UCS Intersight 관리 모드에서 Syslog 구성 및 확인

목차

소개

이 문서에서는 Intersight Managed Mode UCS Domains에서 Syslog 프로토콜을 설정하고 확인하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- UCS(Unified Computing System) 서버
- IMM(Intersight Managed Mode)
- 네트워킹 기본 개념
- Syslog 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Intersight SaaS(Software as a Service)
- Cisco UCS 6536 Fabric Interconnect, 펌웨어 4.3(5.240032)
- 랙 서버 C220 M5, 펌웨어 4.3(2.240090)
- Alma Linux 9

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

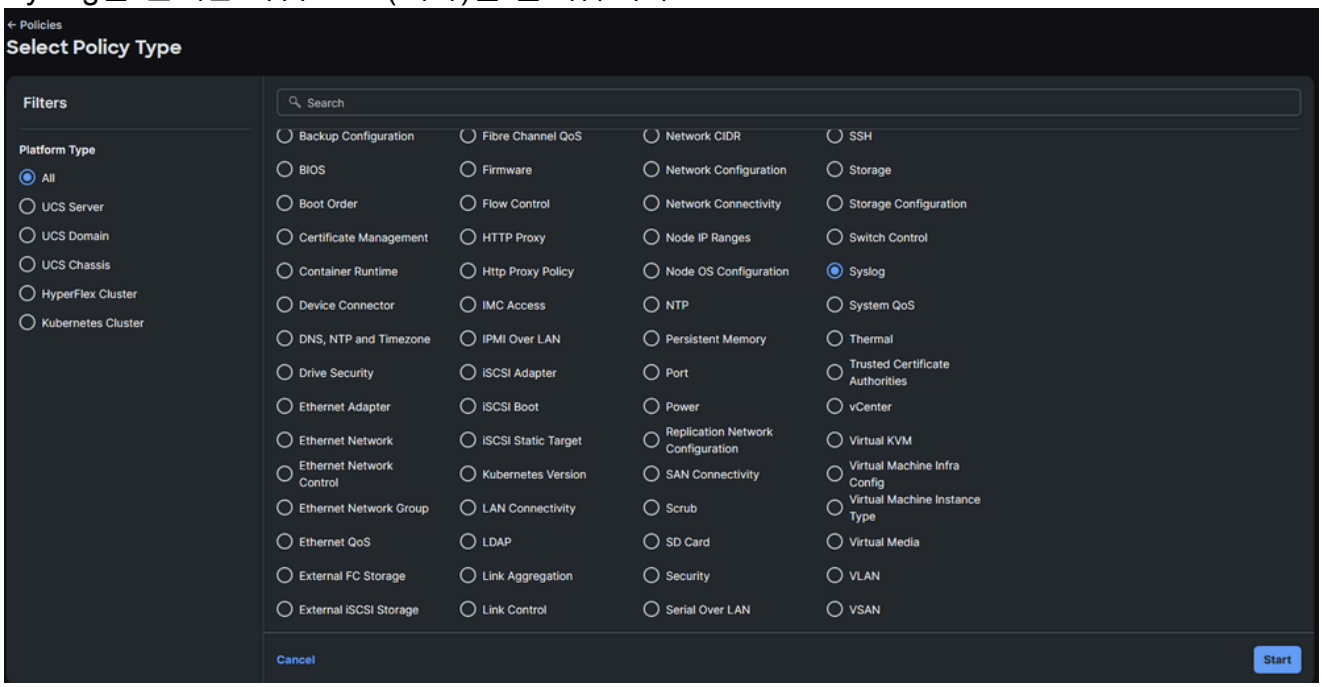
이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Syslog 정책은 패브릭 인터커넥트 및 서버에 적용됩니다. 로컬 및 원격 로깅을 구성할 수 있습니다.

