在UCS Intersight託管模式下配置並驗證系統日誌

目錄

簡介

本文檔介紹在Intersight管理模式UCS域上設定和驗證Syslog協定的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 整合運算系統(UCS)伺服器
- Intersight管理模式(IMM)
- 網路基本概念
- Syslog 通訊協定

採用元件

本檔案中的資訊是根據以下軟體版本：

- Intersight軟體即服務(SaaS)
- Cisco UCS 6536交換矩陣互聯，韌體4.3(5.240032)
- 機架式伺服器C220 M5，韌體4.3(2.240090)
- Alma Linux 9

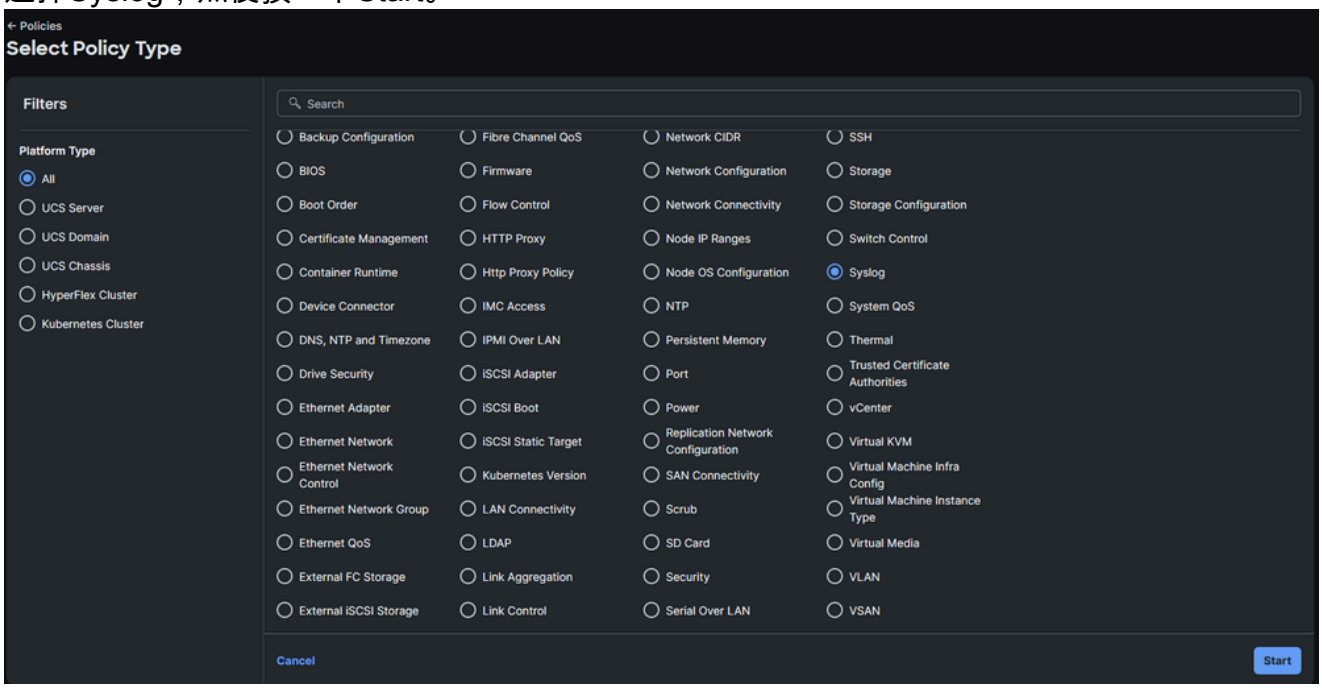
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

