UCS Intersightマネージドモードのsyslogの設定と確認

内容

はじめに

このドキュメントでは、Intersight Managed Mode UCSドメインでSyslogプロトコルをセットアップして確認するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Unified Computing System(UCS)サーバ
- Intersightマネージドモード(IMM)
- ネットワーキングの基本概念
- Syslogプロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Intersight Software as a Service(SaaS)
- Cisco UCS 6536ファブリックインターコネクト、ファームウェア4.3(5.240032)
- ラックサーバC220 M5、ファームウェア4.3(2.240090)
- アルマLinux 9

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

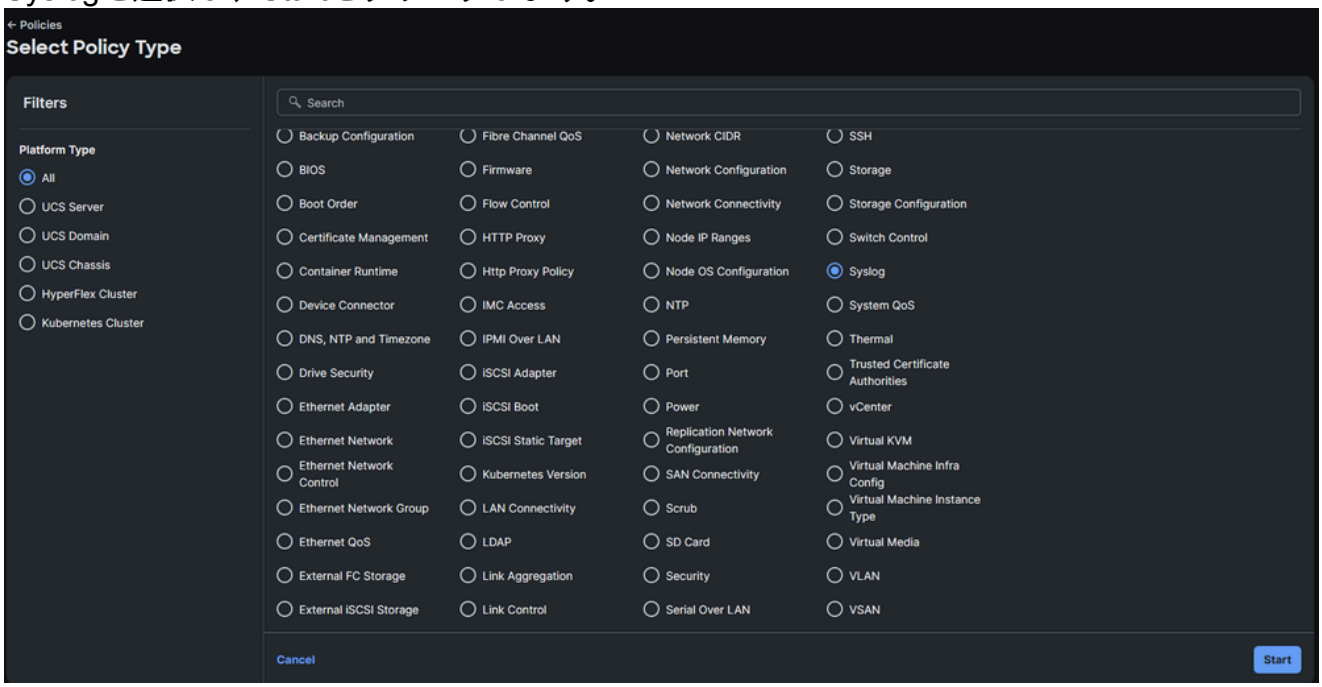
キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Syslogポリシーは、ファブリックインターコネクトとサーバに適用できます。ローカルロギングとリモートロギングを設定できます。