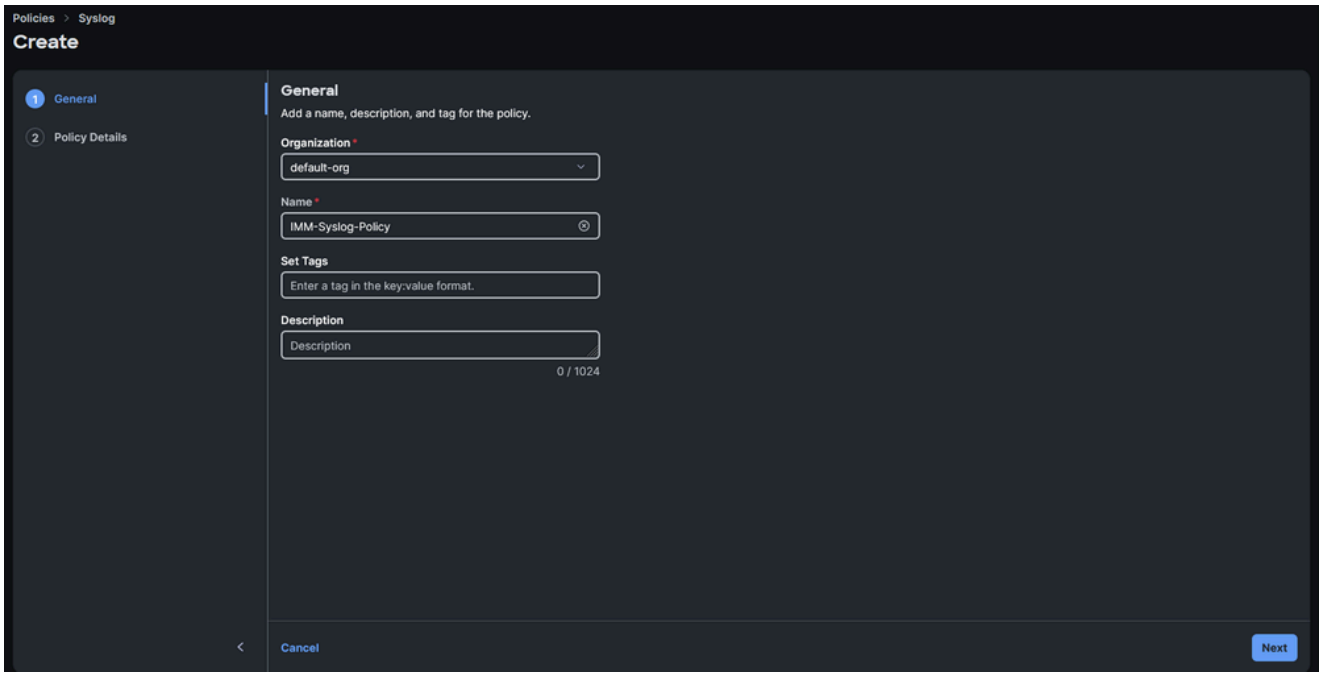
구성

1. Policies(정책) > Create new policy(새 정책 생성)로 이동합니다.
2. Syslog를 선택한 다음 Start(시작)를 클릭합니다.



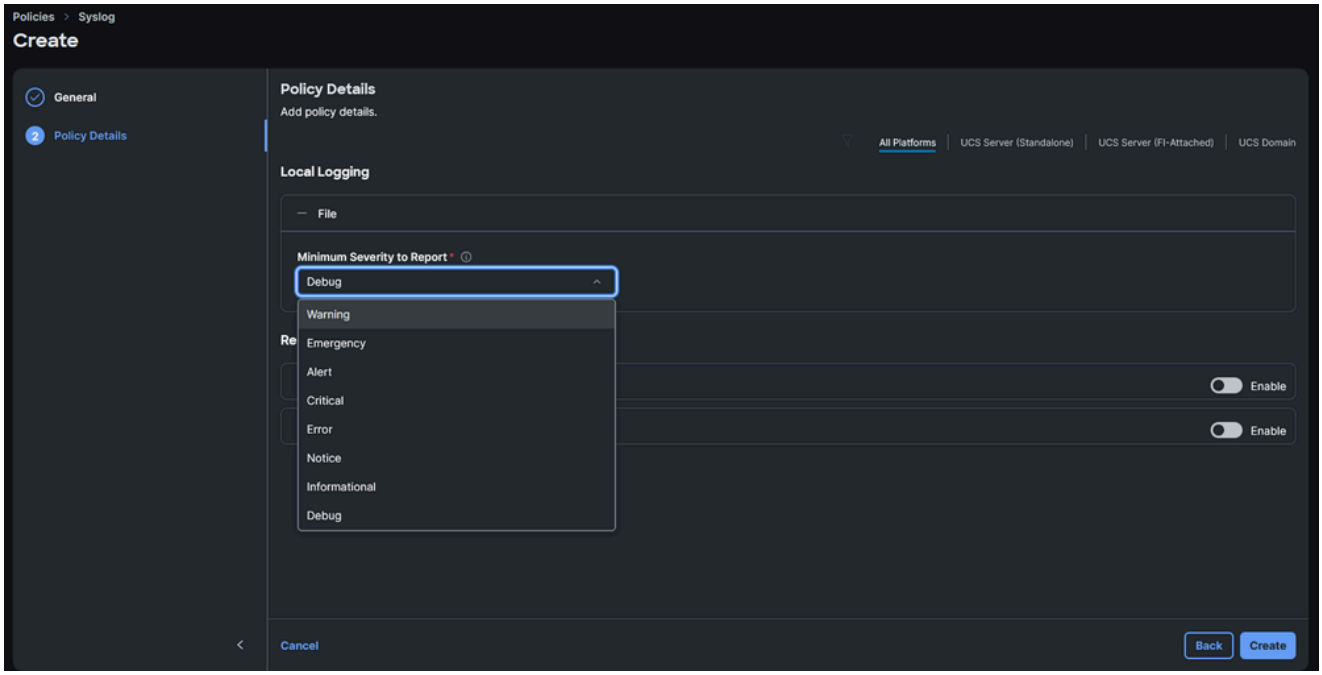
