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

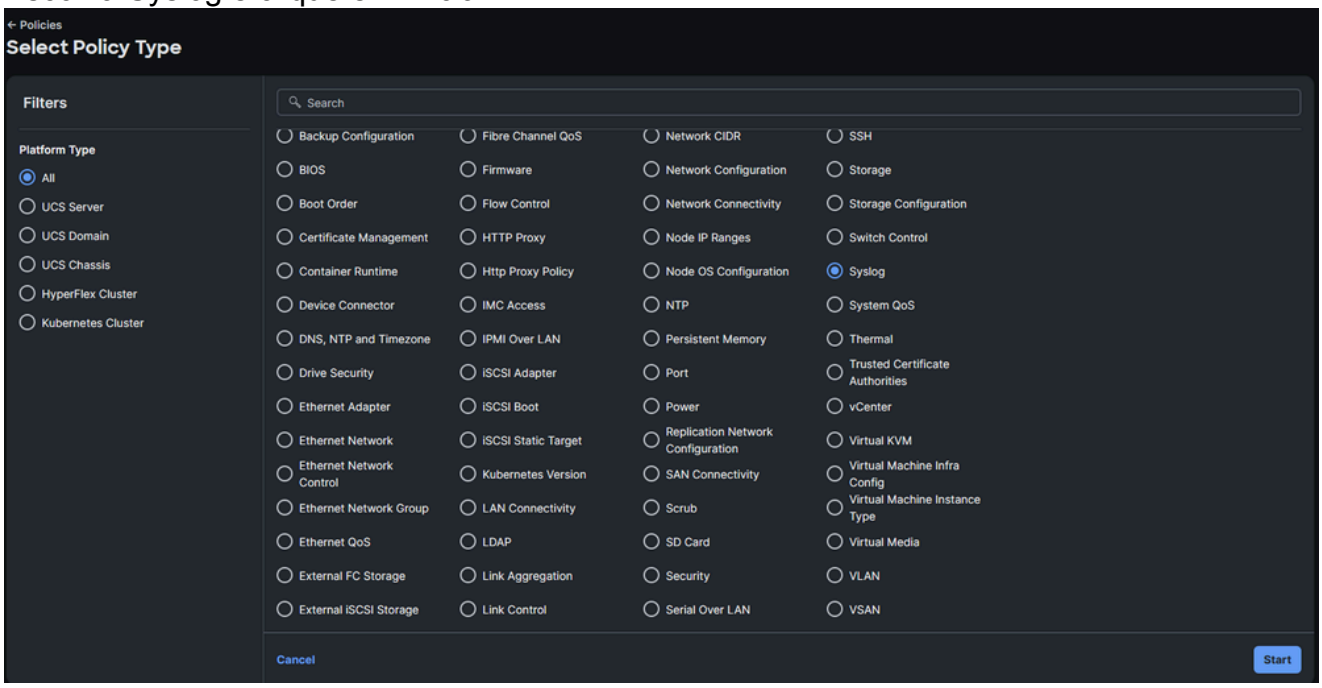
laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