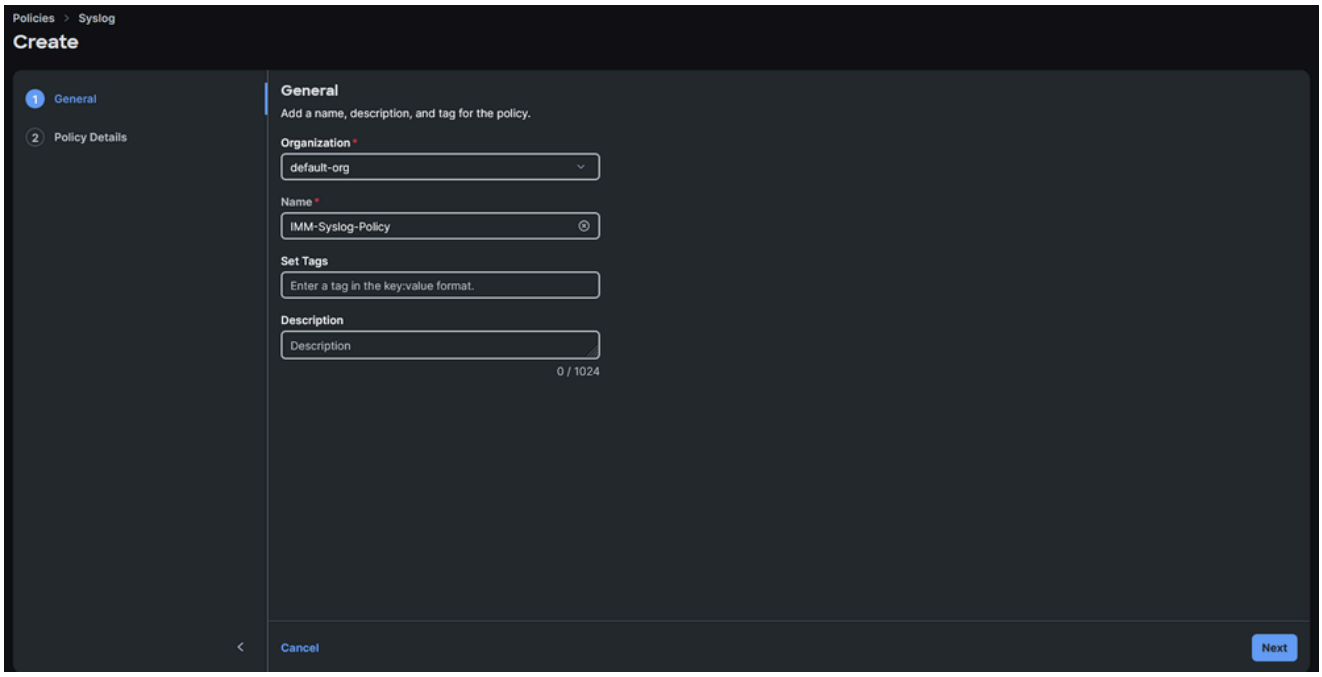
設定

1. Policies > Create new policyの順に移動します。
2. Syslogを選択し、Startをクリックします。



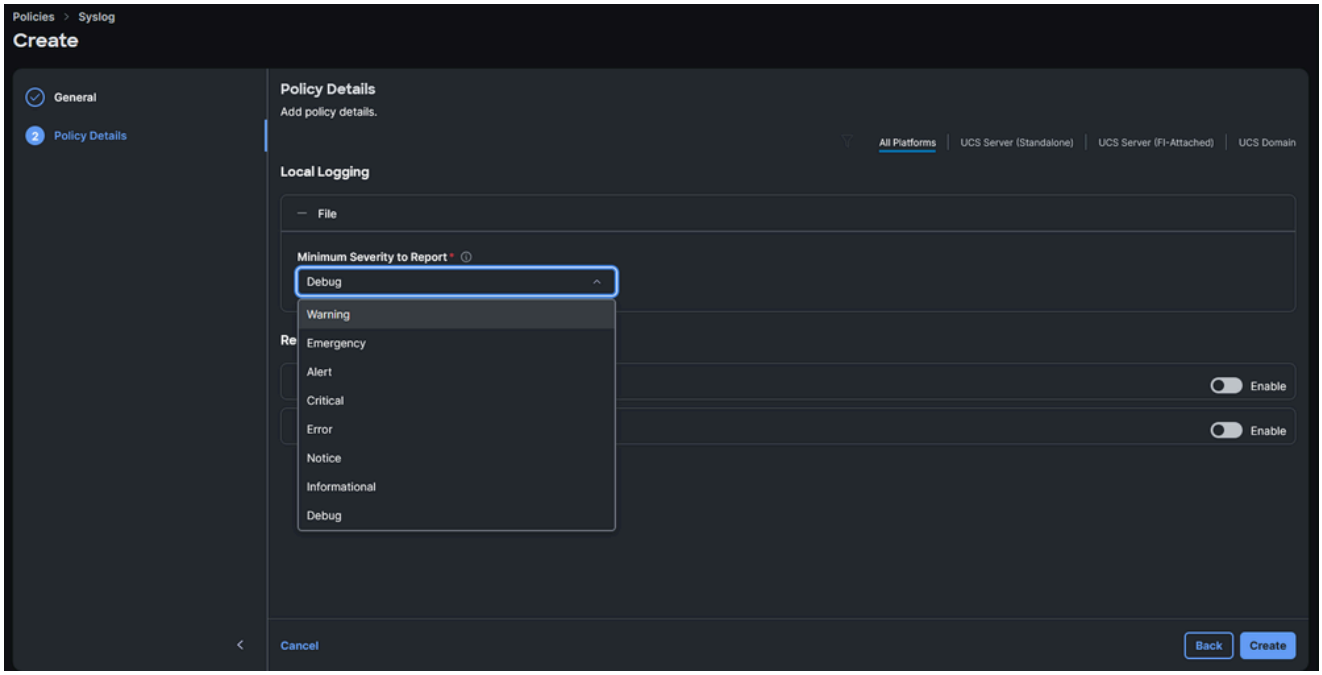
ポリシーの選択

3. 組織を選択して名前を選択し、Nextをクリックします。



組織と名前の設定

4. ローカルロギングに対してレポートする最小重大度を選択します。重大度は、RFC 5424で参照できます。