系統日誌策略適用於交換矩陣互聯和伺服器。它們允許配置本地和遠端日誌記錄。

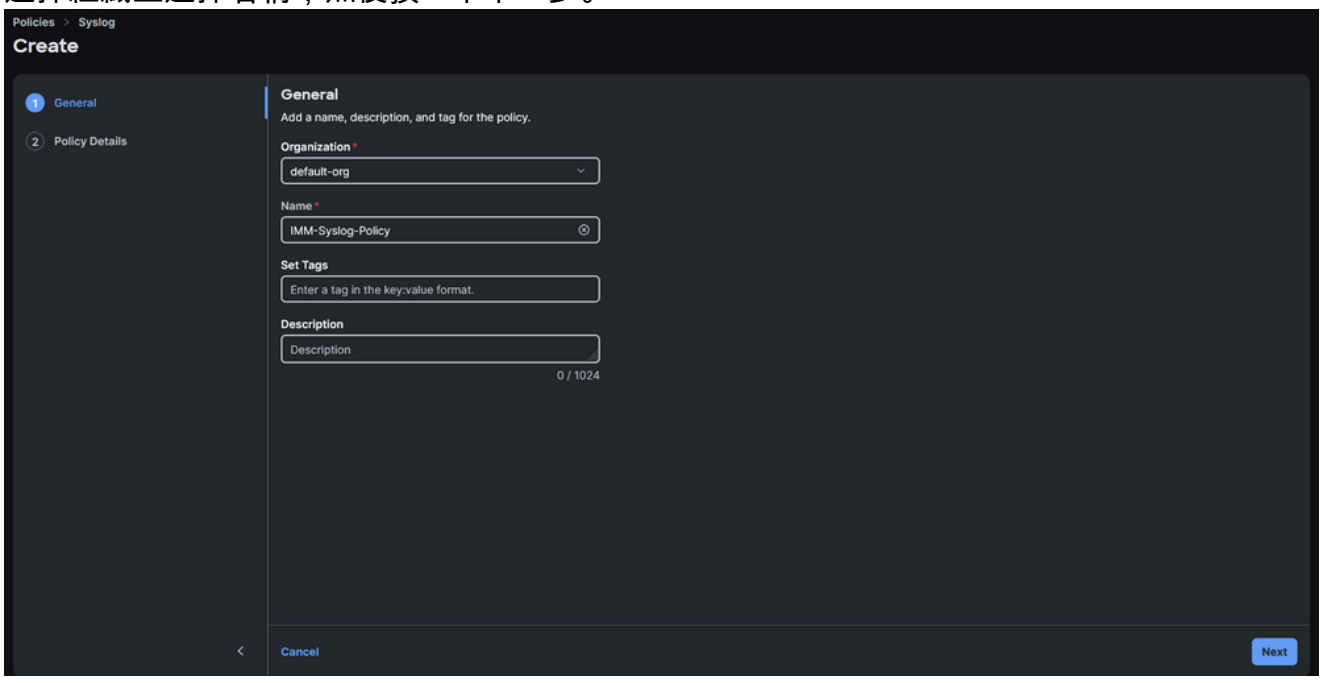
設定

1. 導航到Policies > Create new policy。
2. 選擇Syslog，然後按一下Start。



