

Configureer en controleer Syslog in de UCS Intersight Managed Mode

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Fabric-verbindingen](#)

[Servers](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces voor het instellen en verifiëren van het Syslog-protocol op Intersight Managed Mode UCS-domeinen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Unified Computing System (UCS) servers
- Intersight Managed Mode (IMM)
- Basisconcepten voor netwerken
- Syslog-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Intersightssoftware als een service (SaaS)
- Cisco UCS 6536 fabric interconnect, firmware 4.3(5.240032)
- Rackserver C220 M5, firmware 4.3(2.240090)
- Alma Linux 9

De informatie in dit document is gebaseerd op de apparaten in een specifieke

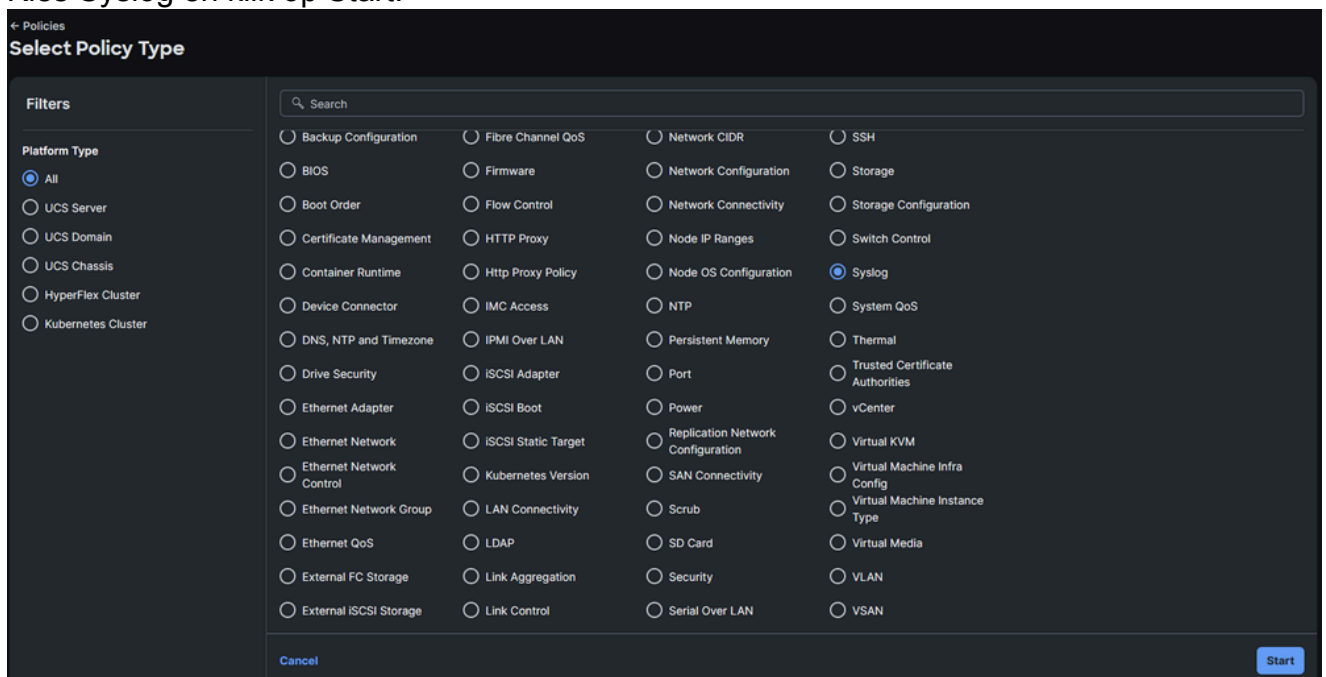
laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Syslog-beleid is van toepassing op Fabric Interconnects en Servers. Ze maken configuratie van lokale en externe vastlegging mogelijk.

Configureren

1. Ga naar **Beleid > Nieuw beleid maken**.
2. Kies **Syslog** en klik op **Start**.



Beleidsselectie

3. Kies de **Organisatie** en kies een naam, klik dan op **Volgende**.

Policies > Syslog

Create

1 General

2 Policy Details

General

Add a name, description, and tag for the policy.

