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

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

- Fabric Interconnects
- Servidores

Verificación

Troubleshoot

Información 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

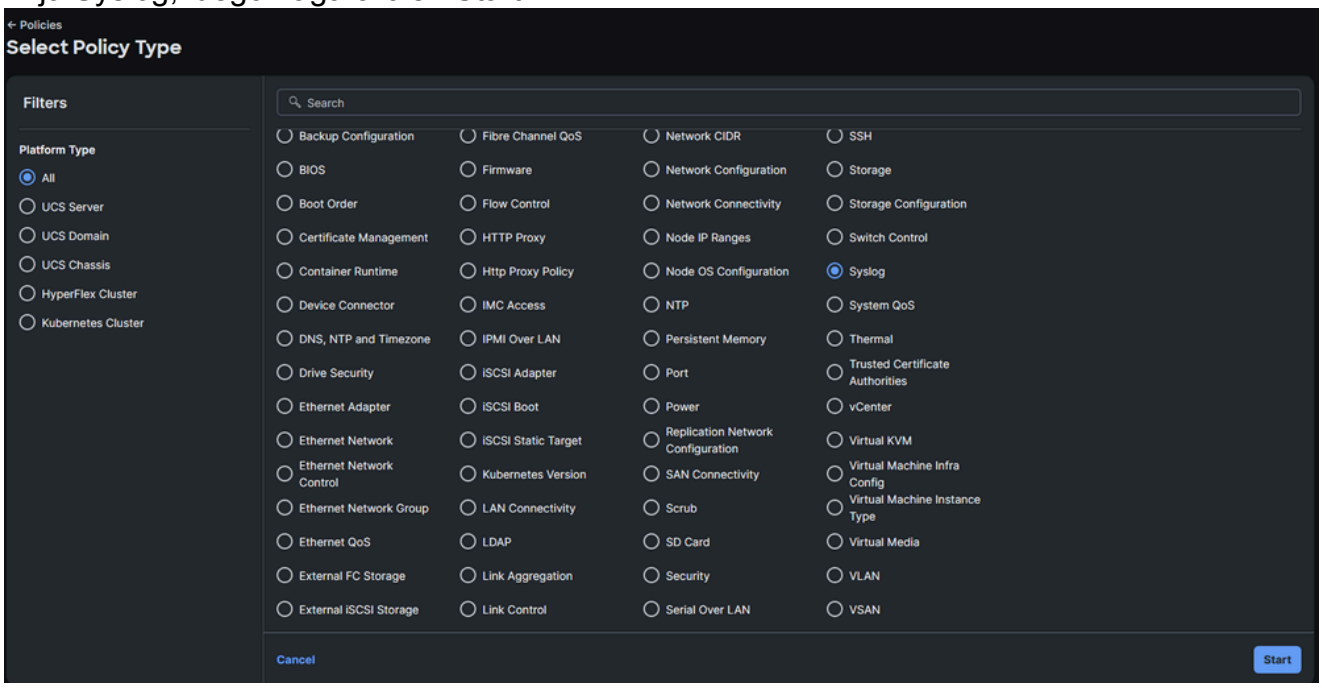
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

