Configuración y verificación de Syslog en el modo administrado de UCS Intersight

Contenido

ntroducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Fabric Interconnects
Servidores
<u>/erificación</u>
Troubleshoot
nformación Relacionada

Introducción

Este documento describe el proceso para configurar y verificar el protocolo Syslog en los dominios UCS del modo administrado de intersección.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidores de Unified Computing System (UCS)
- Modo gestionado de interacción (IMM)
- · Conceptos básicos de redes
- protocolo Syslog

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- · Software como servicio (SaaS) de Intersight
- Fabric Interconnect Cisco UCS 6536, firmware 4.3(5.240032)
- Servidor en rack C220 M5, firmware 4.3(2.240090)
- Linux 9 de Alma

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las políticas de Syslog se aplican a Fabric Interconnects y servidores. Permiten configurar el registro local y remoto.

Configurar

- 1. Vaya a Políticas > Crear nueva política.
- 2. Elija Syslog, luego haga clic en 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 Centrol Ethernet Network Croup 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 LDAP Link Aggregation Link Control 	 Network CIDR Network Configuration Network Configuration Network Configuration 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 Infra Config Virtual Machine Instance Type Virtual Media VILAN VSAN
	Cancel			Start

Selección de políticas

3. Elija la Organización y elija un nombre, luego haga clic en Siguiente.

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

Configurar organización y nombre

4. Seleccione la gravedad mínima que desee incluir en el informe para el registro local. Se puede hacer referencia a los niveles de gravedad en <u>RFC 5424</u>.

Policies > Syslog Create		
General Policy Details	Policy Details Add policy details. All Patforms UCS Server (Standalone) UCS Server (FI-Attached) UCS Do Local Logging UCS Server (Standalone) UCS Server (FI-Attached) UCS Do	omain
	 File Minimum Severity to Report* Debug Warning Ree Emergency Alert Critical Error Notice Informational Debug 	ble
	Cancel Back Crea	ate

Elija la gravedad mínima del informe para el registro local

5. Seleccione la gravedad mínima que desee incluir en el informe de registro remoto y los parámetros necesarios. Se trata de la dirección IP o el nombre de host del servidor remoto, el número de puerto y el protocolo de puerto (TCP o UDP).

Nota: En este ejemplo se utiliza el valor predeterminado UDP port 514. Aunque el número de puerto se puede cambiar, esto sólo se aplica a los servidores. Los Fabric

Niterconnects utilizan el puerto predeterminado 514 por diseño.

General	Policy Details		
Daliay Datalia	Add policy details.		
		All Platforms	UCS Server (Standalone) UCS Server (FI-Attached) UCS Domain
	Local Logging		
	+ File		
	Demote Longing		
	Remote Logging		
	 Syslog Server 1 		Enable
	Hostname/IP Address * ①	Port* ()	Protocol * ①
	[192.0.2.2 🛞]	514) UDP ~
		1 - 655	5
	Minimum Severity To Report * ①		
	Debug		
			-
	- Sysiog Server 2		Enable
	Hostname/IP Address * ①	Port* ①	Protocol * ()
	0.0.0.0 🛞	514	
		1 - 655	5
<	Cancel		Back

Configurar parámetros de registro remoto

- 6. Haga clic en Crear.
- 7. Asigne la directiva a los dispositivos deseados.

Fabric Interconnects

- 1. Vaya al Perfil de dominio, haga clic en Editar y, a continuación, haga clic en Siguiente hasta el paso 4 de Configuración de dominio UCS.
- 2. En Management > Syslog, elija la política de Syslog que desee.

6 LICS Domain Profiles		
Edit UCS Domain Profile (IM	1M-6536)	
	·	
General	UCS Domain Configuration	
UCS Domain Assignment	Select the compute and management policies to be associated with the Fabric Interconnect.	
- UCS Domain Assignment	Show Attached Policies (4)	
VLAN & VSAN Configuration	A Management 2 of 6 Policies Configured	
Ports Configuration		
S UCS Domain Configuration	NTP	Select Policy
6 Summary	Syslog	≅ ⊘ ⊕ ○ IMM-Syslog
	Network Connectivity	Select Policy
	SNMP	Select Policy
	LDAP	□ Ø Φ O LDAP-IMM
	Certificate Management	🖹 🗷 👁 • IMM-LDAPS-Cert
	V Network 2 of 2 Policies Configured	
,		
· · · · · · · · · · · · · · · · · · ·	Close	Back

Elija la política syslog en un perfil de dominio de Fabric Interconnect

3. Haga clic en Siguiente y después en Implementar. La implementación de esta política no es perjudicial.

Servidores

- 1. Navegue hasta el perfil de servidor, haga clic en Edit, luego vaya a Next hasta el paso 4 Management Configuration.
- 2. Elija la política Syslog.