Organization *
default-org

Name *
IMM-Syslog-Policy

Set Tags
Enter a tag in the key:value format.

Description
Description
0 / 1024

Cancel Next

Organisatie en naam configureren

4. Kies de gewenste minimale ernst om te melden voor lokaal vastlegging. De niveaus van de strengheid kunnen op [RFC 5424](#) worden van verwijzingen voorzien.

Policies > Syslog

Create

1 General

2 Policy Details

Policy Details

Add policy details.

All Platforms | UCS Server (Standalone) | UCS Server (FI-Attached) | UCS Domain

Local Logging

File

Minimum Severity to Report * ⓘ
Debug

Warning

Emergency

Alert

Critical

Error

Notice

Informational

Debug

Enable

Enable

Cancel Back Create

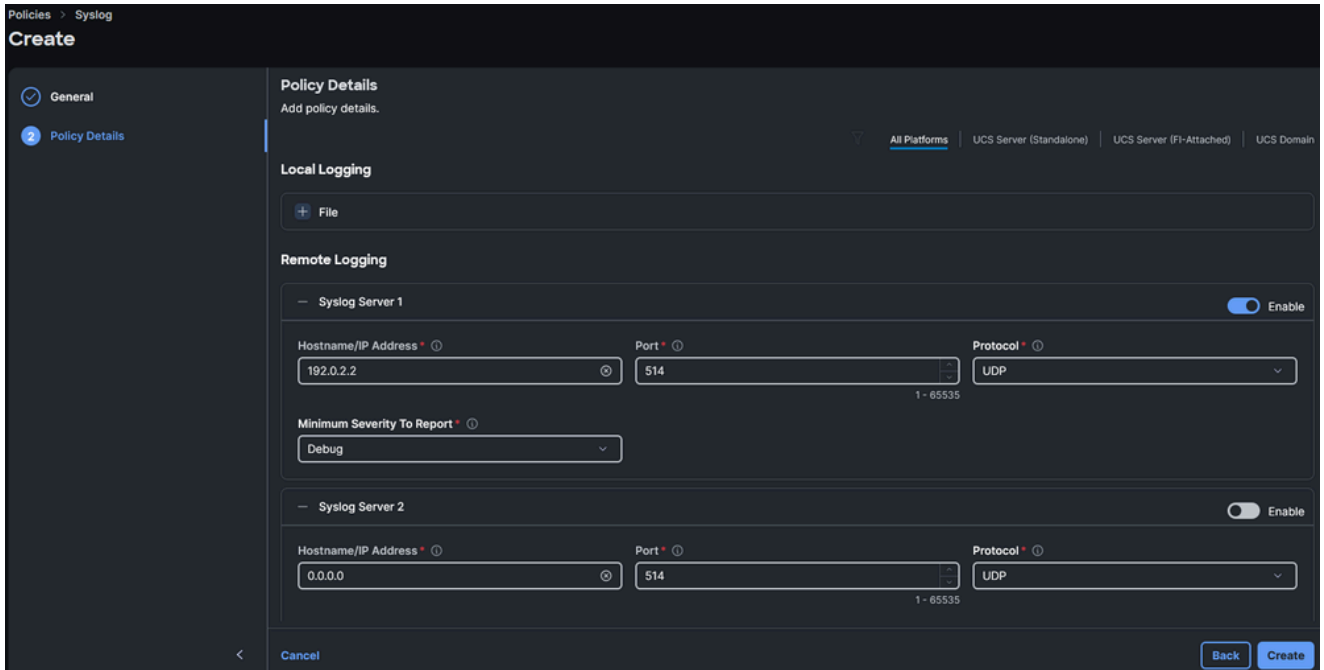
Kies de minimale ernst die u wilt melden voor lokaal vastleggen

5. Kies de gewenste minimale ernst om te melden voor vastlegging op afstand en de gewenste instellingen. Dit zijn de externe server(s), IP-adres of hostnaam, het poortnummer en het poortprotocol (TCP of UDP).



Opmerking: In dit voorbeeld wordt de standaard-instelling UDP-poort 514 gebruikt. Het poortnummer kan worden gewijzigd, maar dit is alleen van toepassing op servers.

 Fabric Interconnects gebruiken de standaardpoort 514 op basis van ontwerp.