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

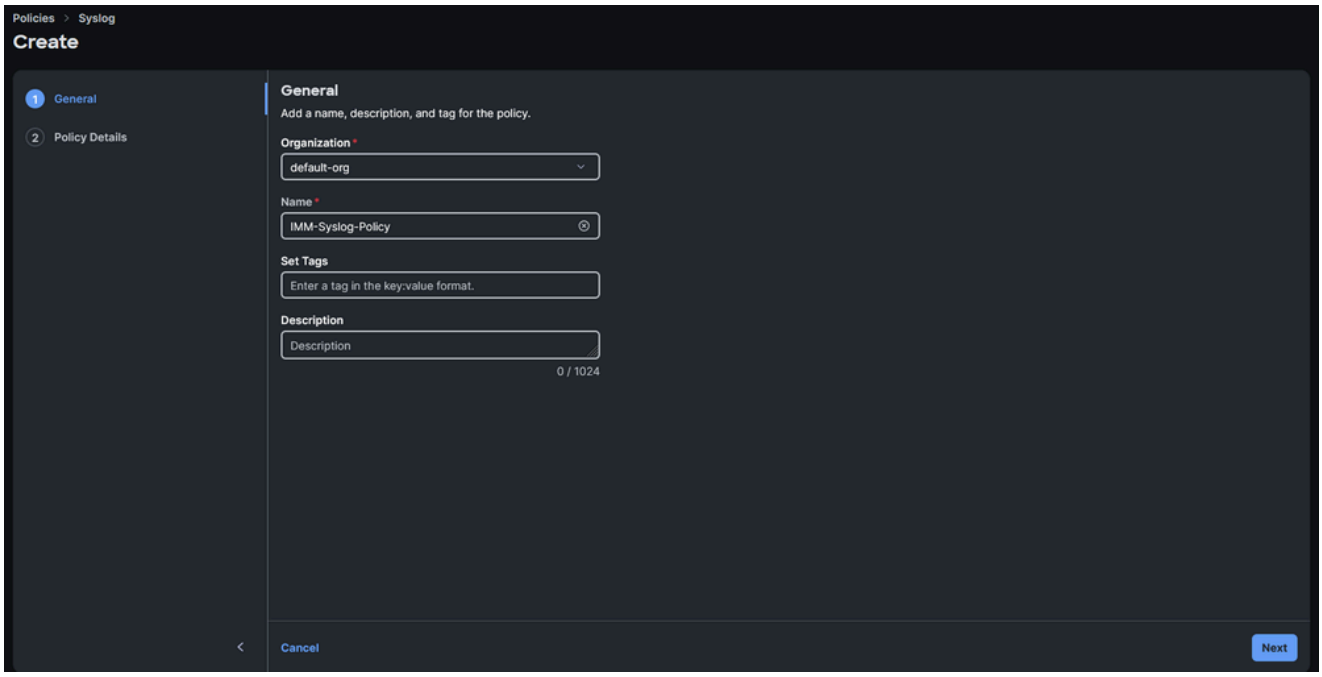
Configurar

1. Vaya a Políticas > Crear nueva política.
2. Elija Syslog, luego haga clic en Start.



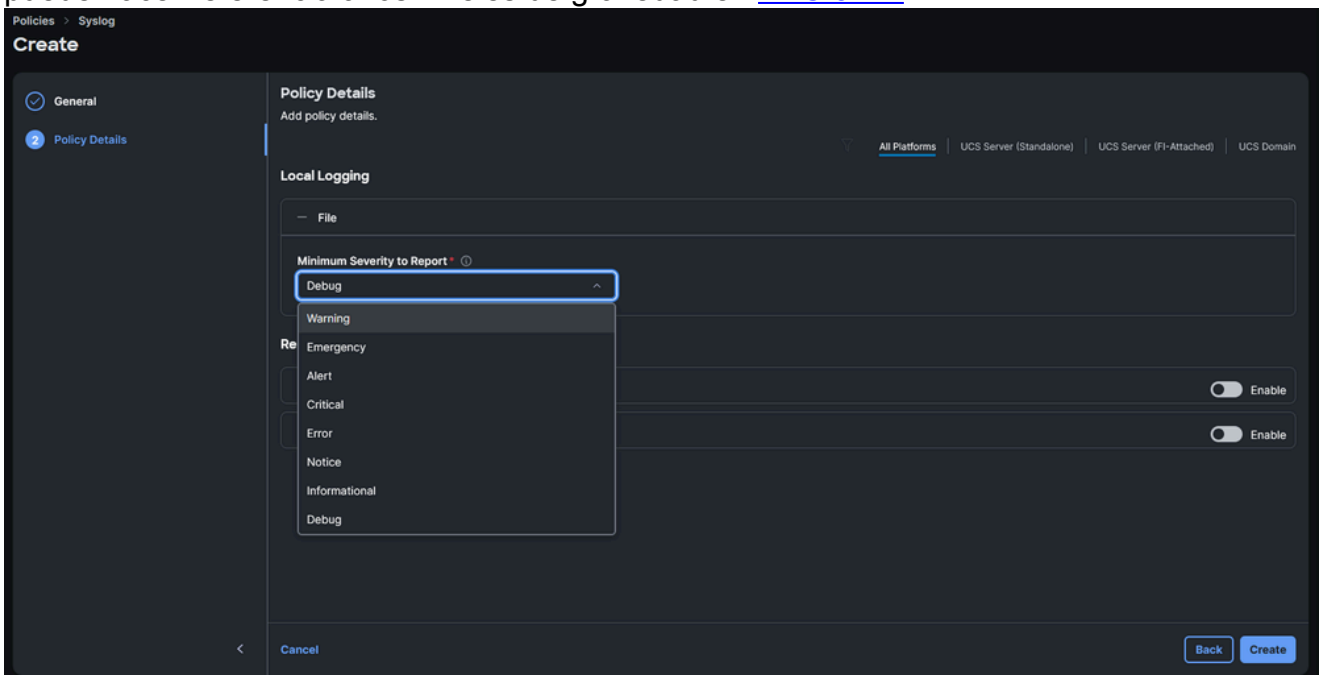
