# Configurar e verificar o Syslog no modo gerenciado UCS Intersight

Contents
Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Interconexões em malha
Servidores
Verificar
Troubleshooting
Informações Relacionadas

# Introdução

Este documento descreve o processo para configurar e verificar o protocolo Syslog em Domínios UCS do Modo Gerenciado de Intersight.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Servidores Unified Computing System (UCS)
- IMM (Intersight Managed Mode, modo gerenciado de supervisão)
- · Conceitos básicos de rede
- protocolo de Syslog

## **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software:

- Software como serviço (SaaS) da Intersight
- Interconexão em malha Cisco UCS 6536, firmware 4.3(5.240032)
- Servidor rack C220 M5, firmware 4.3(2.240090)
- Linux Alma 9

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

As políticas de syslog são aplicáveis para Interconexões em malha e servidores. Permitem a configuração de registro local e remoto.

# Configurar

- 1. Navegue até Policies > Create new policy.
- 2. Escolha Syslog e clique em Iniciar.

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

Seleção de política

3. Escolha a Organização, escolha um nome e clique em Avançar.

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

Configurar organização e nome

4. Escolha a severidade mínima desejada a ser relatada para o Log Local. Os níveis de gravidade podem ser referenciados no <u>RFC 5424</u>.

Policies > Syslog Create		
<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add policy details. Local Logging	T All Platforms UCS Server (Standalone) UCS Server (FI-Attached) UCS Domain
	<ul> <li>File</li> <li>Minimum Severity to Report*          <ul> <li>Debug</li> <li>Warning</li> </ul> </li> <li>Ree Emergency         <ul> <li>Alert</li> <li>Critical</li> <li>Error</li> <li>Notice</li> <li>Informational</li> <li>Debug</li> </ul> </li> </ul>	Enable
<	Cancel	Back Create

Escolha a severidade mínima a ser relatada para o Log Local

5. Escolha a severidade mínima desejada a ser relatada para o Log Remoto e as configurações necessárias. Esses são o endereço IP ou o nome do host do(s) servidor(es) remoto(s), o número da porta e o protocolo da porta (TCP ou UDP).

Note: Este exemplo usa a configuração padrão UDP porta 514. Embora o número da porta possa ser alterado, isso se aplica somente a Servidores. As interconexões em

💊 malha usam a porta padrão 514 por design.

Policies > Syslog Create			
General     Policy Details	Policy Details Add policy details.	∑ All Platfor	ns UCS Server (Standalone) UCS Server (Fi-Attached) UCS Domain
	Local Logging		
	+ File		
	Remote Logging		
	- Syslog Server 1		Cnable
	Hostname/IP Address* ①	Port* ①	Protocol * ①
	192.0.2.2	514	UDP ~
	Minimum Severity To Report * ①		
	Debug ~		
	- Syslog Server 2		Enable
	Hostname/IP Address • ()	Port* ()	Protocol* ()
	0.0.0.0 🛞	514	
<	Cancel		Back

Configurar parâmetros de Log Remoto

- 6. Clique em Criar.
- 7. Atribua a política aos dispositivos desejados.

#### Interconexões em malha

- 1. Navegue até o Perfil de domínio, clique em Editar e, em seguida, clique em Avançar até a etapa 4 Configuração de domínio do UCS.
- 2. Em Management > Syslog, escolha a Política de Syslog desejada.

61109	Domain Profiles									
Edit	UCS Domain Profile (IN	1M-6536)								
	<b>,</b> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	,								
$\odot$	General	UCS Domain Configuration Select the compute and management policies to be associated with the Fabric Interconnect.								
$\odot$	UCS Domain Assignment	Show Attached Policies (4)								
$\oslash$	VLAN & VSAN Configuration									
$\odot$	Ports Configuration									
5	UCS Domain Configuration	NTP	Select Policy							
6	Summary	Syslog	🖹   🇷   🕕   O IMM-Syslog							
		Network Connectivity	Select Policy							
		SNMP	Select Policy							
		LDAP								
		Certificate Management								
		V Network 2 of 2 Policies Configured								
		Close	Back							

Escolher a política de syslog em um Perfil de domínio de interconexão de estrutura

3. Clique em Avançar e em Implantar. A implantação dessa política não causa interrupções.

## Servidores

- 1. Navegue até o Server Profile, clique em Edit e vá para Next até a etapa 4 Management Configuration.
- 2. Escolha a política de 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	
7 Summary	SNMP	
() Guinnary	Syslog	×   ©   🖉   🛛 IMM-Syslog 📶
	Virtual KVM	© KVM_IMM (
<	Ciose	Back

Escolher a política de syslog em um Server Service Profile

3. Continue até a última etapa e Implantar.

## Verificar

Nesse ponto, as mensagens de Syslog devem ser registradas no(s) servidor(es) remoto(s) Syslog. Para este exemplo, o servidor Syslog foi implantado em um servidor Linux com a biblioteca rsyslog.

Note: A verificação do registro de mensagens de Syslog pode variar dependendo do servidor Syslog remoto em uso.