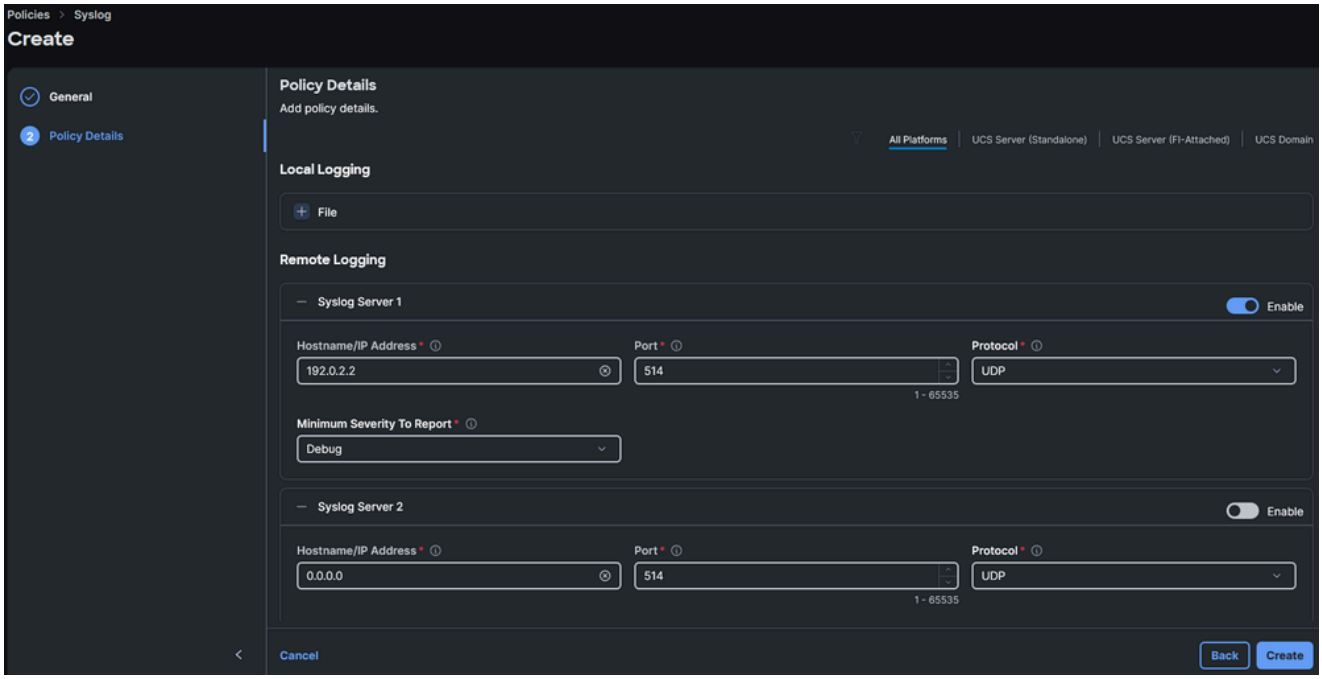


ローカルロギングで報告する重大度の最小値を選択します

5. リモートロギングに対してレポートする最小重大度と必要な設定を選択します。これらは、リモートサーバのIPアドレスまたはホスト名、ポート番号、およびポートプロトコル（TCPまたはUDP）です。

> 注：この例では、デフォルト設定のUDPポート514を使用しています。ポート番号は変更できますが、これはサーバだけに適用されます。ファブリックインターコネクト

は、デフォルトのポート514を使用するように設計されています。