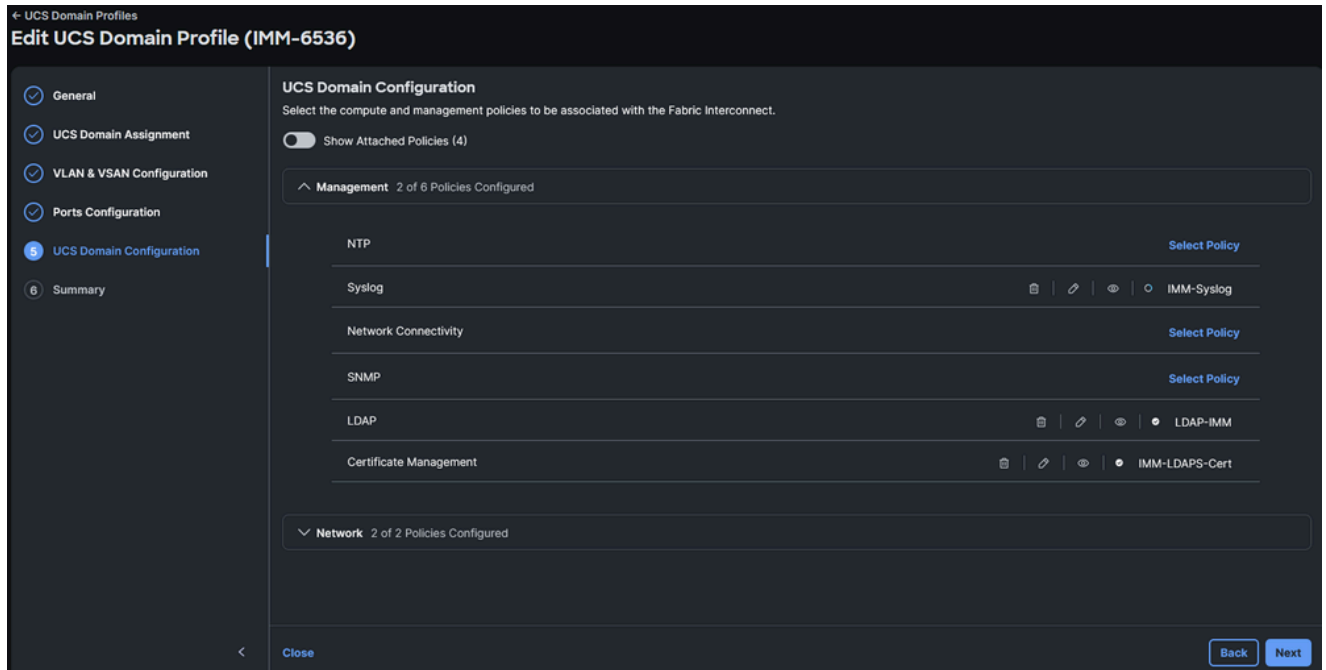


Parameters voor externe vastlegging configureren

6. Klik op Aanmaken.
7. Wijs het beleid toe aan de gewenste apparaten.

Fabric-verbindingen

1. Navigeer naar het Domeinprofiel, klik op Bewerken en klik vervolgens op Volgende tot stap 4 UCS Domain Configuration.
2. Kies onder Beheer > Syslog het gewenste Syslog Policy.