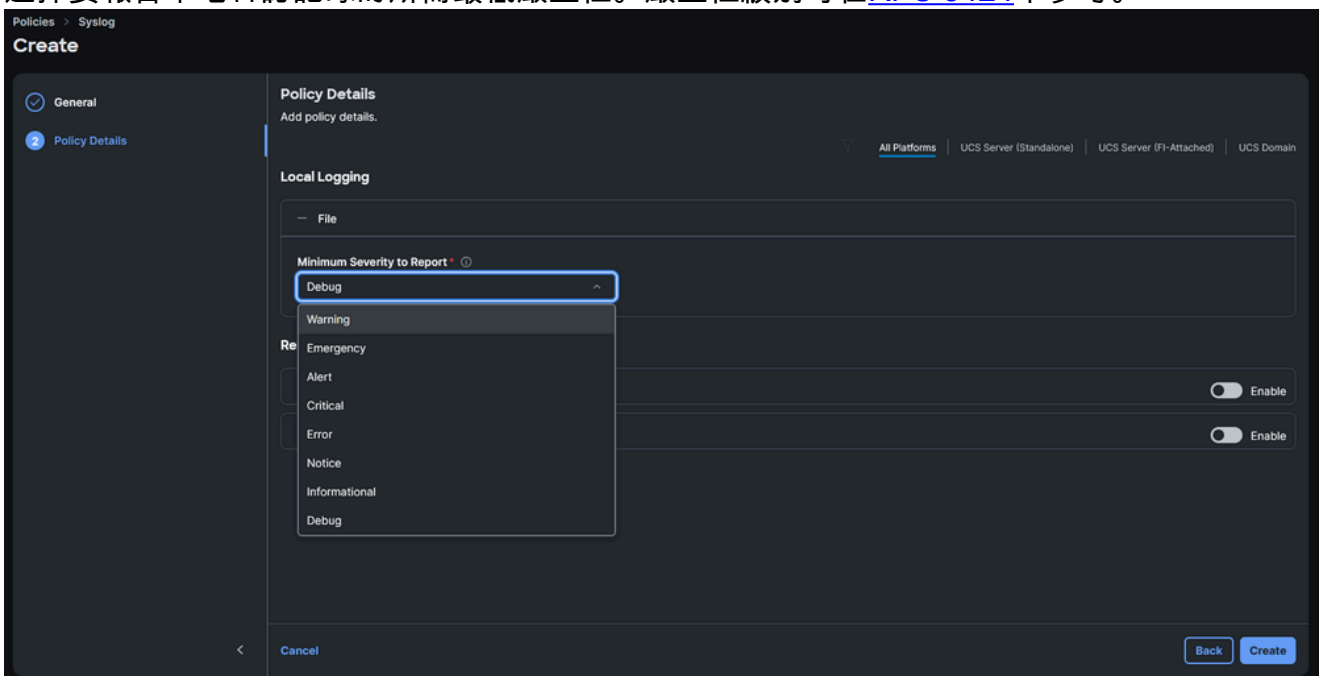
策略選擇

3. 選擇組織並選擇名稱，然後按一下下一步。



配置組織和名稱

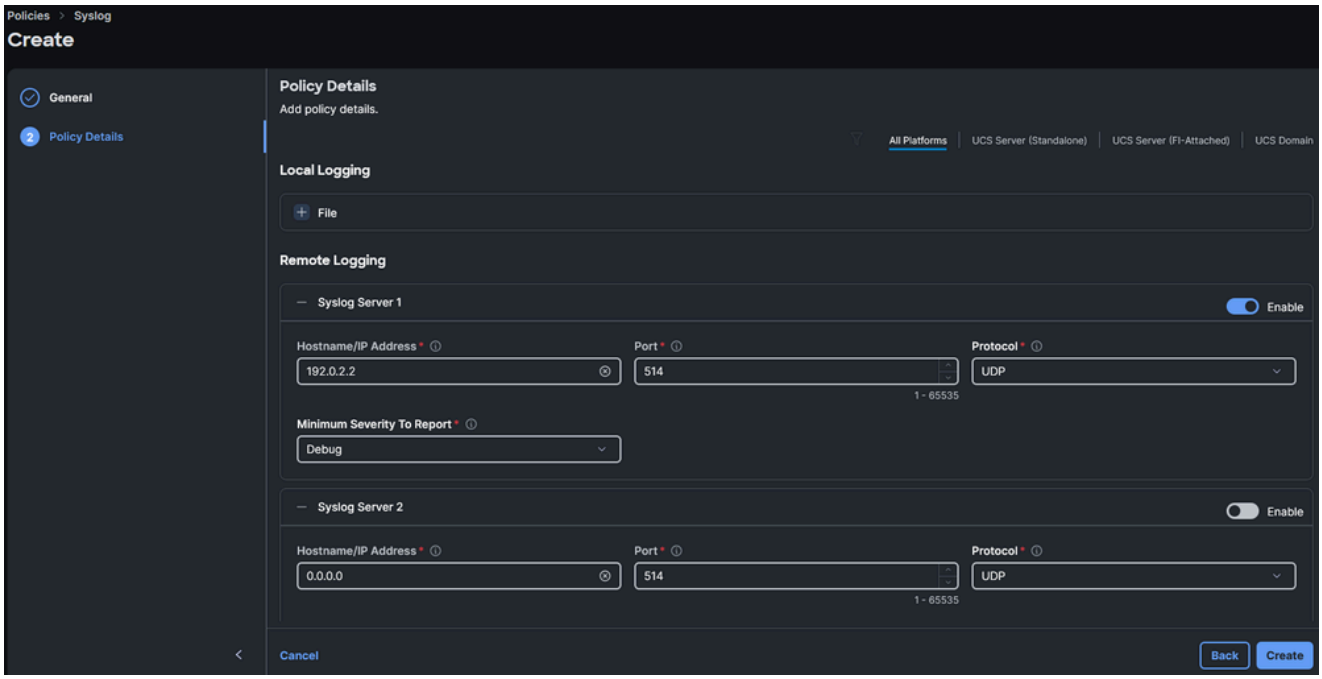
4. 選擇要報告本地日誌記錄的所需最低嚴重性。嚴重性級別可在RFC 5424中參考。