정책 선택

3. 조직을 선택하고 이름을 선택한 후 다음을 누릅니다.



조직 및 이름 구성

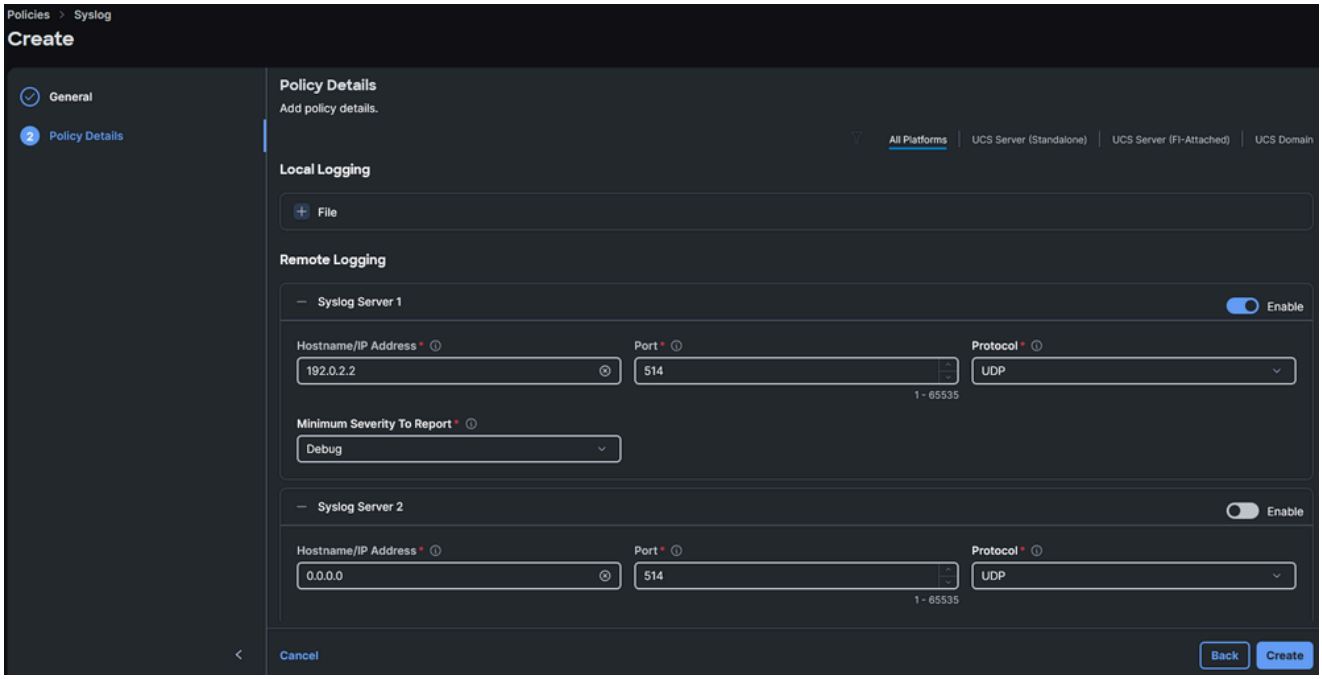
4. 로컬 로깅을 위해 보고하려는 최소 심각도를 선택합니다. 심각도 레벨은 RFC 5424에서 참조할 수 있습니다.