Selección de políticas

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



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 RFC 5424.



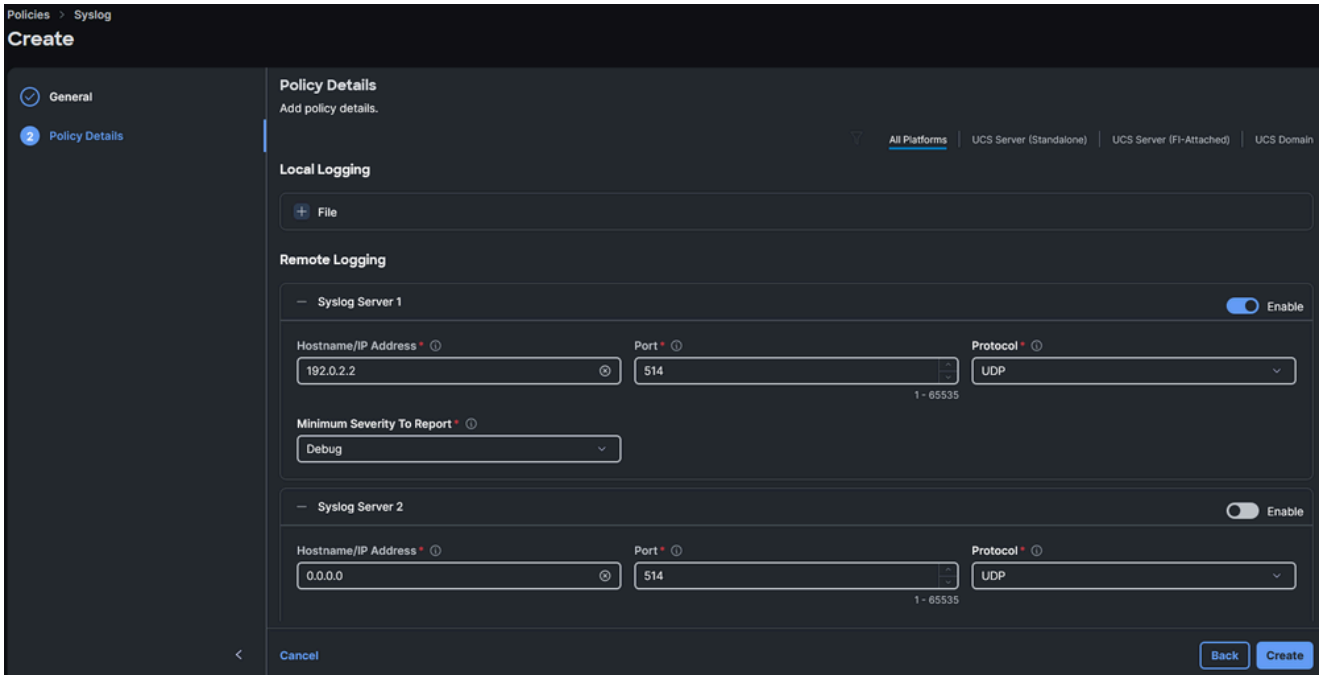
Elija la gravedad mínima del informe para el registro local