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

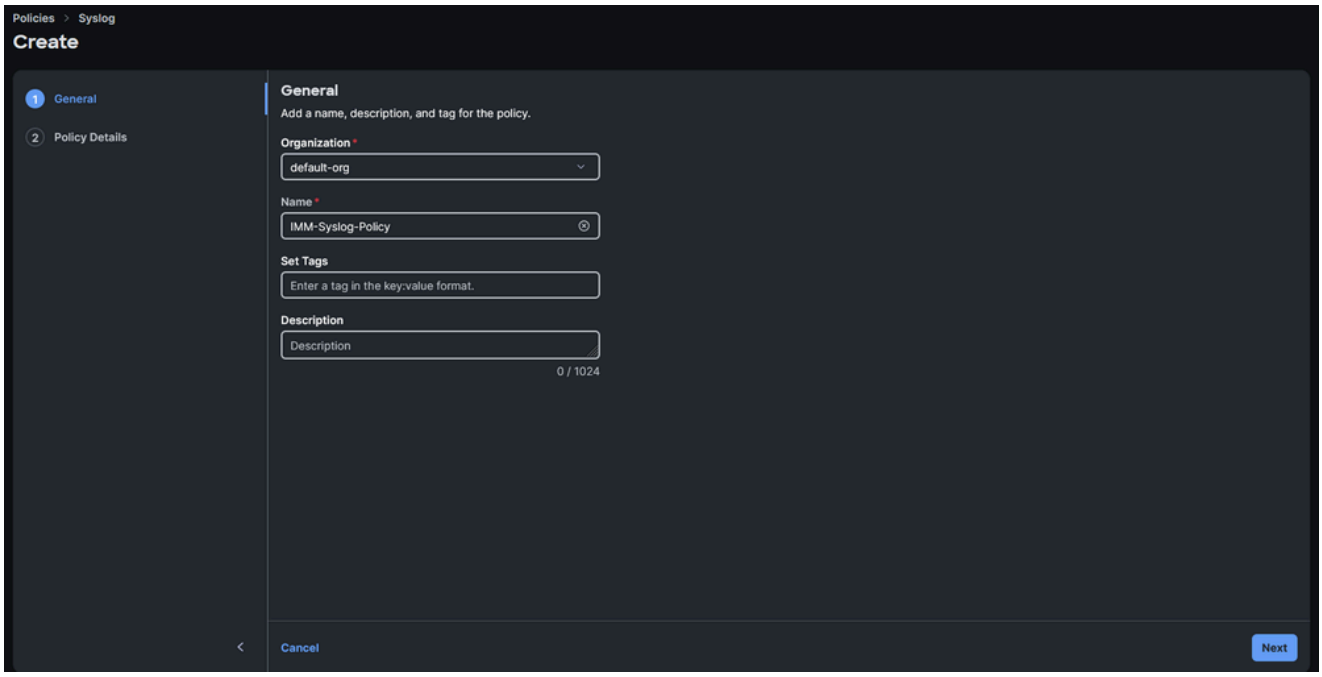
Configurar

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



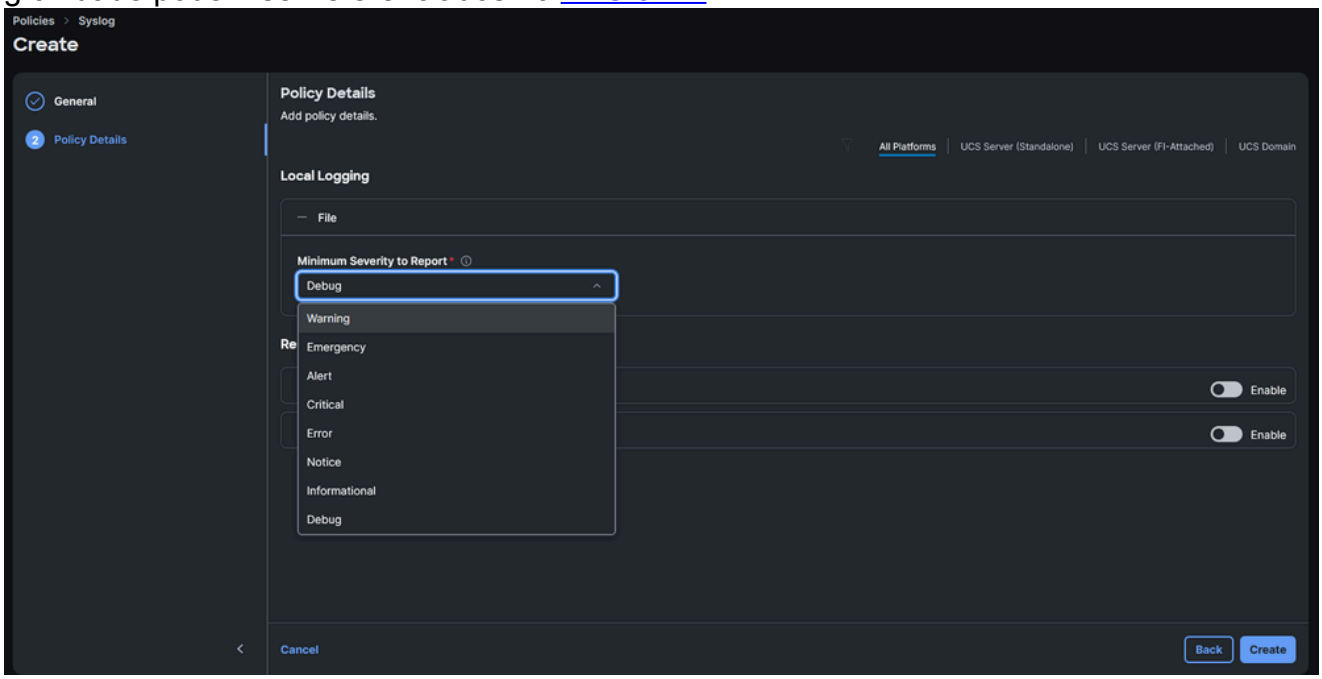
Seleção de política