로컬 로깅을 위해 보고할 최소 심각도 선택

5. 원격 로깅을 위해 보고하려는 최소 심각도 및 필수 설정을 선택합니다. 원격 서버 IP 주소 또는 호스트 이름, 포트 번호 및 포트 프로토콜(TCP 또는 UDP)입니다.

참고: 이 예에서는 기본 설정인 UDP 포트 514를 사용합니다. 포트 번호는 변경할 수 있지만 이 내용은 서버에만 적용됩니다. 패브릭 인터커넥트는 설계에 따라 기본 포트(514)를 사용합니다.

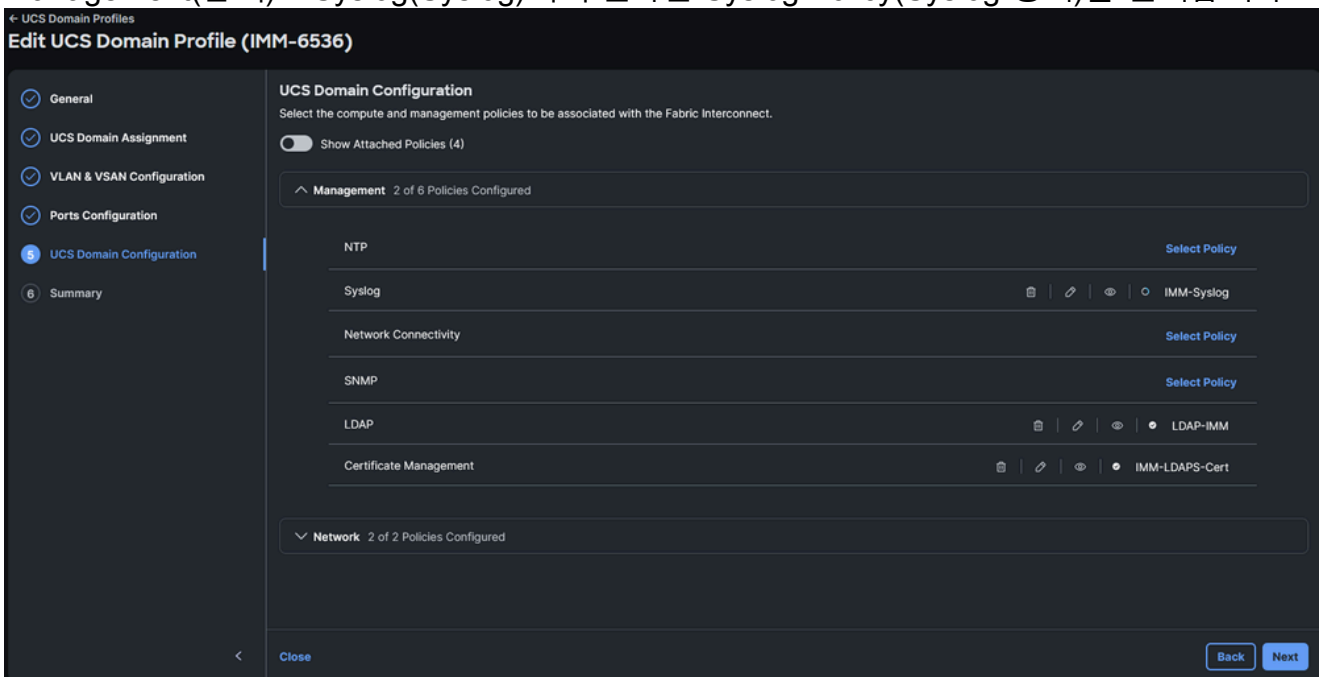


원격 로깅 매개변수 구성

6. Create(생성)를 클릭합니다.
7. 원하는 디바이스에 정책을 할당합니다.

패브릭 인터커넥트

1. Domain Profile(도메인 프로파일)로 이동하여 Edit(수정)를 클릭한 다음 4단계 UCS Domain Configuration(UCS 도메인 컨피그레이션)까지 Next(다음)를 클릭합니다.
2. Management(관리) > Syslog(Syslog)에서 원하는 Syslog Policy(Syslog 정책)를 선택합니다.

