Configuration et vérification de Syslog en mode géré UCS Intersight

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Interconnexions de fabric
Serveurs
Vérifier
<u>Dépannage</u>
Informations connexes

Introduction

Ce document décrit le processus de configuration et de vérification du protocole Syslog sur les domaines UCS en mode géré Intersight.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveurs UCS (Unified Computing System)
- Mode géré Intersight (IMM)
- Concepts de base des réseaux
- protocole Syslog

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Intersight en tant que service (SaaS)
- Interconnexion de fabric Cisco UCS 6536, microprogramme 4.3(5.240032)
- Serveur rack C220 M5, microprogramme 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les stratégies Syslog s'appliquent aux interconnexions de fabric et aux serveurs. Ils permettent de configurer la journalisation locale et distante.

Configurer

- 1. Accédez à Politiques > Créer une nouvelle politique.
- 2. Choisissez Syslog, puis cliquez sur Start.

Filters Search Platform Type Backup Configuration Fibre Channel QoS Network CIDR SSH Image: Platform Type BloS Fibre Channel QoS Network CIDR SSH Image: Platform Type BloS Fibre Channel QoS Network Configuration Storage Image: Platform Type BloS Fibre Channel QoS Network Configuration Storage Image: Platform Type BloS Firmware Network Configuration Storage UCS Server Boot Order Flow Control Network Connectivity Storage Configuration UCS Chassis Certificate Management HTTP Proxy Node IP Ranges Switch Control UCS Chassis Container Runtime Http Proxy Policy Node OS Configuration System QoS Mubernetes Cluster Device Connector IMC Access NTP System QoS Dirive Security ISCSI Adapter Port Trusted Certificate Dirive Security ISCSI Boot Power vcenter Ethernet Network ISCSI Static	 ← Policies Select Policy Type 				
Platform Type Backup Confliguration Fibre Channel QoS Network CIDR SSH Image: All BIOS Firmware Network Configuration Storage UCS Server Boot Order Flow Control Network Connectivity Storage Configuration UCS Domain Certificate Management HTTP Proxy Node IP Ranges Switch Control UCS Chassis Container Runtime Http Proxy Policy Node OS Configuration Syslog HyperFlex Cluster Device Connector IMC Access NTP System QoS Kubernetes Cluster Device Connector IPMI Over LAN Persistent Memory Thermal Drive Security ISCSI Adapter Port Trusted Certificate Analyorities Ethernet Network Ethernet Network ISCSI Static Target Replication Network Configuration Virtual XVM Ethernet Network ISCSI Static Target SAN Connectivity Virtual Machine Infra Configuration Ethernet Network Croup LAN Connectivity Scrub Virtual Machine Instance	Filters	۹ Search			
O Ethernet QoS O LDAP O SD Card O Virtual Media O External FC Storage O Link Aggregation O Security O VLAN O External ISCSI Storage O Link Control O Serial Over LAN O VSAN	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 Centrol Ethernet Network Control Ethernet Network Group Ethernet Sci 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 LANP Link Aggregation Link Control 	 Network ClDR 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 Systog System QoS Thermal Trusted Certificate Authorities vCenter Virtual Machine Infra Config Virtual Machine Instance Type Virtual Media VILAN VSAN

Sélection de stratégie

3. Choisissez l'organisation et choisissez un nom, puis cliquez sur Suivant.

Create	
oreate	
General	General
Constan	Add a name, description, and tag for the policy.
2 Policy Details	Organization -
	default-org ~
	Name *
	MM-Syslog-Policy O
	Set Taos
	Enter a tag in the key-value format.
	Usecription
	0/1024
,	
<	Cancer

Configurer l'organisation et le nom

4. Sélectionnez le niveau de gravité minimum souhaité pour la journalisation locale. Les niveaux de gravité peuvent être référencés dans la <u>RFC 5424</u>.

Policies > Syslog Create				
General Policy Details	Policy Details Add policy details.		All Platforms UCS Server (Standalone)	UCS Server (FI-Attisched) UCS Domain
	Local Logging			
	Minimum Severity to Report * Debug Warning Re Emergency Alert Critical Error Notice Informational Debug)		Enable Enable
	Cancel			Back

Sélectionnez le niveau de gravité minimal à signaler pour la journalisation locale

5. Sélectionnez le niveau de gravité minimum souhaité pour la journalisation à distance et les paramètres requis. Il s'agit de l'adresse IP ou du nom d'hôte du ou des serveurs distants, du numéro de port et du protocole de port (TCP ou UDP).

Remarque : Cet exemple utilise le paramètre par défaut UDP port 514. Bien que le numéro de port puisse être modifié, cela ne s'applique qu'aux serveurs. Les interconnexions de fabric utilisent le port par défaut 514 par conception.