選擇要報告本地日誌記錄的最小嚴重性

5. 選擇要報告遠端日誌記錄的所需最低嚴重性和所需設定。這些是遠端伺服器的IP地址或主機名、埠號和埠協定（TCP或UDP）。

附註：此示例使用預設設定UDP埠514。雖然埠號可以更改，但它僅適用於伺服器。交換矩陣互聯設計使用預設埠514。

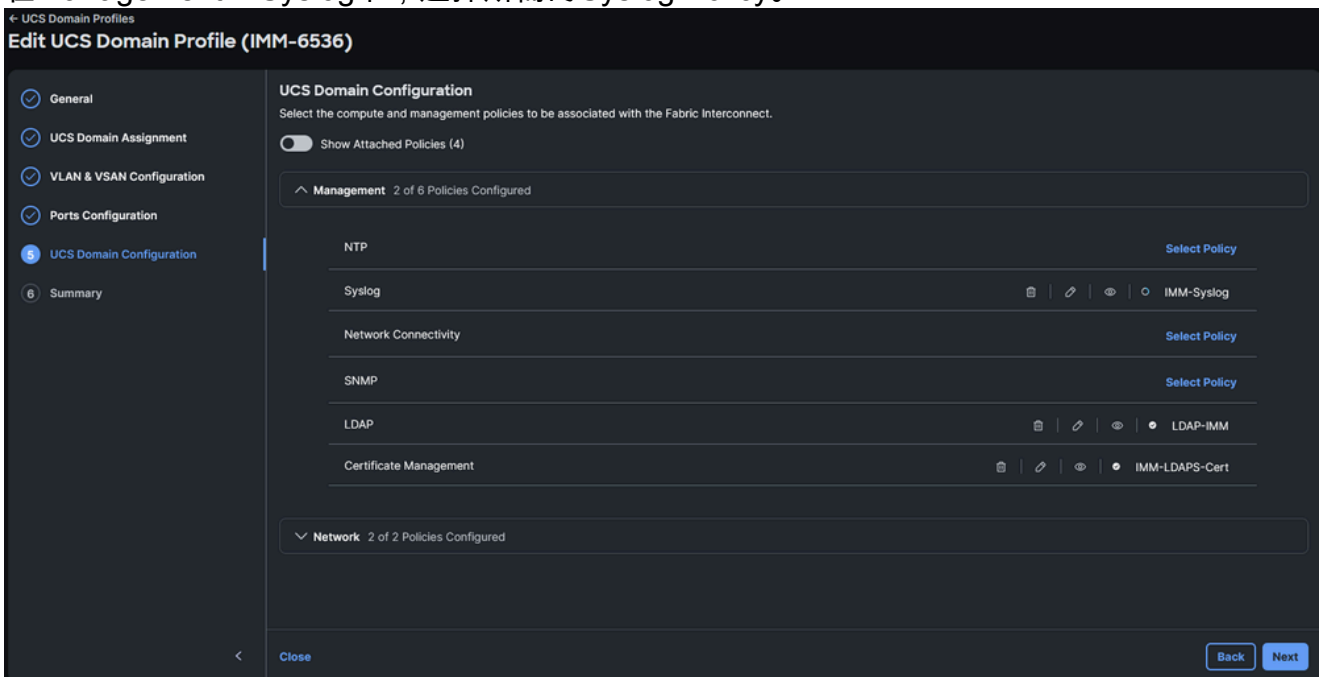


配置遠端日誌記錄引數

6. 按一下「Create」。
7. 將策略分配給所需的裝置。

光纖互連

1. 導航到Domain Profile（域配置檔案），按一下Edit，然後按一下Next（下一步），直到步驟4 UCS Domain Configuration。