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

---

Interconnects utilizan el puerto predeterminado 514 por diseño.

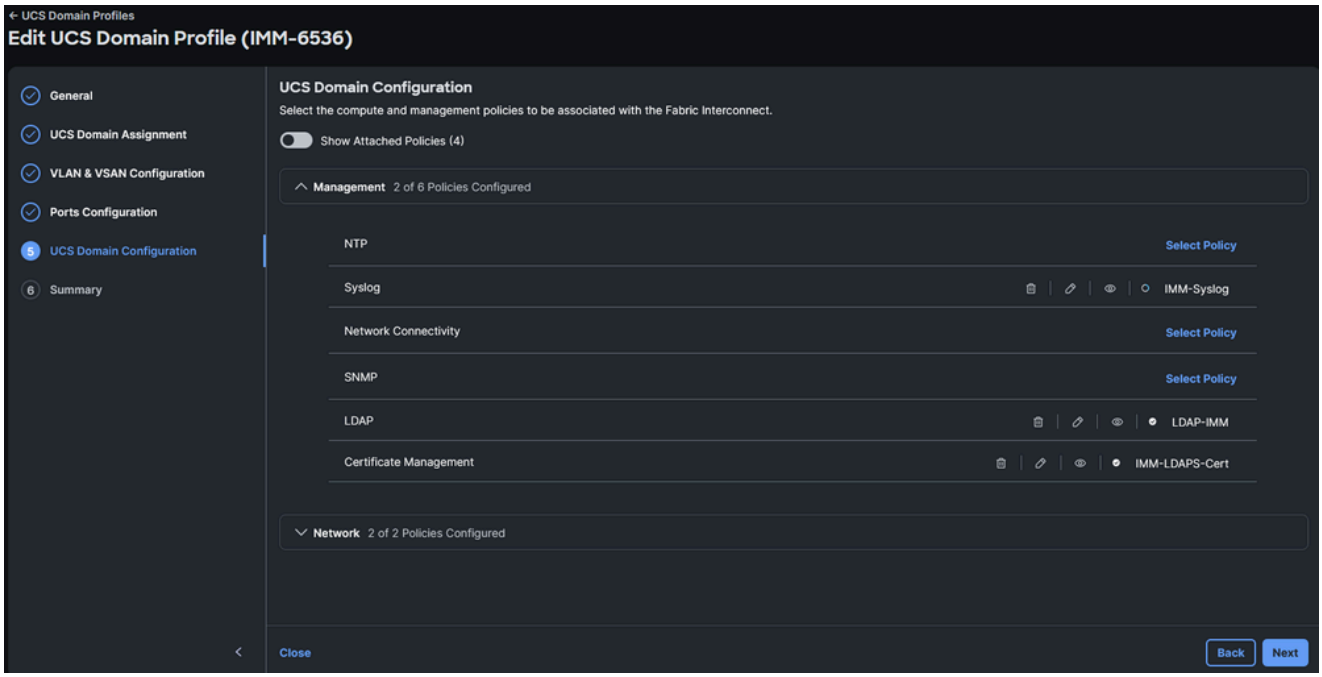


Configurar parámetros de registro remoto

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.