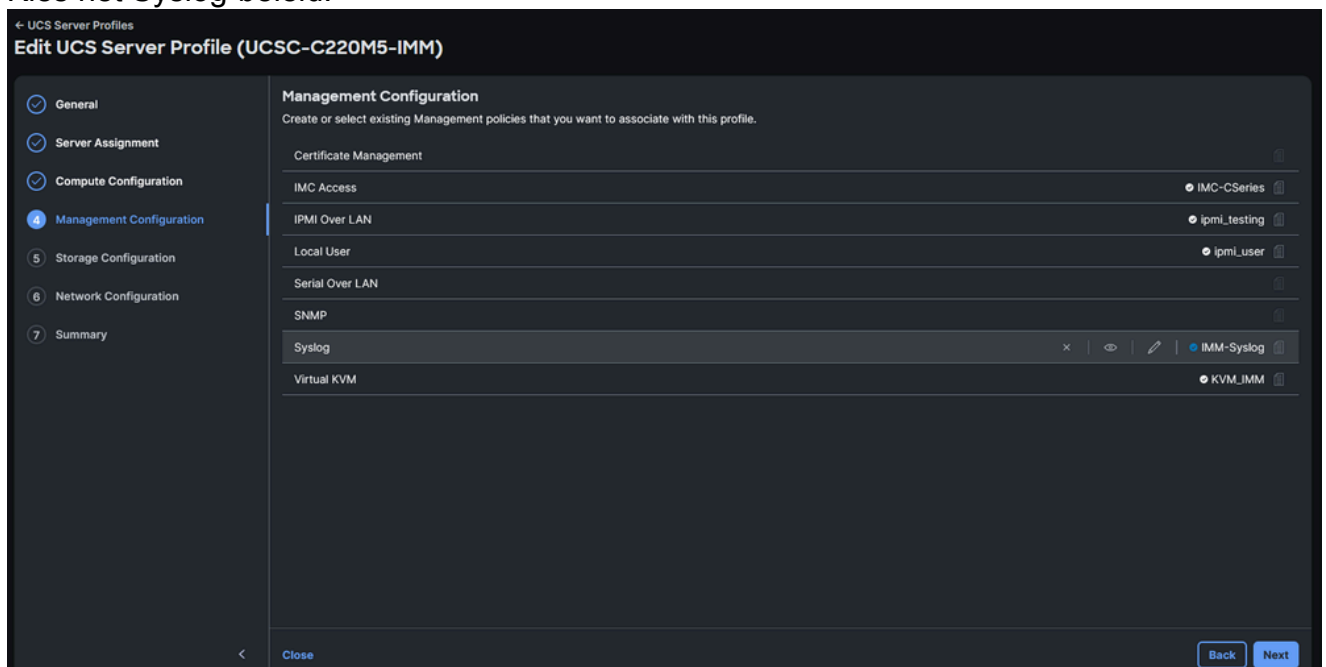


Kies het syslogbeleid voor een Fabric Interconnect Domain Profile

3. Klik op Volgende en implementeer vervolgens. De invoering van dit beleid is niet storend.

Servers

1. Navigeer naar het serverprofiel, klik op Bewerken en ga vervolgens Volgende tot stap 4 Management Configuration.
2. Kies het Syslog-beleid.




Kies het syslogbeleid voor een serverserviceprofiel

3. Ga door tot de laatste stap en implementeer.

Verifiëren

Op dit punt moeten Syslog-berichten worden aangemeld op de Syslog-externe server(s). De Syslog-server werd bijvoorbeeld ingezet op een Linux-server met de rsyslog-bibliotheek.

 **Opmerking:** Verificatie van de Syslog berichten vastlegging kan verschillen afhankelijk van de gebruikte externe Syslog server.

Controleer of de berichten van Fabric Interconnects Syslog op de externe server zijn aangemeld:

```
[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
```

Bevestig dat de berichten van het Syslog van de Servers op de verre server zijn ingelogd:

```
[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 level:3)
Jan 16 20:16:23 192.0.2.5 AUDIT[2257]: Local User Management (strong password policy :disabled) by User:(null)
Jan 16 20:16:23 192.0.2.5 AUDIT[2257]: Password Expiration Parameters (password_history:5,password_expiry:30)
Jan 16 20:16:26 192.0.2.5 AUDIT[2257]: Local Syslog Severity changed to "Debug" by User:(null) from Info
Jan 16 20:16:27 192.0.2.5 AUDIT[2257]: Secured Remote Syslog with(serverId =1, secure_enabled =0) by User:(null)
```

Problemen oplossen

Een pakketopname kan worden uitgevoerd op de Fabric Interconnects om te bevestigen of de Syslog-pakketten correct zijn doorgestuurd. Wijzig de minimale ernst van het rapport voor debug. Zorg ervoor dat Syslog zoveel mogelijk informatie verstrekt.