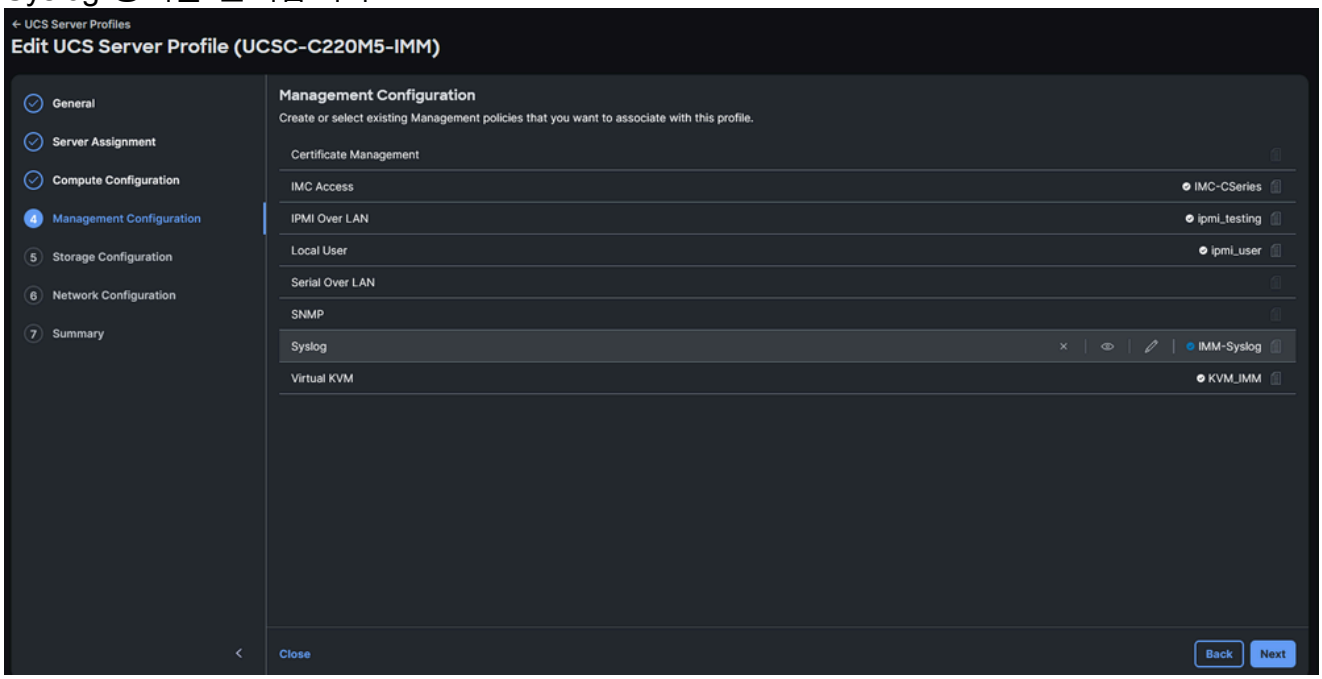


패브릭 인터커넥트 도메인 프로필에서 syslog 정책을 선택합니다

3. Next(다음)를 클릭한 다음 Deploy(구축)를 클릭합니다. 이 정책의 구축은 중단되지 않습니다.

서버

1. Server Profile(서버 프로필)로 이동하여 Edit(편집)를 클릭한 다음 4단계 Management Configuration(관리 컨피그레이션)까지 Next(다음)로 이동합니다.
2. Syslog 정책을 선택합니다.



서버 서비스 프로필에서 syslog 정책 선택

3. 마지막 단계까지 계속하고 구축합니다.

다음을 확인합니다.

이때 Syslog 메시지는 Syslog 원격 서버에 기록되어야 합니다. 이 예에서 Syslog 서버는 rsyslog 라이브러리가 있는 Linux 서버에 구축되었습니다.

