

# 在UCS Intersight管理模式配置和验证系统日志

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[交换矩阵互联](#)

[服务器](#)

[验证](#)

[故障排除](#)

[相关信息](#)

---

## 简介

本文档介绍在Intersight托管模式UCS域上设置和验证系统日志协议的过程。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 统一计算系统(UCS)服务器
- Intersight管理模式(IMM)
- 网络基本概念
- 系统日志协议

### 使用的组件

本文档中的信息基于以下软件版本：

- Intersight软件即服务(SaaS)
- Cisco UCS 6536交换矩阵互联，固件4.3(5.240032)
- 机架式服务器C220 M5，固件4.3(2.240090)
- Alma Linux 9

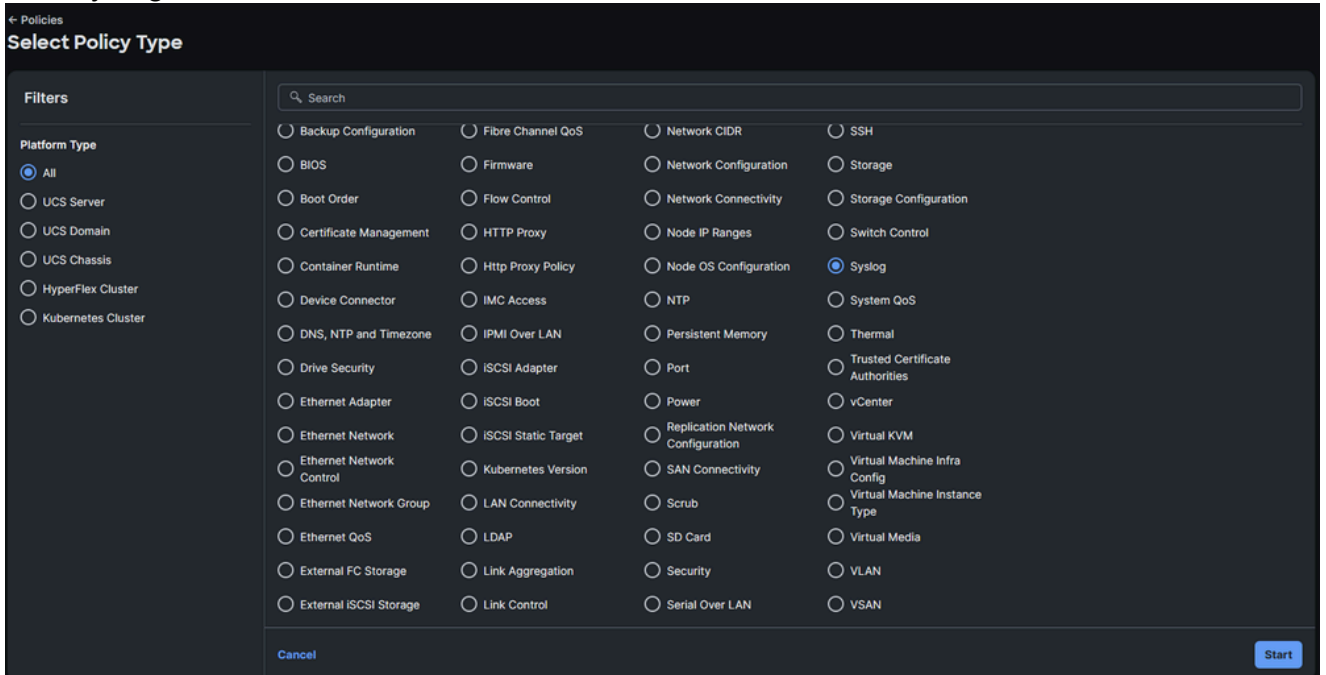
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 背景信息