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



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 RFC 5424.



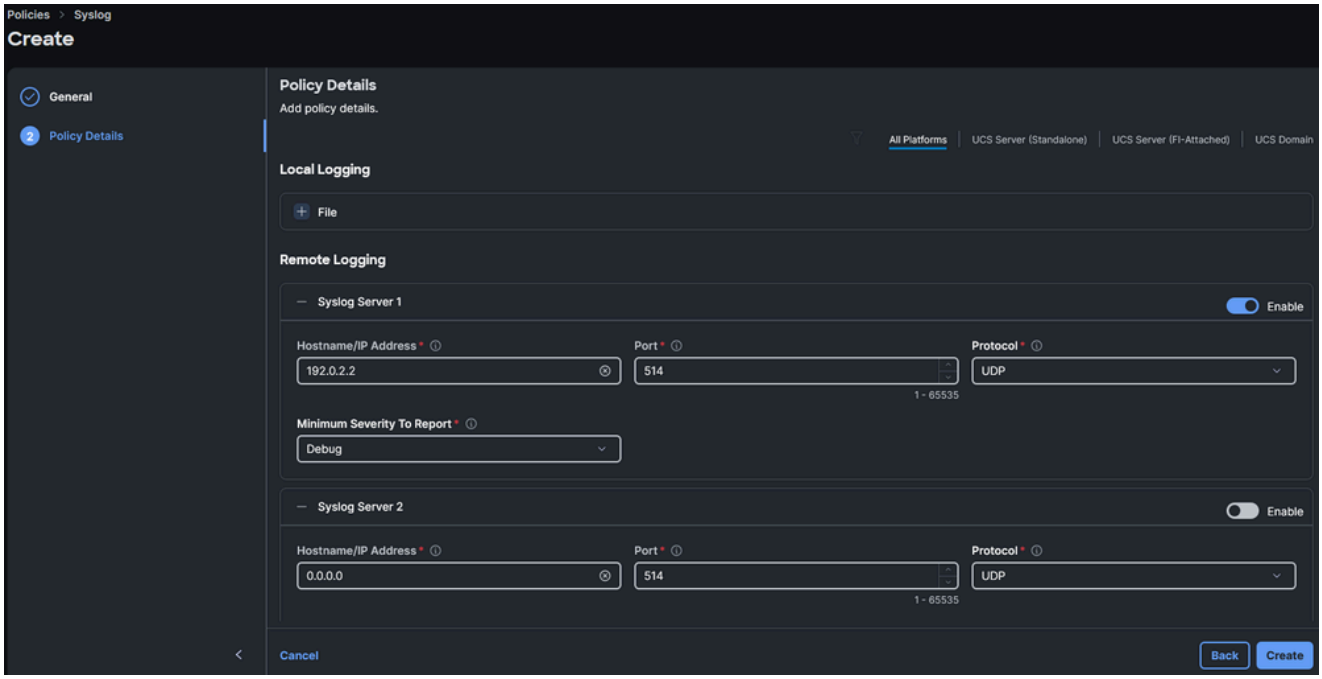
Escolha a severidade mínima a ser relatada para o Log Local

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.