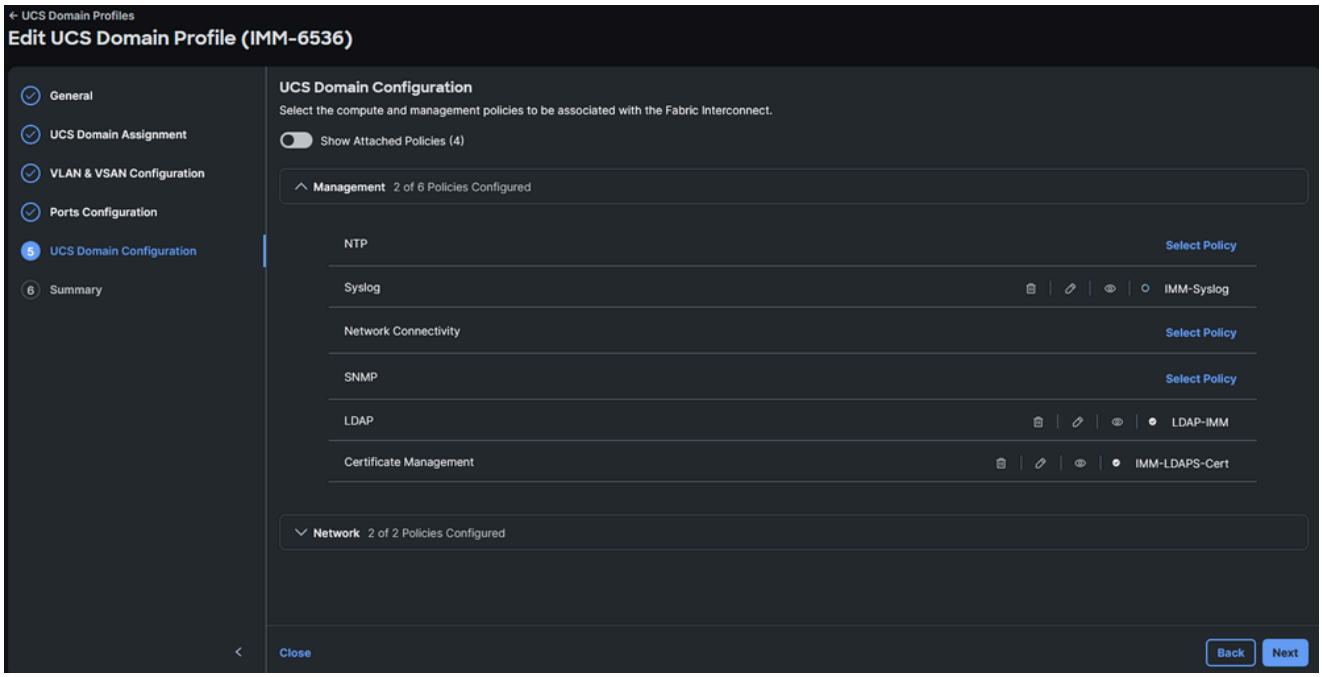


リモートロギングパラメータの設定

6. [Create] をクリックします。
7. 目的のデバイスにポリシーを割り当てます。

Fabric Interconnect

1. Domain Profileに移動して、Editをクリックし、ステップ4 UCS Domain Configurationまで Nextをクリックします。
2. Management > Syslogで、目的のSyslogポリシーを選択します。