2. 在Management > Syslog下，選擇所需的Syslog Policy。

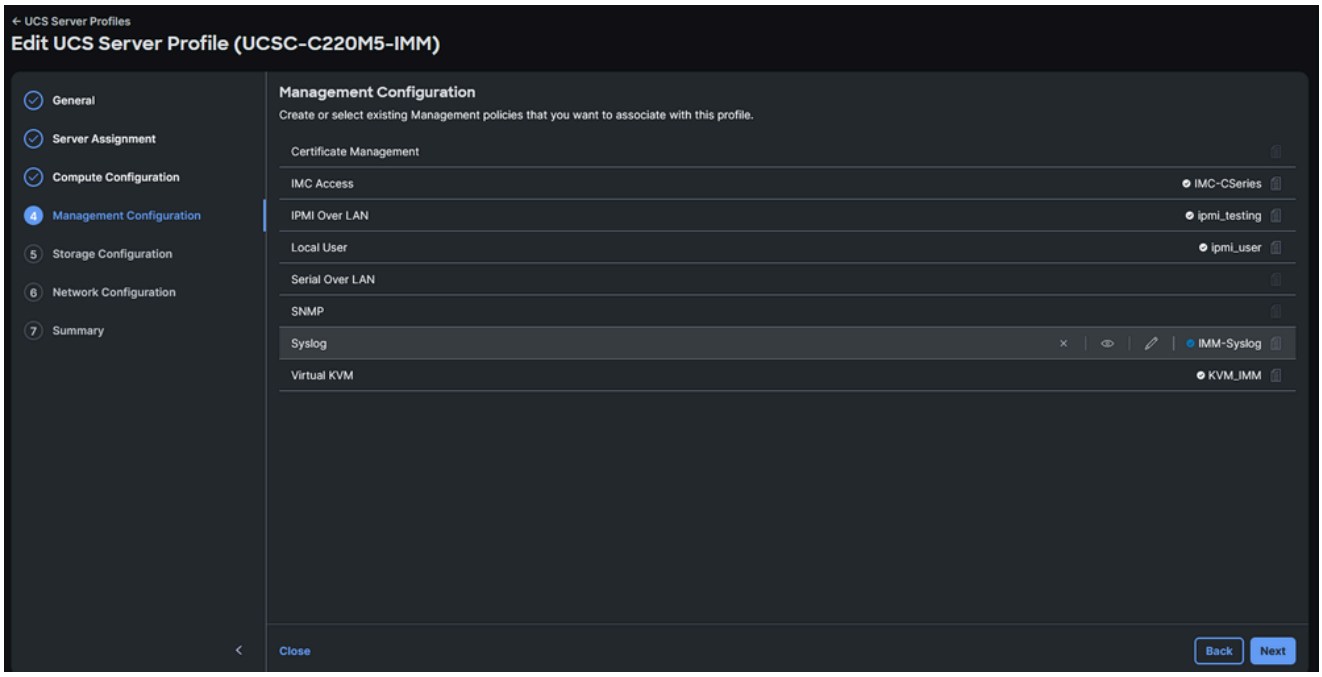


在交換矩陣互聯域配置檔案上選擇系統日誌策略

3. 按一下「Next」，「Deploy」。此策略的部署不會造成中斷。

伺服器

1. 導航到伺服器配置檔案，按一下Edit，然後轉到Next，直到步驟4 Management Configuration。
2. 選擇Syslog Policy。