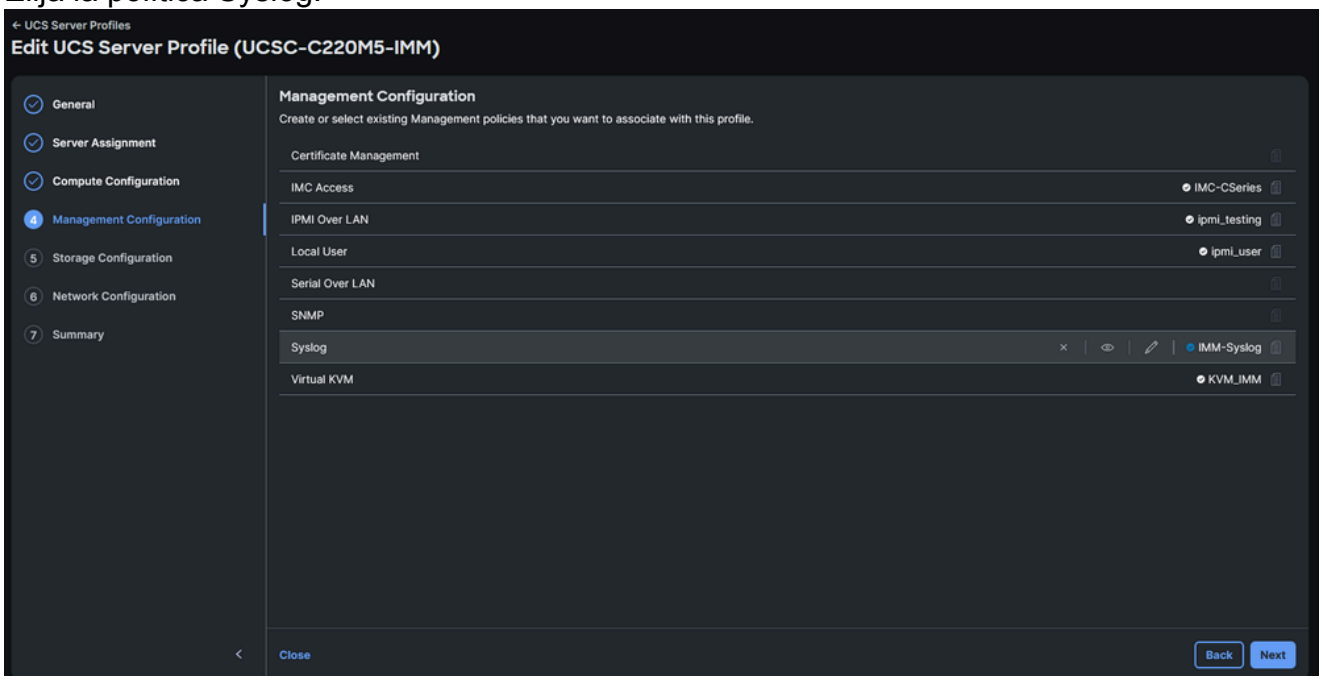


Elija la política syslog en un perfil de dominio de Fabric Interconnect

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.