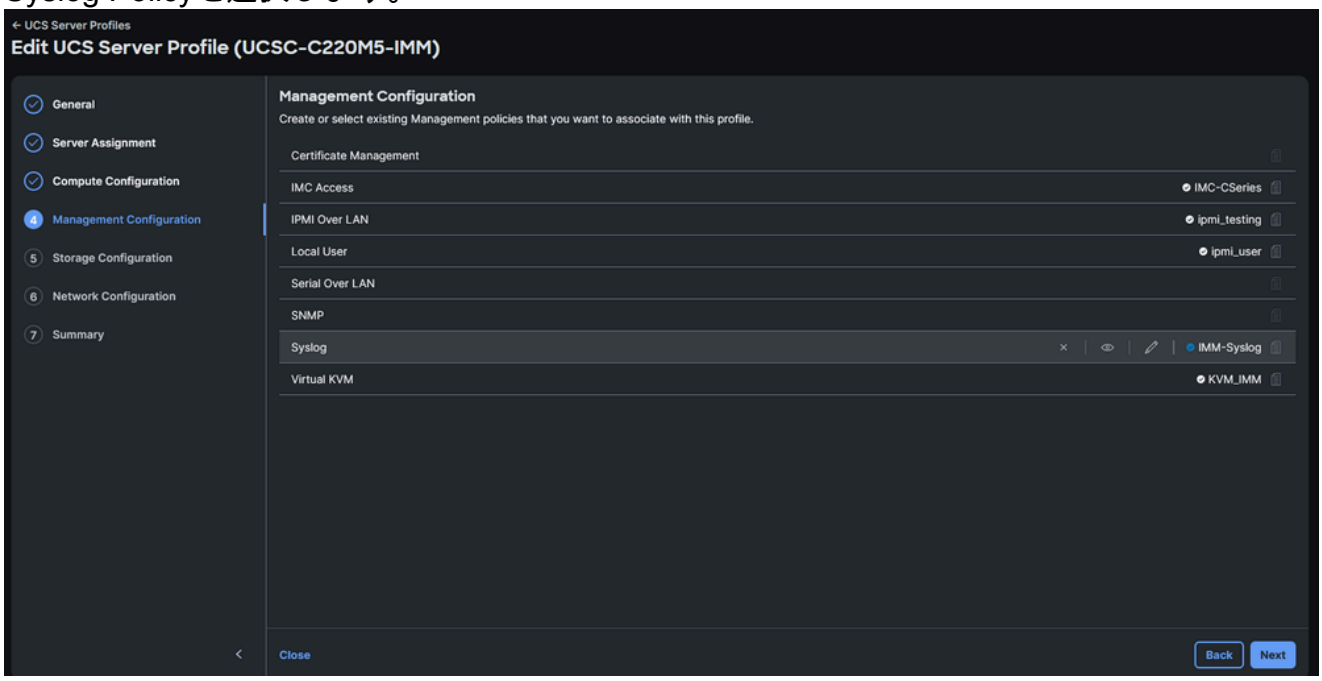


ファブリックインターコネクトドメインプロファイルのsyslogポリシーを選択します

3. Next、Deployの順にクリックします。このポリシーの導入によって中断が発生することはありません。

サーバ

1. Server Profileに移動し、Editをクリックしてから、ステップ4 Management ConfigurationまでNextに進みます。
2. Syslog Policyを選択します。



サーバサービスプロファイルのsyslogポリシーを選択します

3. 最後のステップまで続行し、展開します。

確認

この時点で、SyslogメッセージはSyslogリモートサーバに記録される必要があります。 この例では、syslogサーバはsyslogライブラリを備えたLinuxサーバに展開されています。