Start vanuit de opdrachtregelinterface een pakketopname op de beheerpoort en filter op poort 514 (Syslog-poort):

```
<#root>
```

```
FI-6536-A# connect nxos
```

```
FI-6536-A(nx-os)# ethanalyzer
```

```
local interface mgmt
```

```
capture-filter "
```

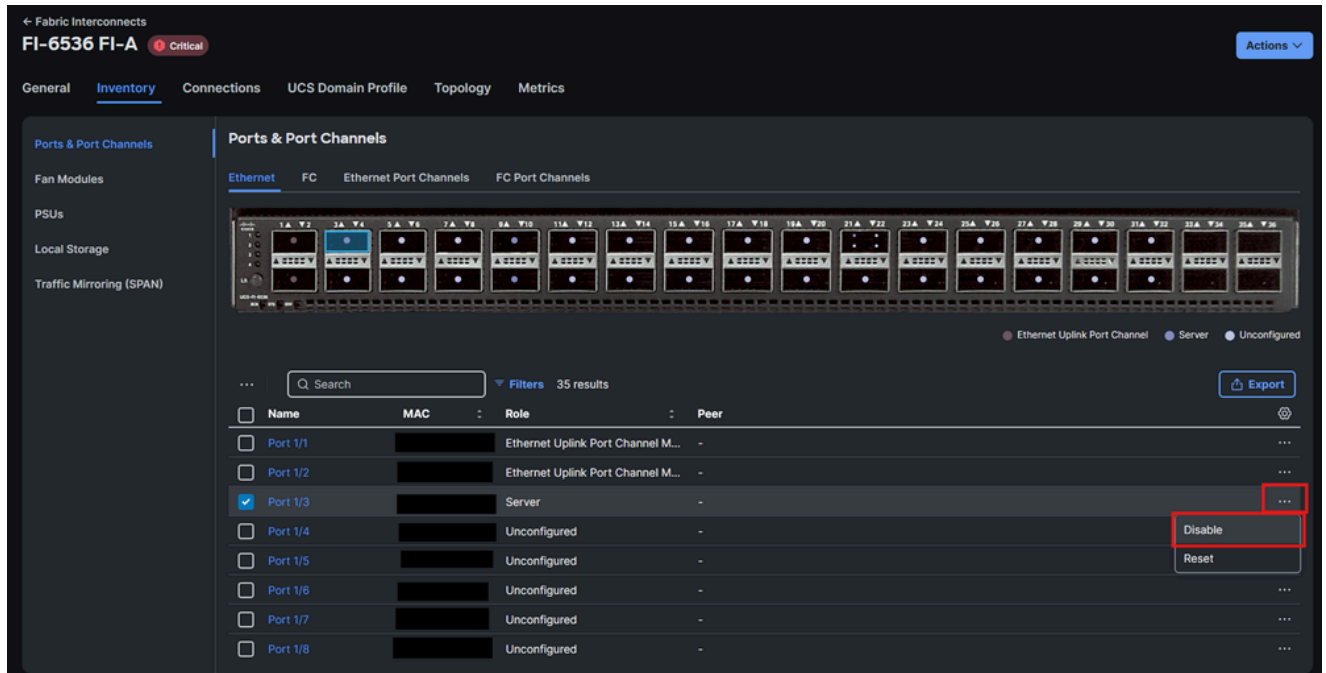
```
port 514
```

```
" limit-captured-frames 0
```

```
Capturing on mgmt0
```

In dit voorbeeld is een serverpoort op Fabric Interconnect A gemarkeerd om Syslog-verkeer te genereren.

1. Navigeer naar Fabric Interconnects > Inventory.
2. Klik op het selectievakje voor de gewenste poort, open het ellipsmenu aan de rechterkant en kies uitschakelen.



Sluit een interface op een Fabric Interconnect af om syslog-verkeer te genereren voor het testen

3. De console in de Fabric Interconnect moet het Syslog-pakket opnemen:

```
<#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. Het bericht moet worden ingelogd op uw externe server:

```
<#root>
```


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

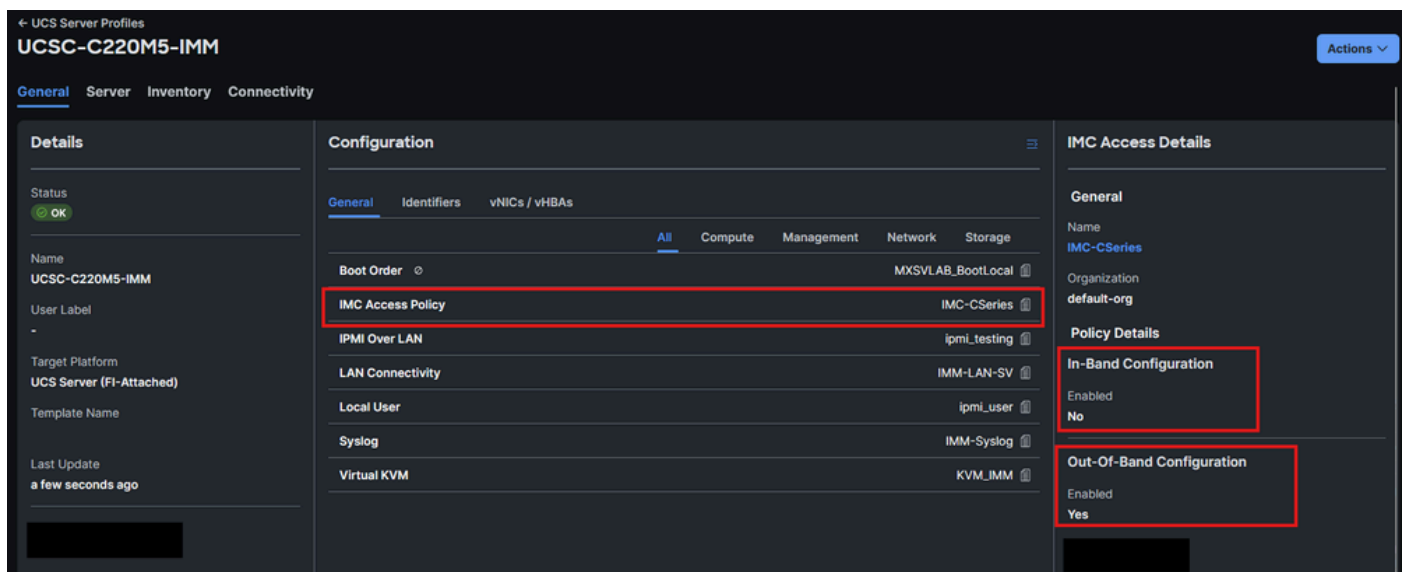
```
192.0.2.3
```

: 2025 Jan 16 22:17:40 UTC:

%ETHPORT-5-IF_DOWN_NONE: Interface Ethernet1/3 is down (Transceiver Absent)

Dezelfde test kan op servers worden uitgevoerd:

 **Opmerking:** Deze procedure werkt alleen voor servers met out-of-band configuratie op hun IMC Access Policy. Als Inband in gebruik is, voer in plaats daarvan de pakketopname op de externe Syslog-server uit, of bereik uit naar TAC om het met interne debug-opdrachten uit te voeren.



The screenshot shows the UCS Server Profiles configuration page for UCSC-C220M5-IMM. The page is divided into three main sections: Details, Configuration, and IMC Access Details. The Configuration section is further divided into tabs: General, Identifiers, and vNICs / vHBAs. The IMC Access Details section is further divided into General and Policy Details. The Policy Details section is further divided into In-Band Configuration and Out-Of-Band Configuration. The In-Band Configuration is set to No, and the Out-Of-Band Configuration is set to Yes. The IMC Access Policy is set to IMC-CSeries.

Controleer de configuratie op het IMC-toegangsbeleid

In dit voorbeeld is de LED locator op een C220 M5 geïntegreerde server ingeschakeld. Dit vereist geen downtime.

1. Controleer welke Fabric Interconnect out-of-band verkeer naar uw server verstuurt. De server IP is 192.0.2.5, dus Fabric Interconnect A stuurt zijn beheerverkeer door ("secundaire route" betekent dat de Fabric Interconnect fungeert als een proxy voor het serverbeheerverkeer):