✎ 참고: Syslog 메시지 로깅의 확인은 사용 중인 원격 Syslog 서버에 따라 다를 수 있습니다.

Fabric Interconnect Syslog 메시지가 원격 서버에 기록되었는지 확인합니다.

```
[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
```

서버 Syslog 메시지가 원격 서버에 기록되었는지 확인합니다.

```
[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
```

문제 해결

Fabric Interconnect에서 패킷 캡처를 수행하여 Syslog 패킷이 올바르게 전달되었는지 확인할 수 있습니다. 디버깅할 보고서의 최소 심각도를 변경합니다. Syslog에서 최대한 많은 정보를 보고하도록 합니다.

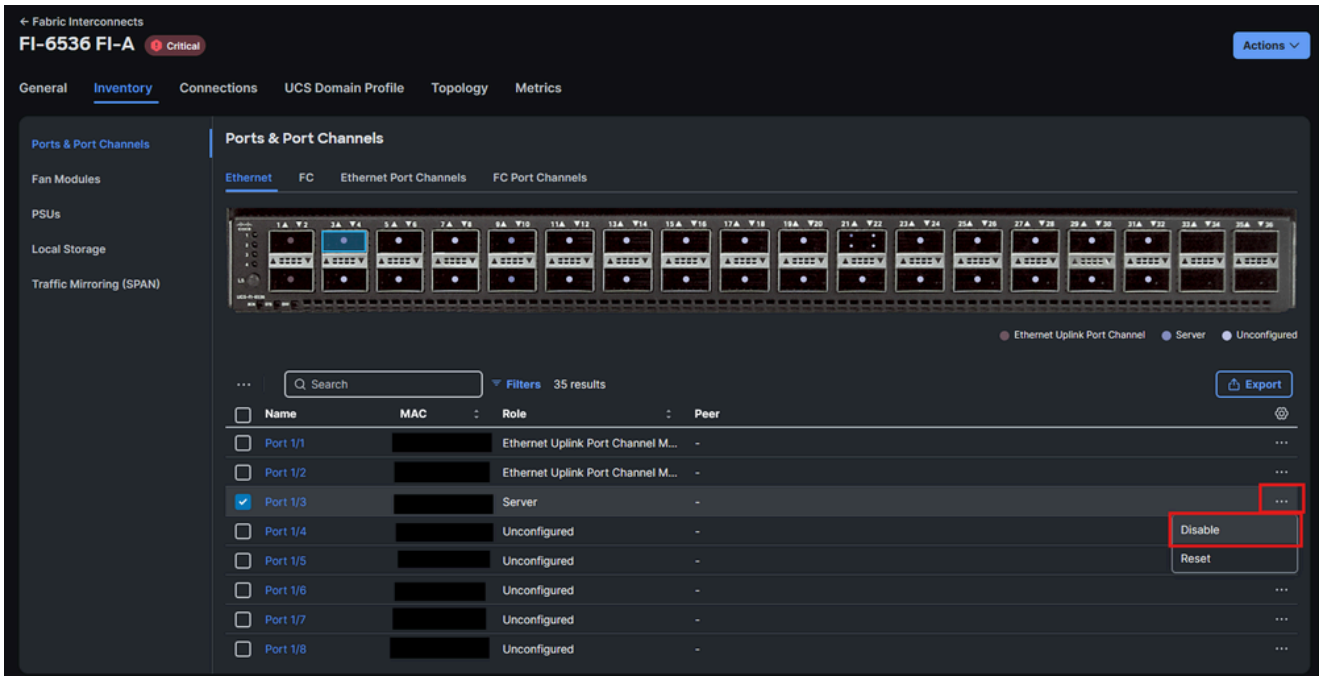
명령줄 인터페이스에서 관리 포트에서 패킷 캡처를 시작하고 포트 514(Syslog 포트)로 필터링합니다.