注:Syslogメッセージの口ギングの検証は、使用しているリモートSyslogサーバによって異なる場合があります。

Fabric Interconnectのsyslogメッセージがリモートサーバに記録されたことを確認します。

```
[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
```

サーバのsyslogメッセージがリモートサーバに記録されたことを確認します。

```
[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
```

トラブルシュート

Syslogパケットが正しく転送されたかどうかを確認するために、ファブリックインターコネクトでパケットキャプチャを実行できます。レポートする重大度の最小値をdebugに変更します。Syslogが可能な限り多くの情報を報告するようにします。

コマンドラインインターフェイスから、管理ポートでパケットキャプチャを開始し、ポート514（Syslogポート）でフィルタリングします。

<#root>

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

local interface mgmt

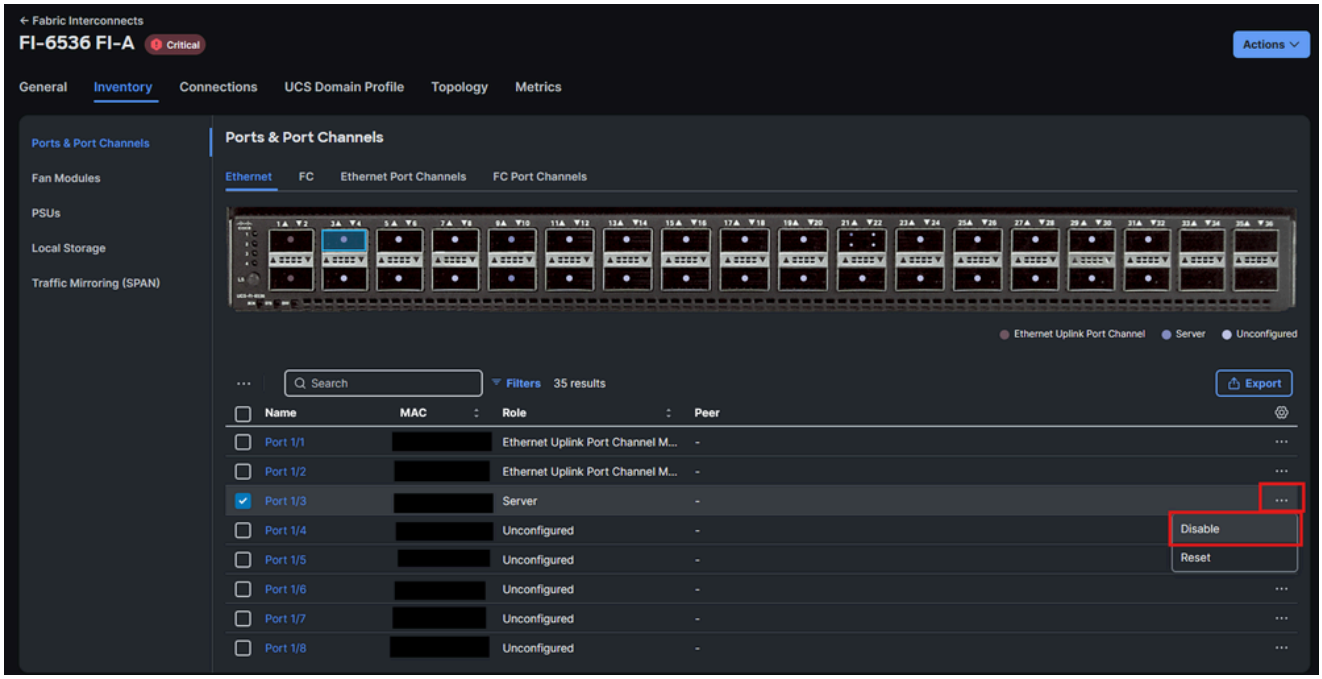
```
 capture-filter "
```

port 514

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

この例では、Syslogトラフィックを生成するために、Fabric Interconnect Aのサーバポートがフラップされました。

1. Fabric Interconnects > Inventoryの順に移動します。
2. 目的のポートのチェックボックスをクリックし、右側の省略記号メニューを開いてdisableを選択します。



テスト用のsyslogトラフィックを生成するためにFabric Interconnect上のインターフェイスをシャットダウンする

3. Fabric Interconnect上のコンソールでは、Syslogパケットをキャプチャする必要があります。

<#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. メッセージは、リモートサーバにログインしている必要があります。