在伺服器服務配置檔案上選擇系統日誌策略

3. 繼續直到最後一步並進行部署。

驗證

此時，系統日誌消息必須記錄在Syslog遠端伺服器上。 在本示例中，系統日誌伺服器部署在Linux伺服器上，其中包含rsyslog庫。

附註：系統日誌消息記錄的驗證可能因使用的遠端系統日誌伺服器而異。

確認遠端伺服器上記錄了交換矩陣互聯系統日誌消息：

```
[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
```

確認遠端伺服器上已記錄伺服器系統日誌消息：

```
[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
```

疑難排解

可以在交換矩陣互聯上執行資料包捕獲，以確認系統日誌資料包是否正確轉發。將報告的最低嚴重性更改為debug。確保系統日誌報告儘可能多的資訊。

從命令列介面，在管理埠上啟動資料包捕獲，然後按埠514（系統日誌埠）進行過濾：

<#root>

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

local interface mgmt

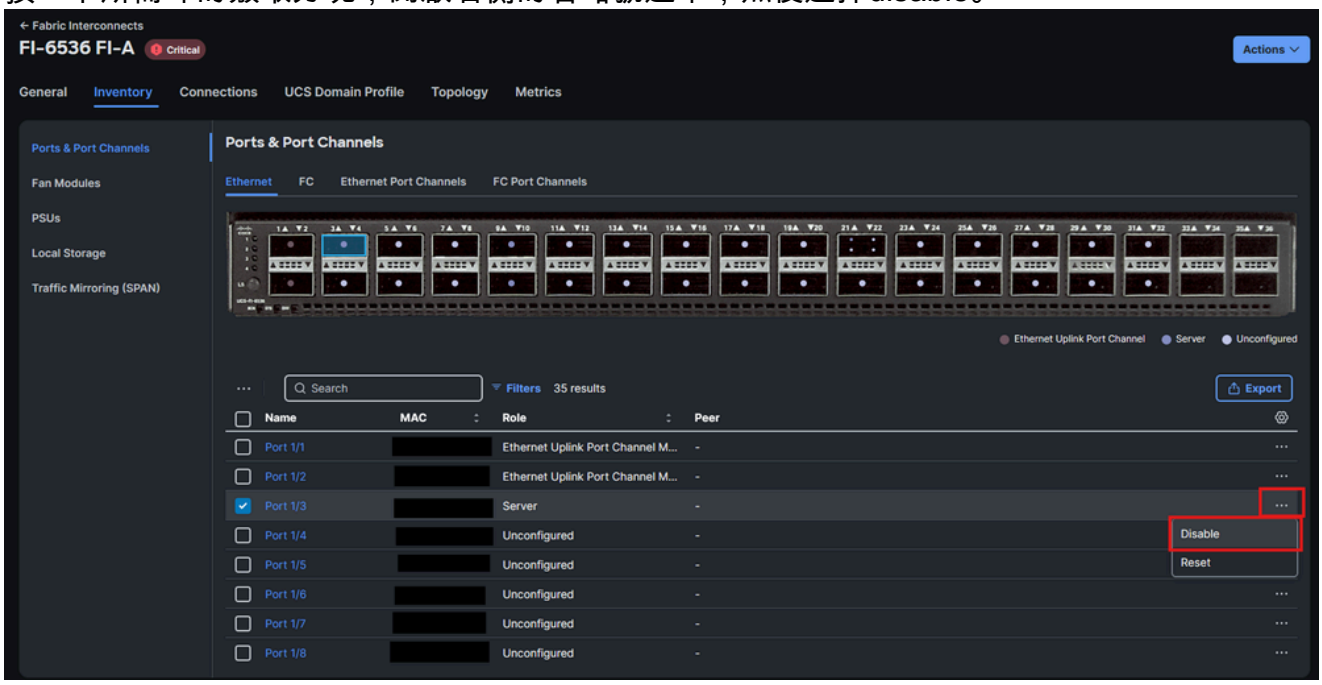
```
 capture-filter "
```

port 514

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