系统日志策略适用于交换矩阵互联和服务器。它们允许配置本地和远程日志记录。

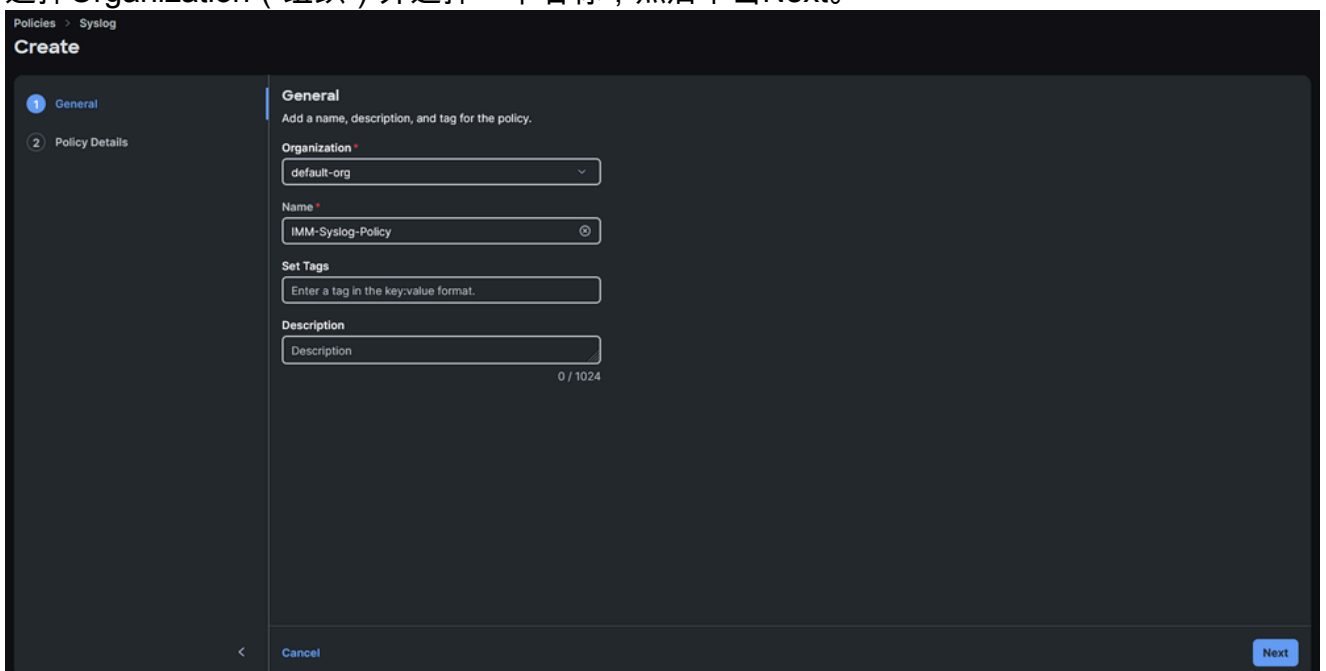
## 配置

1. 导航到Policies > Create new policy。
2. 选择Syslog，然后单击Start。



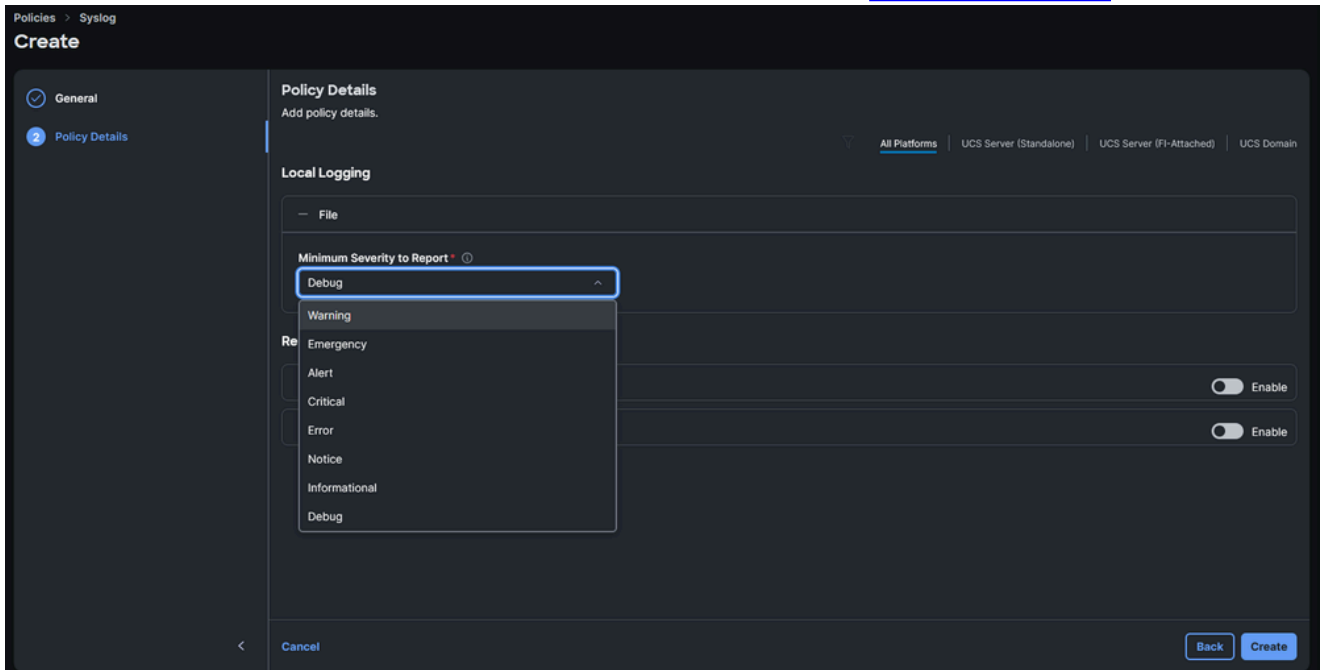