```
<#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
```



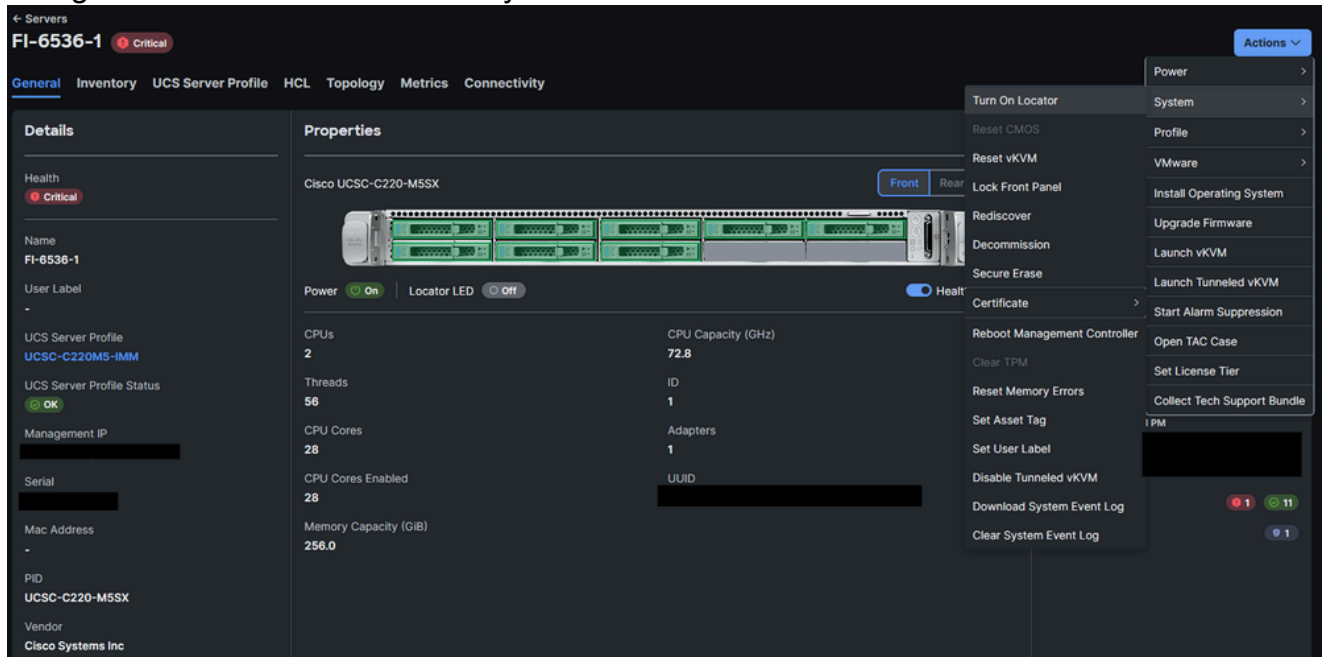
```
secondary route-preference
```

```
: 0, tag: 0
```

2. Start een pakketopname op de juiste fabric interconnect:

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

3. Navigeer naar servers > Acties > Systeem en kies Locator inschakelen:



LED-locator in een server inschakelen

4. De console in de Fabric Interconnect moet het Syslog-pakket tonen dat is opgenomen:

```
<#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. Het Syslog-bericht moet worden ingelogd in uw externe server AUDIT.log-bestand:

```
<#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:
```

Als Syslog-pakketten zijn gegenereerd door UCS, maar de Syslog-server deze niet heeft geregistreerd:

1. Bevestig dat de pakketten op de externe Syslog-server zijn gearriveerd met een pakketopname.
2. Controleer de configuratie van uw externe Syslog-server (inclusief, maar niet beperkt tot: geconfigureerd syslog poort en firewall instellingen).

Gerelateerde informatie

- [RFC 5424 - Het Syslog-protocol](#)
- [Intersight IMM Expert Series - Syslog Policy](#)
- [Cisco Intersight Help Center - UCS Domain Profile Policies configureren](#)
- [Cisco Intersight Help Center - Serverbeleid configureren](#)

Als de server Inband heeft geconfigureerd op zijn IMC-toegangsbeleid, laadt u CIMC debug shell en voert u een pakketopname uit op de **bond0**-interface voor racks of **bond0.x**-interface (waar x het VLAN is) voor bladeservers.

```
[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)
```

- Het systeempoortnummer kan niet worden gewijzigd op Fabric Interconnects, alleen in servers. Dit is door ontwerp en werd gedocumenteerd op

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.