在本示例中，交換矩陣互聯A上的伺服器埠被拍動以生成系統日誌流量。

1. 導航到交換矩陣互聯>清單。
2. 按一下所需埠的覈取方塊，開啟右側的省略號選單，然後選擇disable。



關閉交換矩陣互聯上的介面以生成用於測試的系統日誌流量

3. 交換矩陣互聯上的控制檯必須捕獲Syslog資料包：

<#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. 必須在遠端伺服器中記錄該消息：

<#root>

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

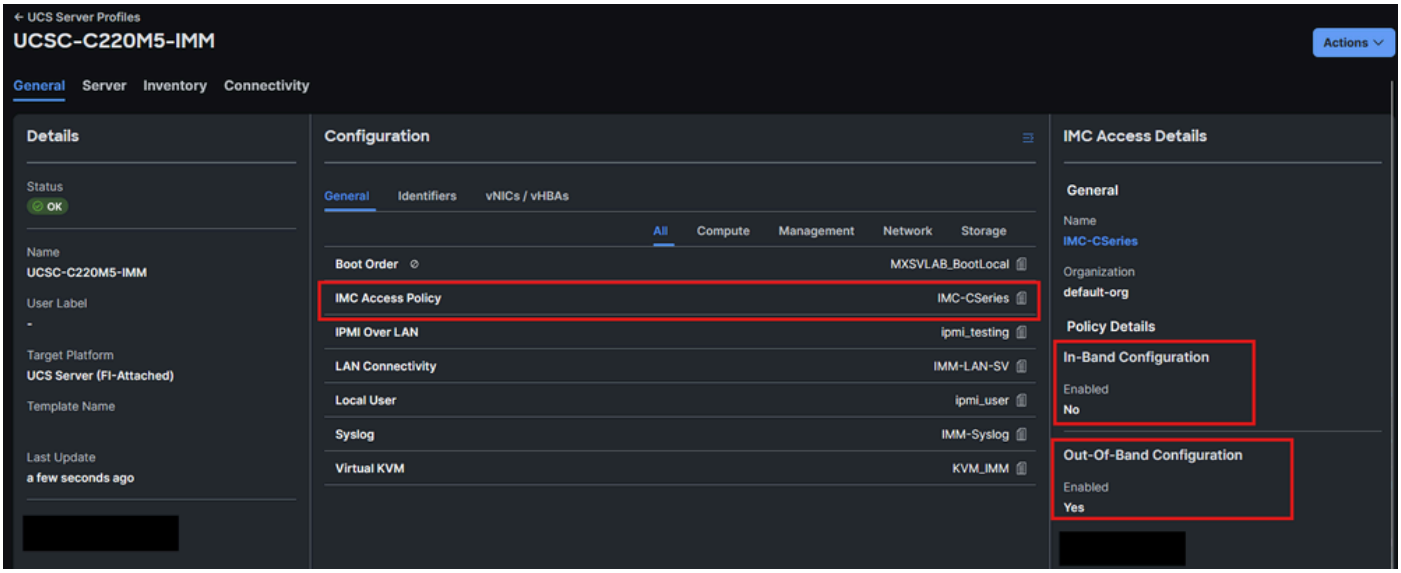
192.0.2.3

: 2025 Jan 16 22:17:40 UTC:

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

可以在伺服器上運行相同的測試：

> 附註：此過程僅適用於其IMC訪問策略中帶有帶外配置的伺服器。如果使用的是帶內，請在遠端Syslog伺服器上執行資料包捕獲，或聯絡TAC使用內部debug命令執行資料包捕獲。



驗證IMC訪問策略上的配置

在本示例中，啟用了C220 M5整合伺服器上的LED定位器。這不需要停機。

1. 驗證哪個交換矩陣互聯會為您的伺服器傳送帶外流量。伺服器IP是192.0.2.5，因此交換矩陣互聯A轉發其管理流量（「次要路由」表示交換矩陣互聯充當伺服器管理流量的代理）：