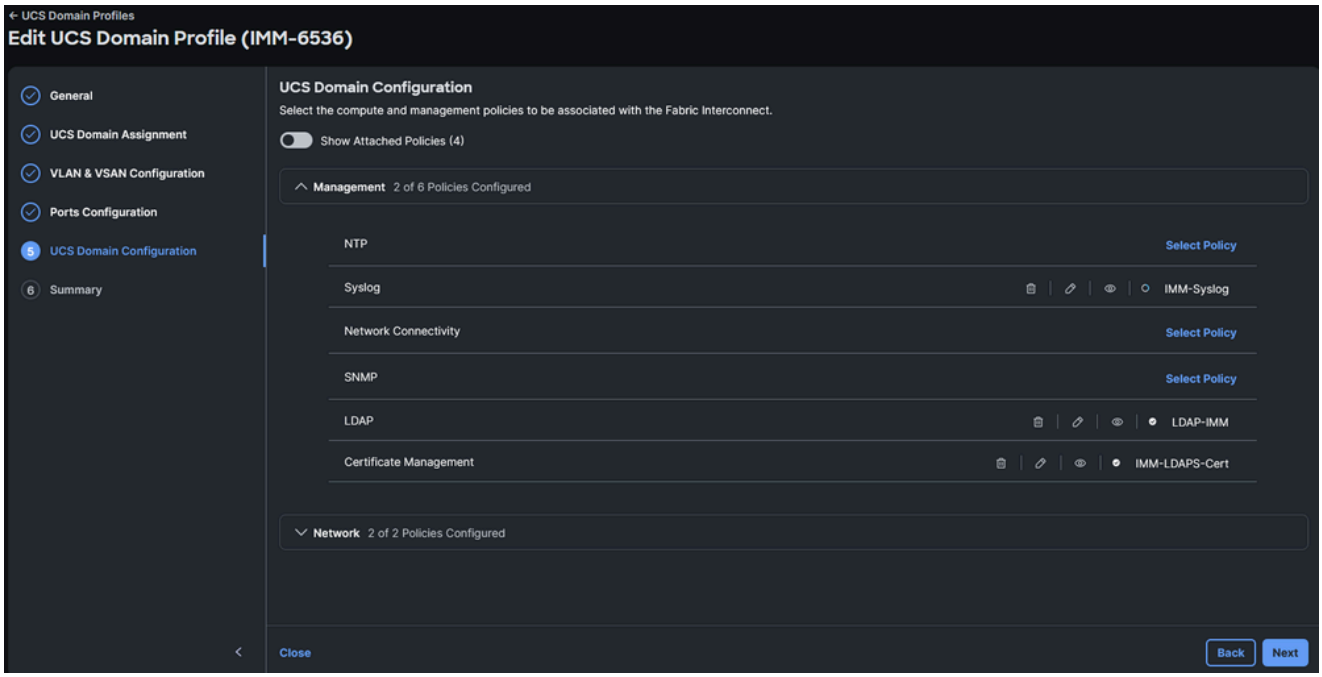


Configurar parâmetros de Log Remoto

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.