Confirme se as mensagens de Syslog das interconexões em malha foram registradas no 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 se as mensagens do Syslog Servers foram registradas no 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 User
```

## Troubleshooting

Uma captura de pacote pode ser executada nas interconexões de estrutura para confirmar se os pacotes Syslog foram encaminhados corretamente. Altere a severidade mínima para relatar para debug. Certifique-se de que o Syslog reporte o máximo de informações possível.

Na interface de linha de comando, inicie uma captura de pacote na porta de gerenciamento e filtre pela porta 514 (porta Syslog):

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

Neste exemplo, uma porta de servidor na Interconexão de estrutura A foi desviada para gerar tráfego Syslog.

- 1. Navegue até Interconexões de estrutura > Inventário.
- 2. Clique na caixa de seleção da porta desejada, abra o menu de reticências à direita e escolha desativar.

← Fabric Interconnects								
FI-6536 FI-A (0 critical								
General Inventory Connections UCS Domain Profile Topology Metrics								
Ports & Port Channels	Ports & Port Channels							
Fan Modules	Ethernet FC Ethernet	Port Channels FG	C Port Channels					
PSUs		A V6 7A V8 8	A ¥10 11A ¥12 13A ¥14 15A	¥16 17A ¥18 19A ¥20 21A ¥22 23A ¥24 25A	<b>V</b> 26 27 A V28 28 A V30 31A V22			
Local Storage								
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 Uplink Port Channel M					
	Port 1/2		Ethernet Uplink Port Channel M					
			Server					
	Port 1/4		Unconfigured			Disable		
	Port 1/5		Unconfigured			Reset		
	Port 1/6		Unconfigured					
	Port 1/7		Unconfigured					
	Port 1/8		Unconfigured					

Desligar uma interface em uma interconexão de estrutura para gerar tráfego de syslog para teste

#### 3. O console no Interconector de estrutura deve capturar o pacote 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. A mensagem deve ser registrada em seu servidor remoto:

```
[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)
```

O mesmo teste pode ser executado em servidores:

Note: Este procedimento funciona apenas para servidores com configuração fora de banda em sua Política de acesso IMC. Se a Inband estiver em uso, realize a captura de pacotes no Servidor Syslog remoto ou entre em contato com o TAC para executá-la com comandos debug internos.

← UCS Server Profiles UCSC-C220M5-IMM		Actions V
General Server Inventory Connectivity		
Details	Configuration	IMC Access Details
Status	General Identifiers vNICs / vHBAs	General
	All Compute Management Network Storage	Name IMC-CSeries
Name UCSC-C220M5-IMM	Boot Order Ø MXSVLAB_BootLoca	Organization
User Label	IMC Access Policy IMC-CSeries	fill 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	
		Yes

Verifique a configuração na política de acesso IMC

Neste exemplo, o localizador de LED em um servidor integrado C220 M5 foi ativado. Isso não requer tempo de inatividade.

 Verifique qual interconexão de estrutura envia tráfego fora de banda para seu servidor. O IP do servidor é 192.0.2.5, portanto a Interconexão de estrutura A encaminha seu tráfego de gerenciamento ("rota secundária" significa que a Interconexão de estrutura atua como um proxy para o tráfego de gerenciamento do 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,
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. Inicie uma captura de pacote na interconexão de estrutura apropriada:

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

3. Navegue até Servers > Actions > System e escolha Turn On Locator:

FI-6536-1 (0 cmtca)						
Canaral Invantory IICS Sarvar Brofila UCI Tanalary Matrice Connectivity						
	ice reputer ounceancy		Turn On Locator	System >		
Details	Properties			Profile >		
			Reset vKVM	VMware >		
Health O Critical	Cisco UCSC-C220-M5SX	Front Rea	Lock Front Panel	Install Operating System		
			Rediscover	Upgrade Firmware		
Name FI-6536-1			Decommission	Launch vKVM		
User Label	Power () On Locator LED Off	C Heat	Secure Erase	Launch Tunneled vKVM		
•			Certificate >	Start Alarm Suppression		
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	Threads 56		Reset Memory Errors	Collect Tech Support Bundle		
Management IP	CPU Cores	Adapters	Set Asset Tag	I PM		
	28		Set User Label			
Serial	CPU Cores Enabled	UUID	Disable Tunneled vKVM			
	28		Download System Event Log			
Mac Address	Memory Capacity (GiB) 256.0		Clear System Event Log			
PID						
UCSC-C220-M5SX						
Vendor Cisco Systems Inc						

Ligar o localizador de LED em um servidor

4. O console no Interconector de estrutura deve mostrar o pacote 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. A mensagem Syslog deve ser registrada no arquivo AUDIT.log do 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:
```

Se os pacotes Syslog foram gerados pelo UCS, mas o servidor Syslog não os registrou:

- 1. Confirme se os pacotes chegaram ao Servidor Syslog remoto com uma captura de pacotes.
- 2. Verifique a configuração do seu servidor Syslog remoto (incluindo, mas não se limitando a: porta de syslog e configurações de firewall configuradas).

## Informações Relacionadas

- <u>RFC 5424 O protocolo Syslog</u>
- Intersight IMM Expert Series Política de Syslog
- <u>Cisco Intersight Help Center Configurar políticas de perfil de domínio do UCS</u>
- <u>Cisco Intersight Help Center Configurar políticas de servidor</u>

Se o servidor tiver a Inband configurada em sua Política de acesso IMC, carregue o shell de depuração do CIMC e execute uma captura de pacote na interface bond0 para racks ou na interface bond0.x (onde x é a VLAN) para 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
```

• O número da porta Syslog não pode ser alterado em Interconexões de estrutura, somente em servidores. Isso foi projetado e documentado em

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.