<#root>

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

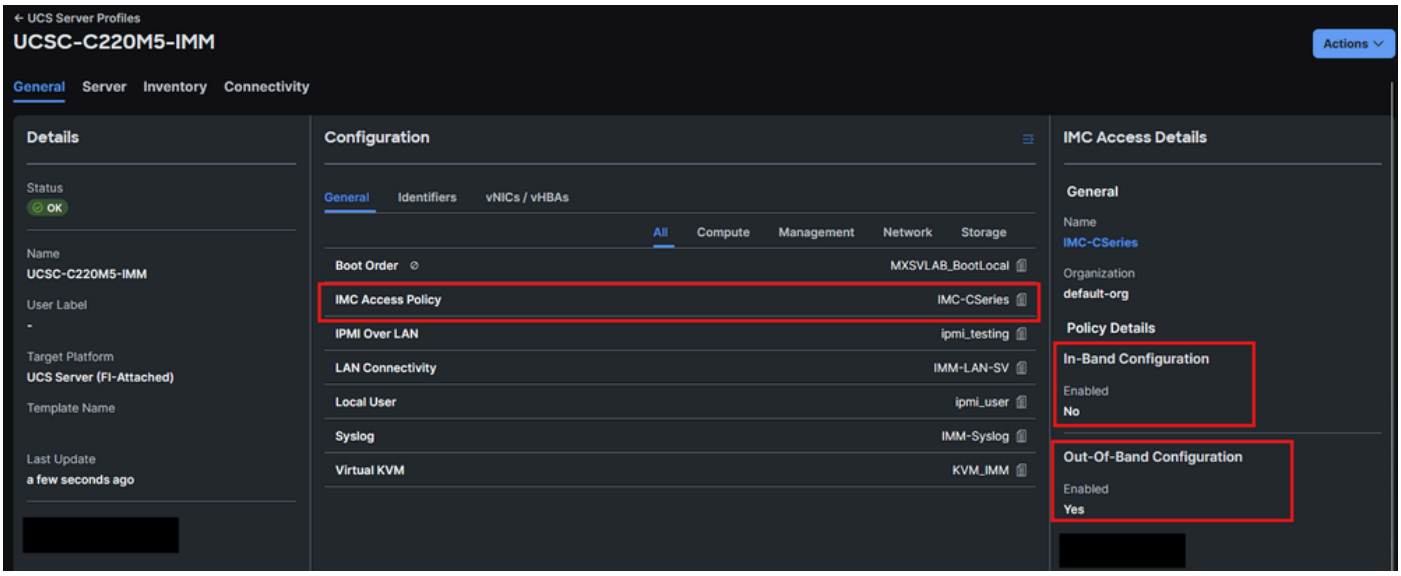
192.0.2.3

```
 : 2025 Jan 16 22:17:40 UTC:
```

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

同じテストをサーバでも実行できます。

注：この手順は、IMCアクセスポリシーでアウトオブバンド設定を行っているサーバでのみ機能します。インバンドを使用している場合は、代わりにリモートsyslogサーバでパケットキャプチャを実行するか、TACに連絡して内部debugコマンドを使用して実行します。



IMCアクセスポリシーの設定を確認します

この例では、C220 M5統合サーバのLEDロケータが有効になっています。これにはダウンタイムは必要ありません。

1. サーバにアウトオブバンドトラフィックを送信するFabric Interconnectを確認します。サーバIPは192.0.2.5であるため、Fabric Interconnect Aはその管理トラフィックを転送します（「セカンダリルート」とは、Fabric Interconnectがサーバ管理トラフィックのプロキシとして動作することを意味します）。