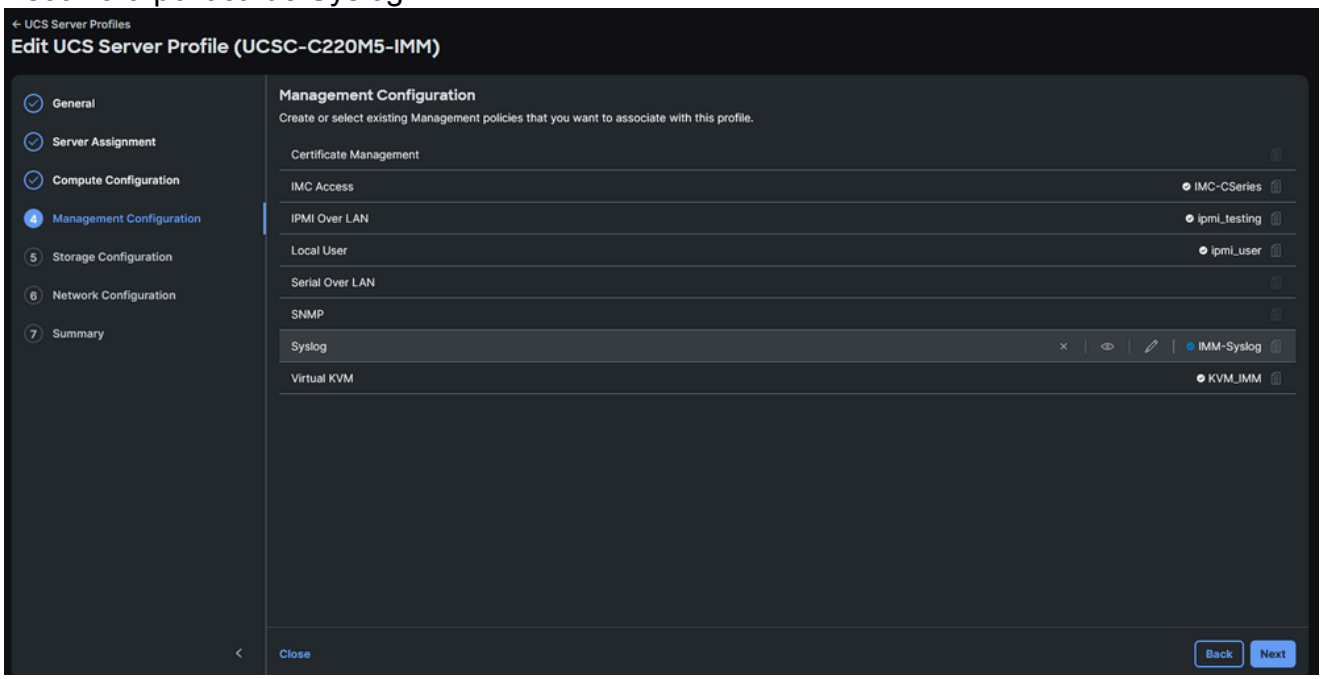


Escolher a política de syslog em um Perfil de domínio de interconexão de estrutura

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.