<#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

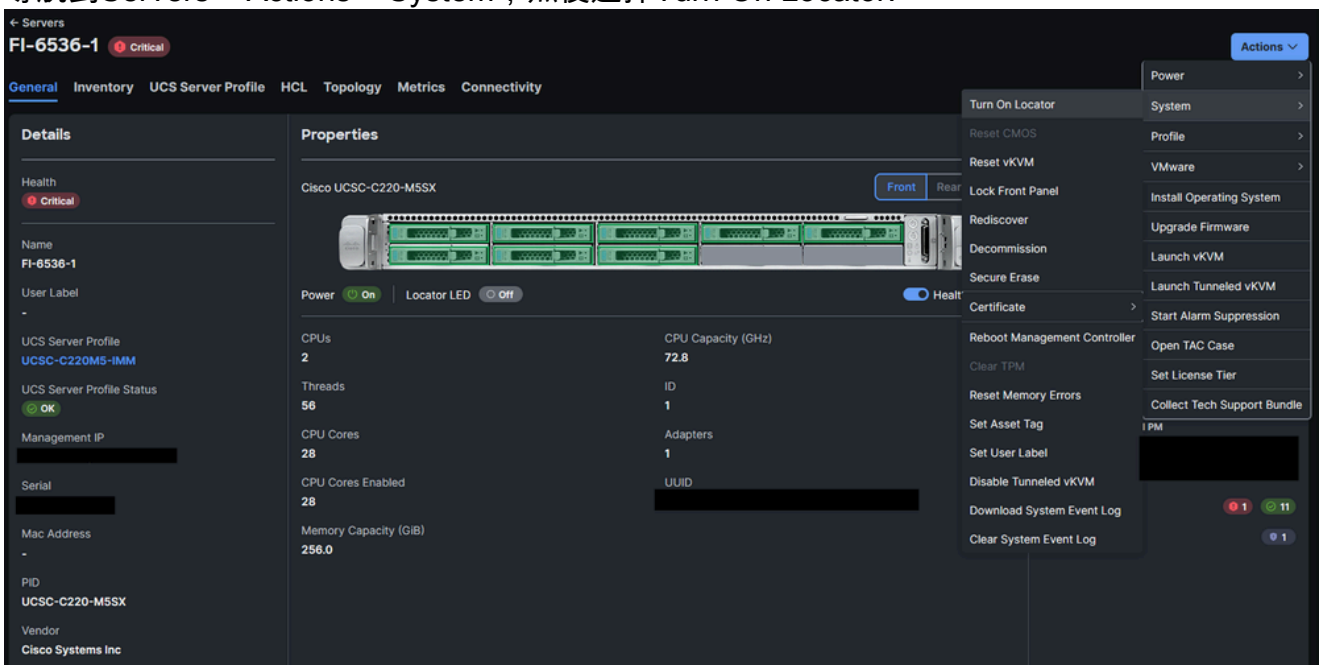
secondary route-preference

: 0, tag: 0

2. 在適當的交換矩陣互聯上開始資料包捕獲：

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

3. 導航到Servers > Actions > System，然後選擇Turn On Locator:



開啟伺服器中的LED定位器

4. 交換矩陣互聯上的控制檯必須顯示捕獲的系統日誌資料包：

<#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. 必須在遠端伺服器AUDIT.log檔案中記錄系統日誌消息:

<#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:
```

如果Syslog資料包由UCS生成，但Syslog伺服器沒有記錄這些資料包：

1. 確認資料包通過資料包捕獲到達遠端Syslog伺服器。
2. 驗證您的遠端Syslog伺服器的配置(包括但不限於：已配置系統日誌埠和防火牆設定)。

相關資訊

- RFC 5424 — 系統日誌協定
- Intersight IMM專家系列 — 系統日誌策略
- Cisco Intersight幫助中心 — 配置UCS域配置檔案策略
- Cisco Intersight幫助中心 — 配置伺服器策略

如果伺服器在其IMC訪問策略上配置了帶內，請載入CIMC調試外殼，並在機架的bond0介面或刀片的bond0.x介面（其中x是VLAN）上執行資料包捕獲。

```
[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)
```

- 不能在交換矩陣互聯上更改系統日誌埠號，只能在伺服器中更改。這是設計好的，記錄在

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。