   <#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

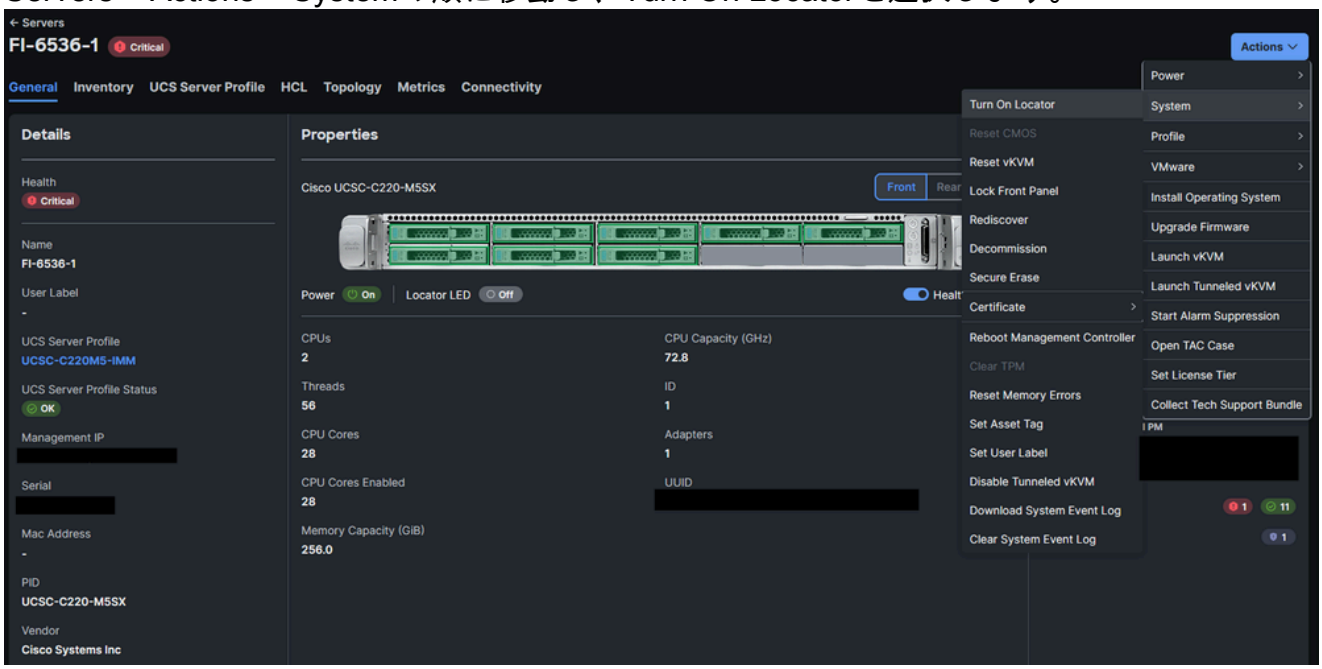
secondary route-preference

: 0, tag: 0

2. 該当するFabric Interconnectでパケットキャプチャを開始します。

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

3. Servers > Actions > Systemの順に移動し、Turn On Locatorを選択します。



サーバのLEDロケータをオンにする

4. Fabric Interconnect上のコンソールには、キャプチャされたSyslogパケットが表示される必要があります。

<#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メッセージは、リモートサーバのAUDIT.logファイルに記録する必要があります:

<#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パケットがUCSによって生成されたものの、syslogサーバがログに記録しなかった場合：

1. パケットキャプチャを使用して、パケットがリモートSyslogサーバに到着したことを確認します。
2. リモートSyslogサーバの設定を確認します（設定されたSyslogポートとファイアウォールの設定を含みますが、これに限定されません）。

関連情報

- RFC 5424 - Syslogプロトコル
- Intersight IMM Expertシリーズ – Syslogポリシー
- Cisco Intersightヘルプセンター – UCSドメインプロファイルポリシーの設定
- Cisco Intersightヘルプセンター – サーバーポリシーの設定

サーバのIMCアクセスポリシーにインバンドが設定されている場合、CIMCデバッグシェルをロードし、ラックの場合はbond0インターフェイス、ブレードの場合はbond0.xインターフェイス（xはVLAN）でパケットキャプチャを実行します。

```
[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)
```

- Syslogポート番号は、サーバ内のみで、ファブリックインターコネクト上では変更できません。これは設計上の問題であり、

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。