Pathalana a Anatan			
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 * ()
	[192.0.2.2 ③	514	UDP ~
		1 - 655	15
	Minimum Severity To Report * ①		
	Debug		
	- Syslog Server 2		Contra
	Hostname/IP Address* ①	Port* ①	Protocol • ①
	0.0.0.	514	
		1-655	5
<	Cancel		Back Create

Configurer les paramètres de journalisation à distance

- 6. Cliquez sur Create.
- 7. Attribuez la stratégie aux périphériques souhaités.

Interconnexions de fabric

- 1. Accédez au profil de domaine, cliquez sur Edit, puis sur Next jusqu'à l'étape 4 de la configuration du domaine UCS.
- 2. Sous Management > Syslog, sélectionnez la politique Syslog souhaitée.

6 UCC Demain Drefiles		
Edit UCS Domain Profile (IM	1M-6536)	
General UCS Domain Assignment	UCS Domain Configuration Select the compute and management policies to be associated with the Fabric Interconnect.	
VLAN & VSAN Configuration	A Management 2 of 6 Policies Configured	
Ports Configuration		
UCS Domain Configuration	NTP	Select Policy
6 Summary	Syslog	Ê │ ⊘ │ ⊕ │ ○ IMM-Syslog
	Network Connectivity	Select Policy
	SNMP	Select Policy
	LDAP	⊞ Ø ⊕ LDAP-IMM
	Certificate Management	
	V Network 2 of 2 Policies Configured	
<	Close	Back

Sélectionnez la stratégie Syslog sur un profil de domaine Fabric Interconnect

3. Cliquez sur Next, puis sur Deploy. Le déploiement de cette stratégie n'est pas perturbateur.

Serveurs

- 1. Accédez au profil de serveur, cliquez sur Edit, puis passez à Next jusqu'à l'étape 4 Management Configuration.
- 2. Sélectionnez la politique Syslog.

← 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	● ipmi_testing 📶
5 Storage Configuration	Local User	● ipmi_user 👔
6 Network Configuration	Serial Over LAN	
C Summary	SNMP	
() Summary	Syslog	× 👁 🖉 🛛 IMM-Syslog 📶
	Virtual KVM	● KVM_IMM
<	Close	Back

Choisir la stratégie Syslog sur un profil de service de serveur

3. Continuez jusqu'à la dernière étape et Déployez.

Vérifier

À ce stade, les messages Syslog doivent être consignés sur le ou les serveurs distants Syslog. Dans cet exemple, le serveur Syslog a été déployé sur un serveur Linux avec la bibliothèque rsyslog.

Remarque : La vérification de la journalisation des messages Syslog peut varier en fonction du serveur Syslog distant utilisé.

Vérifiez que les messages Syslog Fabric Interconnects ont été consignés sur le serveur distant :

[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

Vérifiez que les messages Syslog des serveurs ont été consignés sur le serveur distant :

[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

Dépannage

Une capture de paquets peut être effectuée sur les interconnexions de fabric pour confirmer que les paquets Syslog ont été transférés correctement. Modifiez le niveau de gravité minimum à rapporter au débogage. Assurez-vous que les rapports Syslog contiennent autant d'informations que possible.

À partir de l'interface de ligne de commande, lancez une capture de paquets sur le port de gestion et filtrez par port 514 (port Syslog) :

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

Dans cet exemple, un port de serveur sur Fabric Interconnect A a été mis à l'écart pour générer du trafic Syslog.

- 1. Accédez à Fabric Interconnects > Inventory.
- 2. Cochez la case correspondant au port souhaité, ouvrez le menu de sélection à droite et choisissez disable.

← Fabric Interconnects			
FI-6536 FI-A (0 Critical)			Actions ~
General Inventory Conne	ections UCS Domain Profile	Topology Metrics	
	Ports & Port Channels		
Fan Modules	Ethernet FC Ethernet Port C	annels FC Port Channels	
PSUs	14 T2 24 T4 34 T6	7a VE BA VIO 11A VIZ 13A VI4 15A V16 17A VIE 18A V20 21A V22 23A V24 25A V26 27A V28 28A V30 31	A ¥12 23A ¥34 25A ¥36)
Local Storage			
Traffic Mirroring (SPAN)	•••• •••		
		Fhemet Linix Port Chan	el Server Unconfigured
	Q Search	▼ Filters 35 results	🖄 Export
	Name MAC	t Role t 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 -	

Arrêter une interface sur une interconnexion de fabric pour générer du trafic syslog à des fins de test

3. La console de Fabric Interconnect doit capturer le paquet Syslog :

<#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. Le message doit être connecté à votre serveur distant :

```
[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)
```

Le même test peut être exécuté sur les serveurs :

Remarque : Cette procédure ne fonctionne que pour les serveurs avec une configuration hors bande sur leur politique d'accès IMC. Si Inband est en cours d'utilisation, effectuez plutôt la capture de paquets sur le serveur Syslog distant, ou contactez le TAC pour l'effectuer avec les commandes debug internes.