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

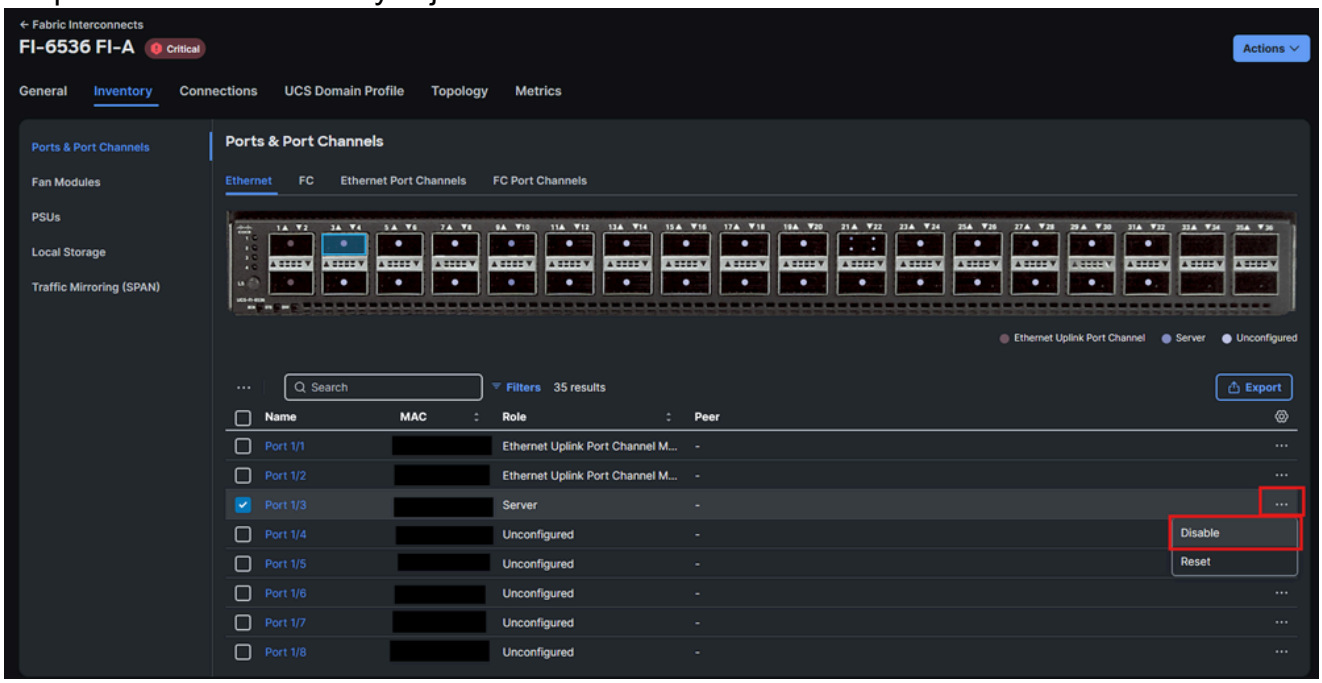
```
 capture-filter "
```

```
port 514

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

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.



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
```