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 Us
```

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 "

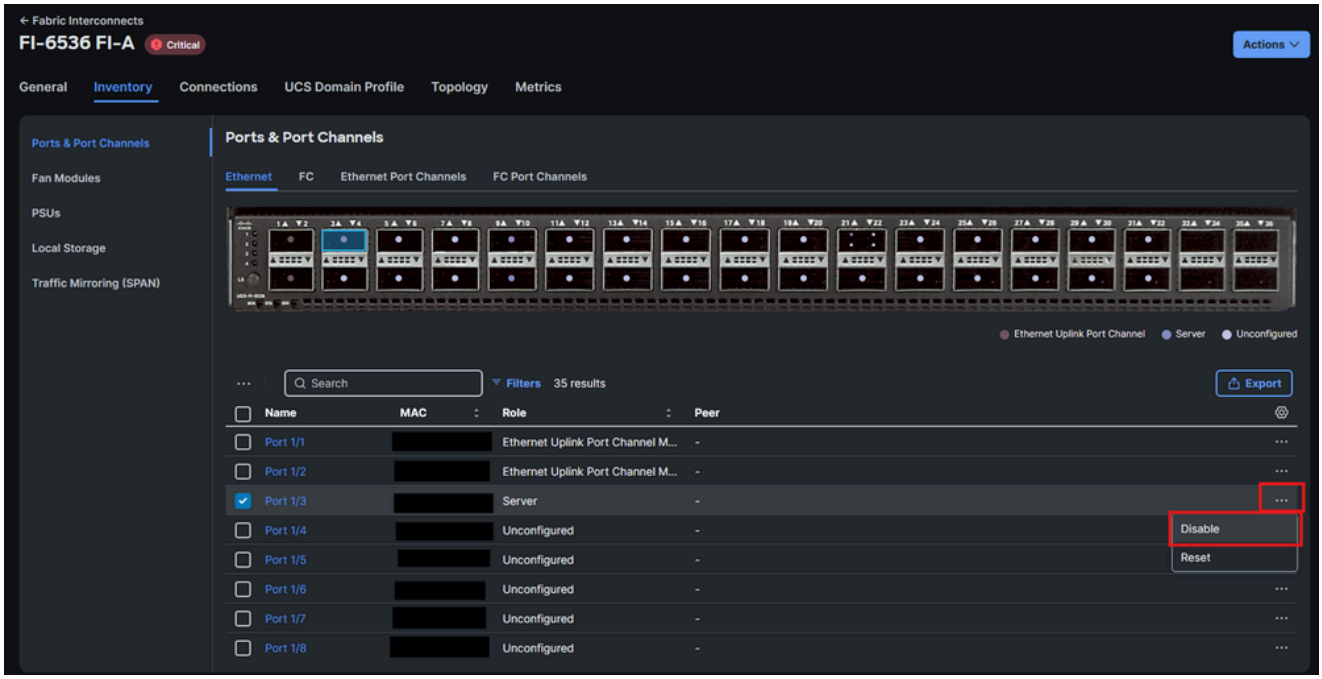
port 514

" limit-captured-frames 0

```
Capturing on mgmt0
```

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.



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>

```
[root@alma jormarqu]# tail -n 1 /var/log/remote/msg/192.0.2.3/_.log
Jan 16 17:15:03
```

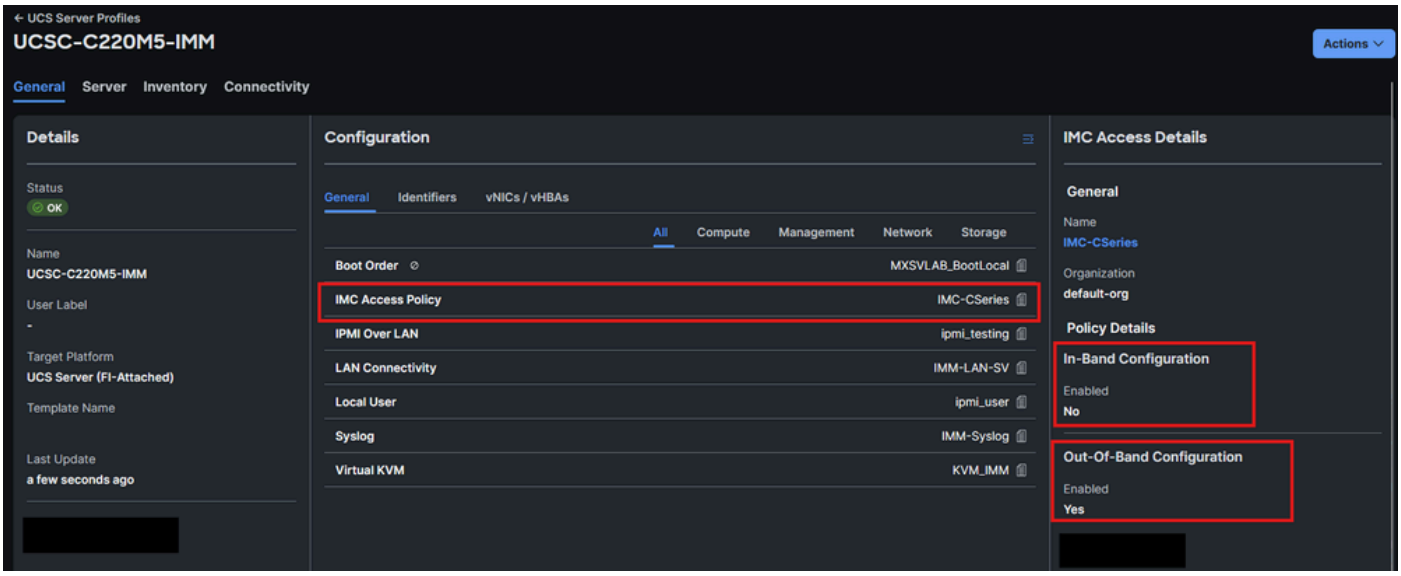
192.0.2.3