<#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
```

이 예에서는 Fabric Interconnect A의 서버 포트가 플래핑되어 Syslog 트래픽을 생성했습니다.

1. Fabric Interconnects(패브릭 인터커넥트) > Inventory(인벤토리)로 이동합니다.
2. 원하는 포트의 확인란을 클릭하고 오른쪽의 줄임표 메뉴를 열고 disable을 선택합니다.



테스트용 syslog 트래픽을 생성하기 위해 Fabric Interconnect에서 인터페이스를 종료합니다

3. 패브릭 인터커넥트의 콘솔은 Syslog 패킷을 캡처해야 합니다.

<#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)
```

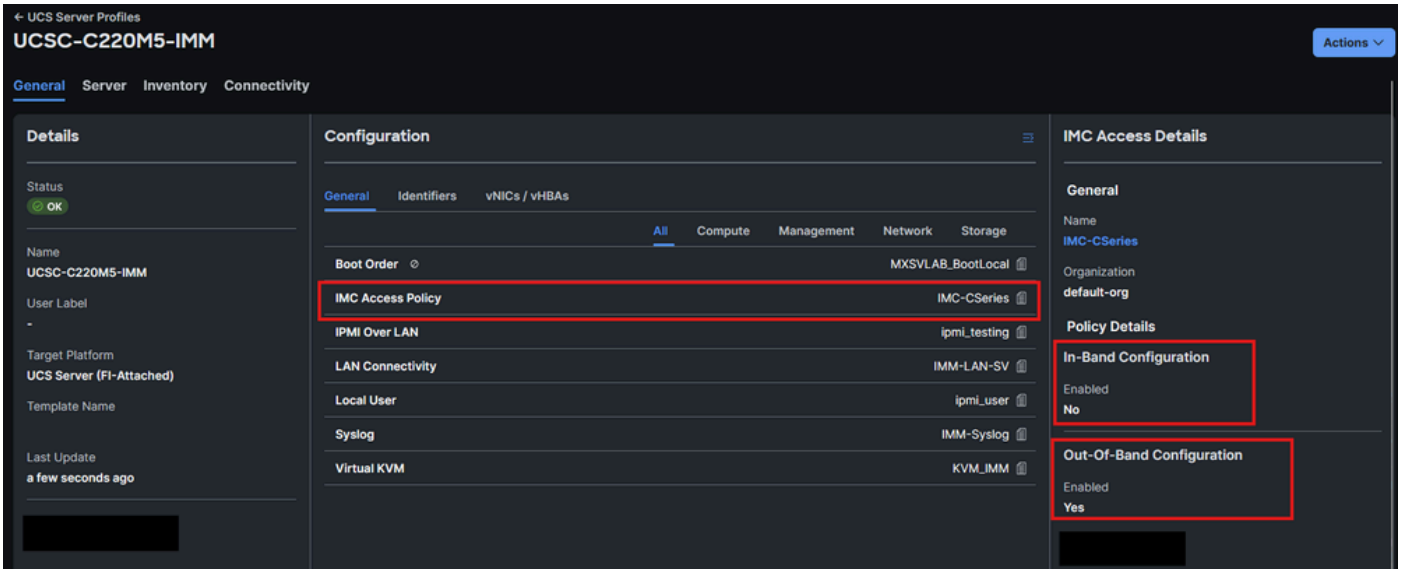
4. 원격 서버에 메시지를 기록해야 합니다.