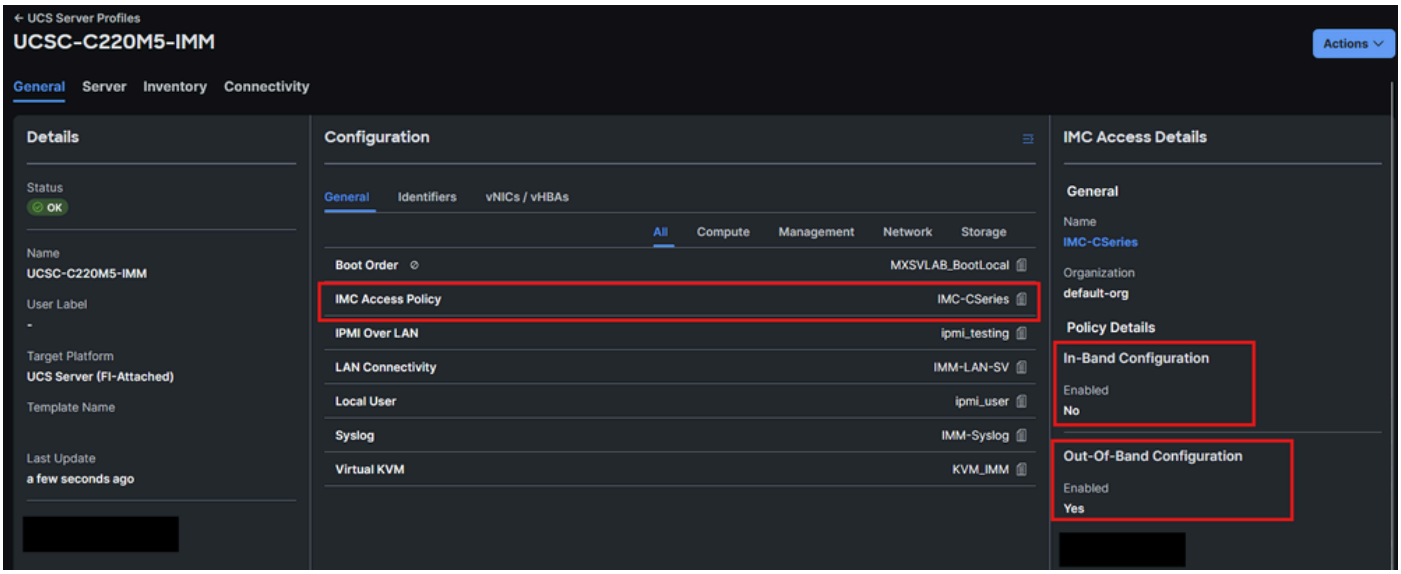
192.0.2.3

```
 : 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.



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.

1. 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,
   ```

```
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

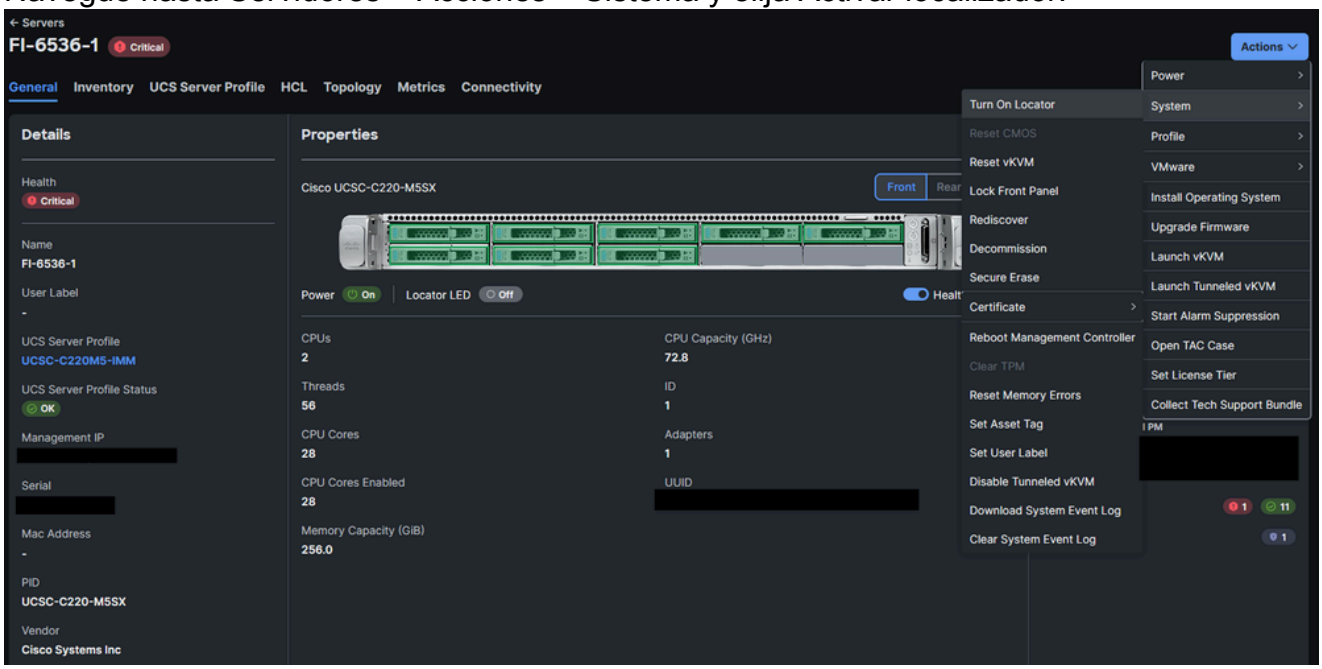
secondary route-preference

: 0, tag: 0

2. Inicie 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:



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

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

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).