```
 : 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.



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.

1. 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

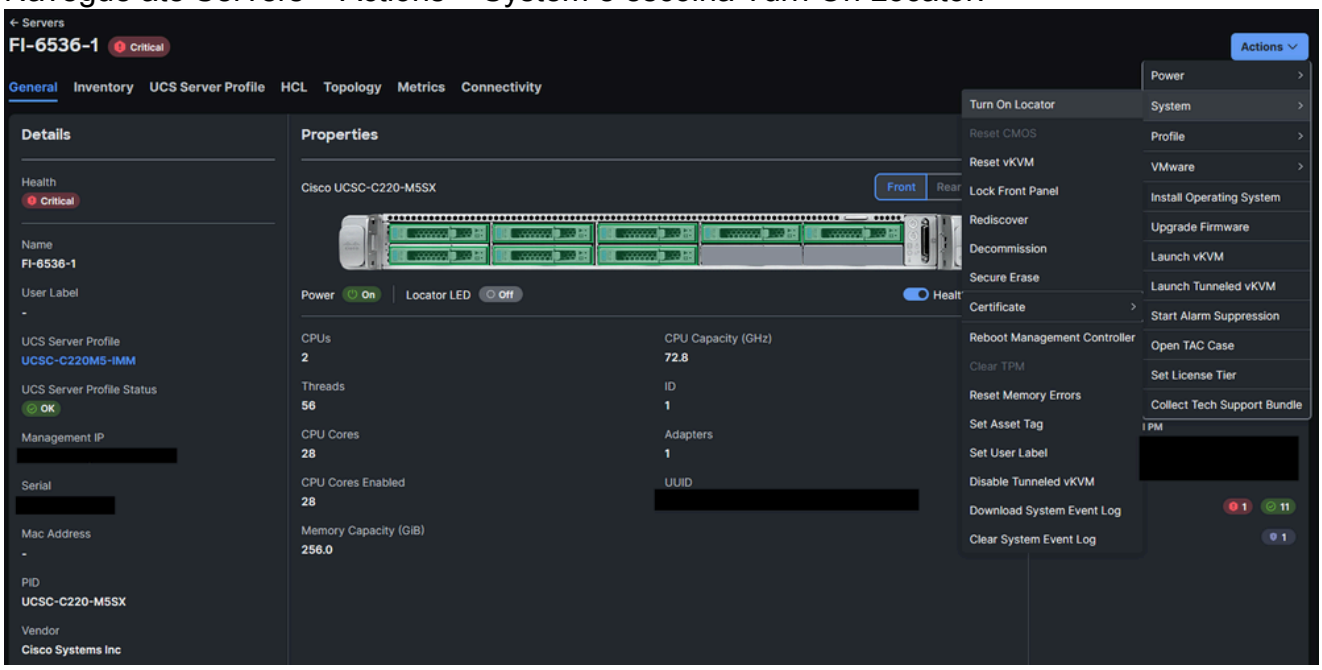
   ```
   (nx-os)# show ip interface mgmt 0

   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:



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

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

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.