM	
User Label	Power On Locator I ED O Off		Secure Erase	Launch Tunneled v	кум
-			Certificate >	Start Alarm Suppre	ssion
UCS Server Profile	CPUs	CPU Capacity (GHz)	Reboot Management Controller	Open TAC Case	
UCSC-C220M5-IMM	2	72.8		Set License Tier	
UCS Server Profile Status	56		Reset Memory Errors	Collect Tech Suppo	ort Bundle
Management IP	CPU Cores	Adapters	Set Asset Tag	I PM	
	28		Set User Label		
Serial	CPU Cores Enabled	UUID	Disable Tunneled vKVM		
	20 Momony Connelity (CID)		Download System Event Log	01	@ 11
Mac Address	256.0		Clear System Event Log		
PID					
UCSC-C220-M5SX					
Vendor Cisco Systems Inc					

サーバのLEDロケータをオンにする

4. Fabric Interconnect上のコンソールには、キャプチャされたSyslogパケットが表示される必要があります。

<#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

5. Syslogメッセージは、リモートサーバのAUDIT.logファイルに記録する必要があります。

<#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:

syslogパケットがUCSによって生成されたものの、syslogサーバがログに記録しなかった場合:

- 1. パケットキャプチャを使用して、パケットがリモートSyslogサーバに到着したことを確認し ます。
- 2. リモートSyslogサーバの設定を確認します(設定されたSyslogポートとファイアウォールの 設定を含みますが、これに限定されません)。

関連情報

- <u>RFC 5424 Syslogプロトコル</u>
- ・ <u>Intersight IMM Expertシリーズ Syslogポリシー</u>
- ・ Cisco Intersightヘルプセンター UCSドメインプロファイルポリシーの設定
- ・ <u>Cisco Intersightヘルプセンター サーバーポリシーの設定</u>

サーバのIMCアクセスポリシーにインバンドが設定されている場合、CIMCデバッグシェルをロ ードし、ラックの場合はbond0インターフェイス、ブレードの場合はbond0.xインターフェイス (xはVLAN)でパケットキャプチャを実行します。

[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

Syslogポート番号は、サーバ内のみで、ファブリックインターコネクト上では変更できません。これは設計上の問題であり、

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。