← UCS Server Profiles Edit UCS Server Profile (UC)	SC-C220M5-IMM)	
	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 🗍
	Virtual KVM	●KVM_IMM @
<	Close	Back

Elija la política syslog en un perfil de servicio de servidor

3. Continúe hasta el último paso e implemente.

Verificación

En este momento, los mensajes de Syslog deben registrarse en los servidores remotos de Syslog. Para este ejemplo, el servidor Syslog se implementó en un servidor Linux con la biblioteca rsyslog.

Nota: La verificación del registro de mensajes de Syslog puede variar en función del servidor Syslog remoto en uso.

Confirme que los mensajes de Syslog de Fabric Interconnects fueron registrados en el servidor remoto:

[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

Confirme que los mensajes Syslog de servidores fueron registrados en el servidor remoto:

[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

Se puede realizar una captura de paquetes en las Fabric Interconnects para confirmar si los paquetes Syslog se reenviaron correctamente. Cambie la gravedad mínima del informe a debug. Asegúrese de que Syslog informa de la mayor cantidad de información posible.

Desde la interfaz de línea de comandos, inicie una captura de paquetes en el puerto de administración y filtre por el puerto 514 (puerto Syslog):

<#root>

```
FI-6536-A# connect nxos
FI-6536-A(nx-os)# ethanalyzer
local interface mgmt
capture-filter "
```

```
" limit-captured-frames 0
Capturing on mgmt0
```

port 514

En este ejemplo, un puerto de servidor en Fabric Interconnect A fue inestable para generar el tráfico de Syslog.

- 1. Vaya a Fabric Interconnects > Inventory.
- 2. Haga clic en la casilla de verificación del puerto deseado, abra el menú de puntos suspensivos a la derecha y elija disable.

← Fabric Interconnects						
FI-6536 FI-A O Critical						Actions ~
General Inventory Conne	ections UCS Domain Prof	ile Topology Me	trics			
	Ports & Port Channels					
Fan Modules	Ethernet FC Ethernet	Port Channels FC Port	Channels			
PSUs	14 T2 34 T4 5	A V6 7A V8 9A V10	114 V12 134 V14 154	₩16 17A ₩18 18A ₩20 21A ₩22 23A ₩24 25A ₩26	27 A ¥28 29 A ¥30 31 A ¥32	23A ¥34 25A ¥26
Local Storage						
Traffic Mirroring (SPAN)		•				
					Ethernet Uplink Port Channel	Server Ounconfigured
	Q Search		rs 35 results			🛆 Export
	Name	MAC : Role		Peer		<u>©</u>
	Port 1/1	Ether	net Uplink Port Channel M			
	Port 1/2	Ether	net Uplink Port Channel M			
		Serve				
	Port 1/4	Unco	nfigured			Disable
	Port 1/5	Unco	nfigured			Reset
	Port 1/6	Unco	nfigured			
	Port 1/7	Unco	nfigured			
	Port 1/8	Unco	nfigured			

Cierre una interfaz en una Fabric Interconnect para generar tráfico de syslog para realizar pruebas

3. La consola en Fabric Interconnect debe capturar el paquete 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. El mensaje debe estar registrado en su servidor remoto:

<#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)
```

La misma prueba se puede ejecutar en los servidores:

Nota: Este procedimiento sólo funciona para servidores con configuración fuera de banda en su política de acceso IMC. Si Inband está en uso, realice la captura de paquetes en el servidor Syslog remoto en su lugar, o comuníquese con el TAC para realizarla con los comandos de depuración internos.

← UCS Server Profiles UCSC-C220M5-IMM			Actions ~
General Server Inventory Connectivity			
Details	Configuration		■ IMC Access Details
Status	General Identifiers vNICs / vHBAs		General
Name	All Compute	Management Network Storage	Name IMC-CSeries
UCSC-C220M5-IMM	Boot Order ©	MXSVLAB_BootLocal	Drganization
User Label	IMC Access Policy	IMC-CSeries	default-org
•	IPMI Over LAN	ipmi_testing (Policy Details
Target Platform UCS Server (FI-Attached)	LAN Connectivity	IMM-LAN-SV	In-Band Configuration
Template Name	Local User	ipmi_user (Enabled No
	Syslog	IMM-Syslog	
Last Update a few seconds ago	Virtual KVM	KVM_IMM (
			Enabled Yes

Verifique la configuración en la política de acceso de IMC

En este ejemplo, se habilitó el localizador LED en un servidor integrado C220 M5. Esto no requiere tiempo de inactividad.

 Verifique qué Fabric Interconnect envía tráfico fuera de banda para su servidor. La IP del servidor es 192.0.2.5, por lo que Fabric Interconnect A reenvía su tráfico de gestión (la "ruta secundaria" significa que Fabric Interconnect actúa como un proxy para el tráfico de gestión del servidor):

```
<#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,
```

<pre>IP address: 192.0.2.3, IP subnet: 192.0.2.0/24 route-preference: 0, tag: IP address:</pre>	0
192.0.2.5	
, IP subnet: 192.0.2.0/24	
secondary route-preference	
: 0, tag: 0	

2. Inicie una captura de paquetes en el Fabric Interconnect apropiado:

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

3. Navegue hasta Servidores > Acciones > Sistema y elija Activar localizador:

FI-6536-1 (Critical					Actions ~
General Inventory UCS Server Profile H	ICL Topology Metrics Connectivity			Power	>
			Turn On Locator	System	
Details	Properties			Profile	
			Reset vKVM	VMware	>
Health Oritical	Cisco UCSC-C220-M5SX	Front Rea	Lock Front Panel	Install Operatin	g System
			Rediscover	Upgrade Firmw	are
Name FI-6536-1		2 180 :: I	Decommission	Launch vKVM	
User Label	Power On Locator LED Off	C Hea	Secure Erase	Launch Tunnele	ed vKVM
			Certificate >	Start Alarm Sup	pression
UCS Server Profile	CPUs	CPU Capacity (GHz)	Reboot Management Controller	Open TAC Case	
UCSC-C220M5-IMM	Z Throade	12.0		Set License Tie	e
OCS Server Profile Status	56		Reset Memory Errors	Collect Tech Su	pport Bundle
Management IP	CPU Cores	Adapters	Set Asset Tag	IPM	
	28		Set User Label		
Serial	CPU Cores Enabled	UUID	Disable Tunneled vKVM		
	Nemon Canacity (CiR)		Download System Event Log		011 @11
Mac Address	256.0		Clear System Event Log		01
PID					
UCSC-C220-M5SX					
Vendor					
Cisco Systems inc					

Activar el localizador LED en un servidor

4. La consola en Fabric Interconnect debe mostrar el paquete Syslog capturado:

<#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. El mensaje Syslog debe estar registrado en el archivo AUDIT.log del servidor remoto:

```
<#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 los paquetes de Syslog fueron generados por UCS, pero el servidor Syslog no los registró:

- 1. Confirme que los paquetes llegaron al servidor Syslog remoto con una captura de paquetes.
- 2. Verifique la configuración de su servidor Syslog remoto (incluyendo pero no limitado a: configuración del puerto syslog y del firewall).

Información Relacionada

- <u>RFC 5424: protocolo Syslog</u>
- Intersight IMM Expert Series: política de Syslog
- <u>Centro de ayuda de Cisco Intersight: configuración de políticas de perfiles de dominio de</u> <u>UCS</u>
- <u>Centro de ayuda de Cisco Intersight: configuración de políticas de servidor</u>

Si el servidor tiene Inband configurado en su política de acceso de IMC, cargue el shell de depuración de CIMC y realice una captura de paquetes en la interfaz bond0 para los racks, o la interfaz bond0.x (donde x es la VLAN) para los servidores blade.

```
[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
```

 El número de puerto de Syslog no se puede cambiar en Fabric Interconnects, sólo en servidores. Esto se ha diseñado y se ha documentado en

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).