<#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)
```

동일한 테스트를 서버에서 실행할 수 있습니다.

참고: 이 절차는 IMC 액세스 정책에 대역 외 컨피그레이션이 있는 서버에서만 작동합니다. 인밴드가 사용 중인 경우 대신 원격 Syslog 서버에서 패킷 캡처를 수행하거나, TAC에 문의하여 내부 debug 명령으로 수행합니다.



IMC 액세스 정책의 컨피그레이션을 확인합니다.

이 예에서는 C220 M5 Integrated Server의 LED 로케이터를 활성화했습니다. 따라서 다운타임이 필요하지 않습니다.

1. 어떤 Fabric Interconnect가 서버에 대해 대역외 트래픽을 전송하는지 확인합니다. 서버 IP는 192.0.2.5이므로 Fabric Interconnect A가 관리 트래픽을 전달합니다("보조 경로"는 Fabric Interconnect가 서버 관리 트래픽의 프록시 역할을 함을 의미함).

   <#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

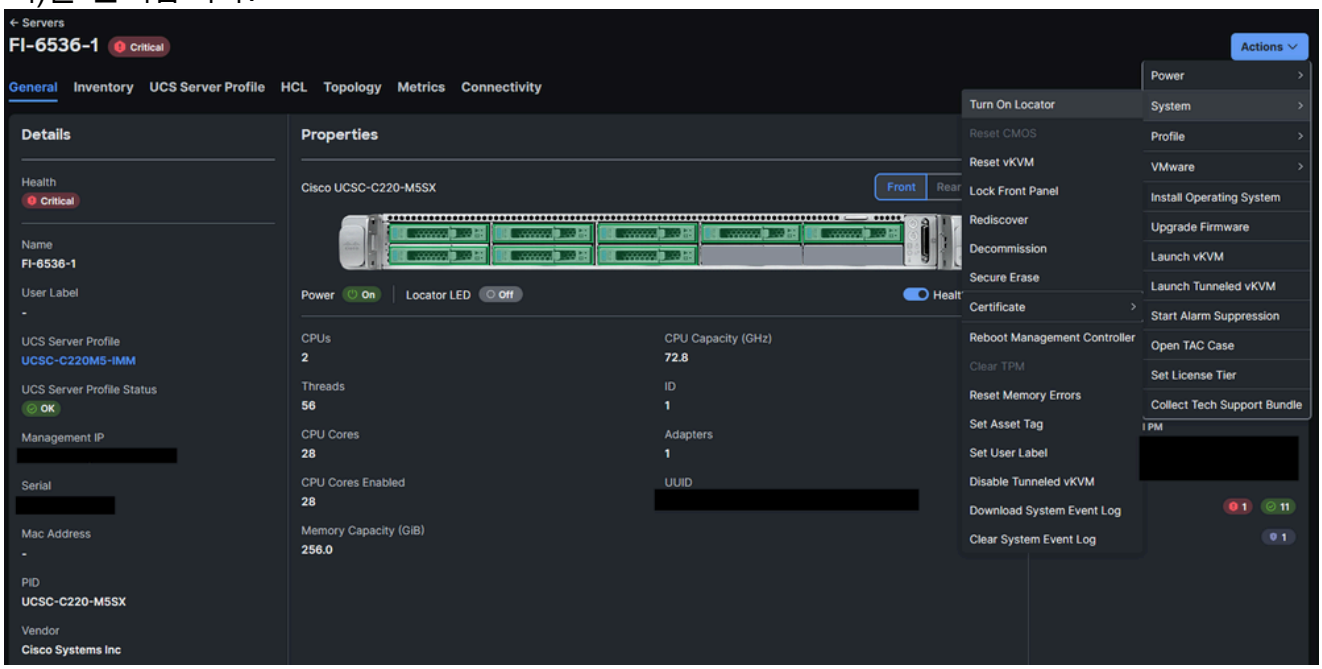
   secondary route-preference

   : 0, tag: 0

2. 적절한 Fabric Interconnect에서 패킷 캡처를 시작합니다.

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

3. Servers(서버) > Actions(작업) > System(시스템)으로 이동하고 Turn On Locator(로케이터 켜기)를 선택합니다.



서버에서 LED 로케이터 켜기

4. 패브릭 인터커넥트의 콘솔에는 캡처된 Syslog 패킷이 표시되어야 합니다.

<#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. Syslog 메시지는 원격 서버 AUDIT.log 파일에 기록되어야 합니다:

<#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:
```

Syslog 패킷이 UCS에 의해 생성되었지만 Syslog 서버가 이를 기록하지 않은 경우:

1. 패킷이 패킷 캡처와 함께 원격 Syslog 서버에 도착했는지 확인합니다.
2. 원격 Syslog 서버의 컨피그레이션을 확인합니다(다음을 포함하되 이에 국한되지 않음). syslog 포트 및 방화벽 설정을 구성했습니다.

관련 정보

- RFC 5424 - Syslog 프로토콜
- Intersight IMM Expert Series - Syslog 정책
- Cisco Intersight Help Center - UCS 도메인 프로파일 정책 구성
- Cisco Intersight Help Center - 서버 정책 구성

서버에 IMC 액세스 정책에 인밴드가 구성되어 있는 경우 CIMC 디버그 셸을 로드하고 bond0 인터페이스 for Racks 또는 bond0.x 인터페이스(x는 VLAN)에서 패킷 캡처를 수행합니다.

```
[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)
```

- Fabric Interconnect에서는 Syslog 포트 번호를 변경할 수 없으며 서버에서만 변경할 수 있습니다. 이는 설계에 따른 것이며

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.