策略选择

3. 选择Organization (组织) 并选择一个名称，然后单击Next。




配置组织和名称

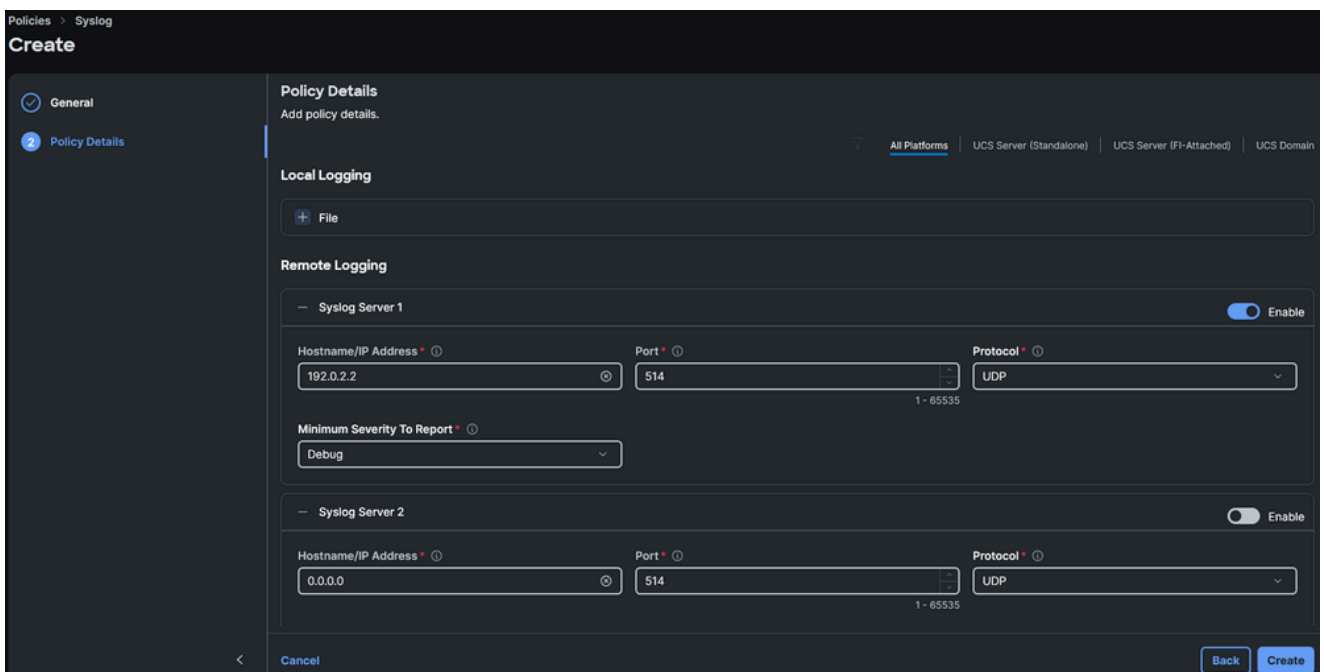
4. 选择要报告本地日志记录的所需最低严重性。严重性级别可在[RFC 5424](#)中引用。