← UCS Server Profiles UCSC-C220M5-IMM								Actions ~
General Server Inventory Connectivity								
Details	Configuration					IMC Access Deta	nils	
Status	General Identifiers vNICs / vHBAs					General		
		All Compute	Management	Network	Storage	Name IMC-CSeries		
UCSC-C220M5-IMM	Boot Order MXSVLAB_BootLocal			Organization				
User Label	IMC Access Policy			IN	MC-CSeries 🗐	default-org		
-	IPMI Over LAN			ij	pmi_testing 🗐	Policy Details		
Target Platform	LAN Connectivity			IM	IM-LAN-SV 🗐	In-Band Configurat	tion	
Template Name	Local User				ipmi_user 🗐	Enabled No		
	Syslog			I	MM-Syslog 🗐			
Last Update a few seconds ago	Virtual KVM				KVM_IMM 🗐	Out-Of-Band Confi	guration	
						Enabled Yes		

Vérifier la configuration de la stratégie d'accès IMC

Dans cet exemple, l'indicateur LED d'un serveur intégré C220 M5 a été activé. Cela ne nécessite pas de temps d'arrêt.

 Vérifiez quel Fabric Interconnect envoie le trafic hors bande pour votre serveur. L'adresse IP du serveur est 192.0.2.5, de sorte que Fabric Interconnect A transfère son trafic de gestion (« route secondaire » signifie que Fabric Interconnect agit comme un proxy pour le trafic de gestion du serveur) :

```
<#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. Démarrez une capture de paquets sur l'interconnexion de fabric appropriée :

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

3. Accédez à Serveurs > Actions > Système et choisissez Activer le localisateur :

FI-6536-1 Ocritical				Act	tions \vee
General Inventory UCS Server Profile H	ICI Topology Metrics Connectivity			Power	>
			Turn On Locator	System	
Details	Properties			Profile	
			Reset vKVM	VMware	
Health Critical	Cisco UCSC-C220-M5SX	Front Real	Lock Front Panel	Install Operating Sys	stem
			Rediscover	Upgrade Firmware	
Name FI-6536-1			Decommission	Launch vKVM	
User Label	Power On Locator LED Off	- Heal	Secure Erase	Launch Tunneled vK	VM
-			Certificate >	Start Alarm Suppres	sion
UCS Server Profile	CPUs	CPU Capacity (GHz)	Reboot Management Controller	Open TAC Case	
UCSC-C220M5-IMM	Z Threads	12.8		Set License Tier	
UCS Server Profile Status	56		Reset Memory Errors	Collect Tech Suppor	rt Bundle
Management IP	CPU Cores	Adapters	Set Asset Tag	IPM	
	28		Set User Label		
Serial	CPU Cores Enabled	UUID	Disable Tunneled vKVM		
	20 Memory Canacity (GiB)		Download System Event Log		01
Mac Address	256.0		Clear System Event Log		01
PID					
UCSC-C220-M5SX					
Vendor Cisco Systems Inc					

Allumer le voyant de localisation d'un serveur

4. La console de Fabric Interconnect doit afficher le paquet Syslog capturé :

<#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. Le message Syslog doit être consigné dans le fichier AUDIT.log de votre serveur distant:

```
<#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:
```

Si des paquets Syslog ont été générés par UCS, mais que le serveur Syslog ne les a pas consignés :

- 1. Vérifiez que les paquets sont arrivés sur le serveur Syslog distant avec une capture de paquets.
- 2. Vérifiez la configuration de votre serveur Syslog distant (y compris, mais sans s'y limiter : configuration du port syslog et des paramètres de pare-feu).

Informations connexes

- <u>RFC 5424 Protocole Syslog</u>
- <u>Série Intersight IMM Expert Politique Syslog</u>
- <u>Centre d'aide Cisco Intersight Configuration des stratégies de profil de domaine UCS</u>
- <u>Centre d'aide Cisco Intersight Configuration des stratégies de serveur</u>

Si le serveur est configuré en intrabande sur sa politique d'accès IMC, chargez l'interpréteur de commandes de débogage CIMC et effectuez une capture de paquets sur l'interface bond0 pour les racks, ou l'interface bond0.x (où x est le VLAN) pour les lames.

```
[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
```

• Le numéro de port Syslog ne peut pas être modifié sur les interconnexions de fabric, uniquement sur les serveurs. Ceci est par conception et a été documenté sur

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.