选择要报告本地日志记录的最小严重性

5. 选择要报告远程日志记录的所需最低严重性，以及所需的设置。这些是远程服务器的IP地址或主机名、端口号和端口协议（TCP或UDP）。

 **注意：**此示例使用默认设置UDP端口514。虽然端口号可以更改，但它仅适用于服务器。交换矩阵互联在设计上使用默认端口514。

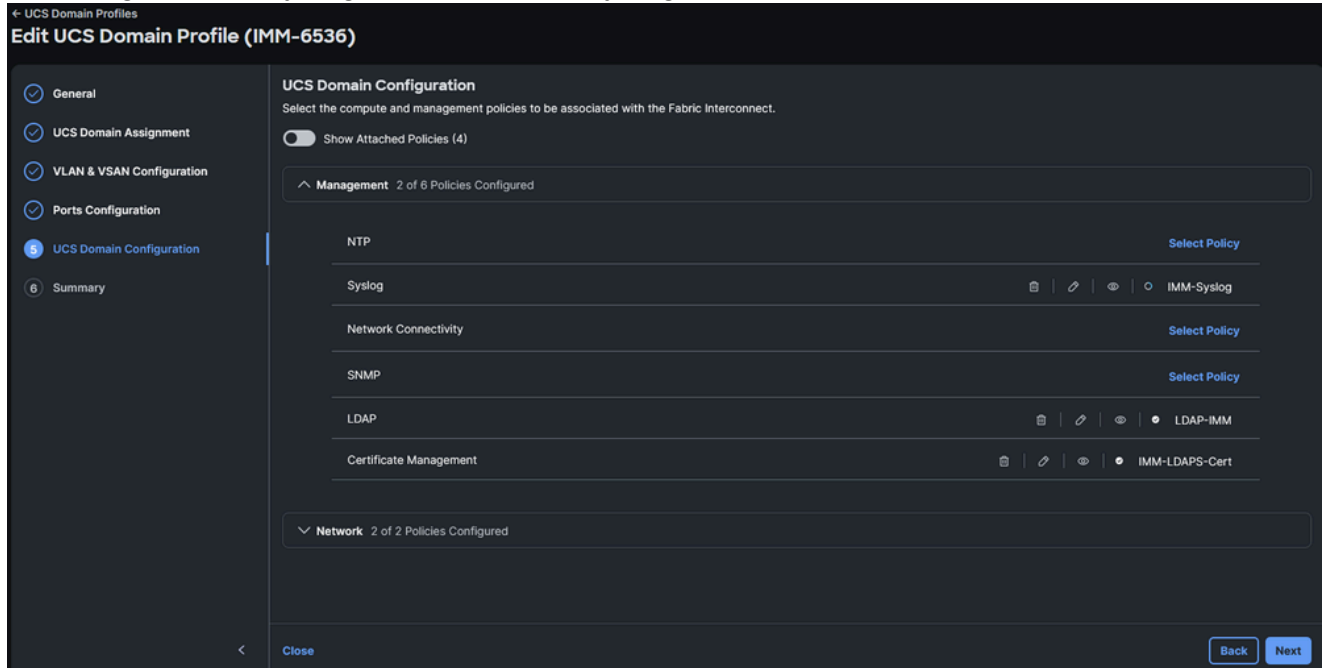


配置远程日志记录参数

6. Click Create.
7. 将策略分配给所需的设备。

## 交换矩阵互联

1. 导航到域配置文件，点击编辑，然后点击下一步，直到第4 UCS域配置。
2. 在Management > Syslog下，选择所需的Syslog策略。

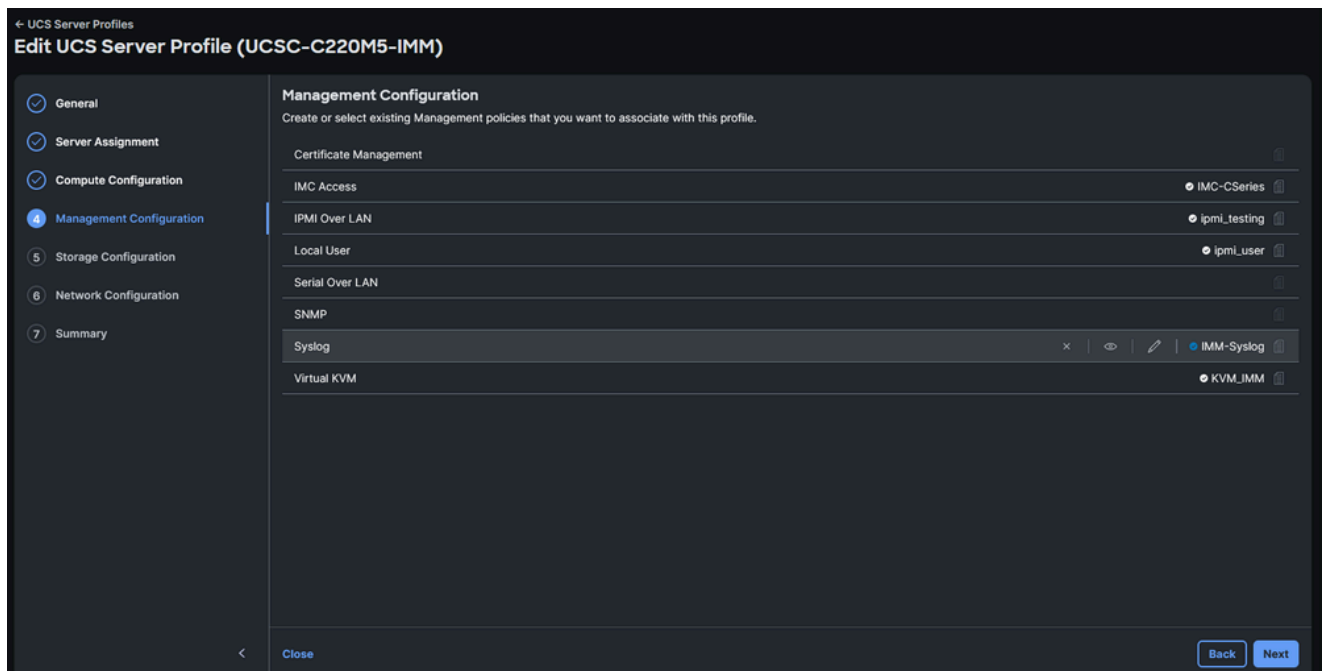


在交换矩阵互联域配置文件上选择系统日志策略

3. 单击下一步，然后单击部署。此策略的部署不会造成中断。

## 服务器

1. 导航到Server Profile，单击Edit，然后转到Next，直到第4步Management Configuration。
2. 选择Syslog Policy。




选择服务器服务配置文件上的系统日志策略

3. 继续到最后一步，然后部署。

## 验证

此时，必须在系统日志远程服务器上记录系统日志消息。在本示例中，系统日志服务器部署在 Linux 服务器上并带有 rsyslog 库。

 **注意：**系统日志消息日志记录的验证可能因使用的远程系统日志服务器而异。

确认远程服务器上记录了交换矩阵互联系统日志消息：

```
[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
```

确认服务器系统日志消息已记录在远程服务器上：

```
[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
```

# 故障排除

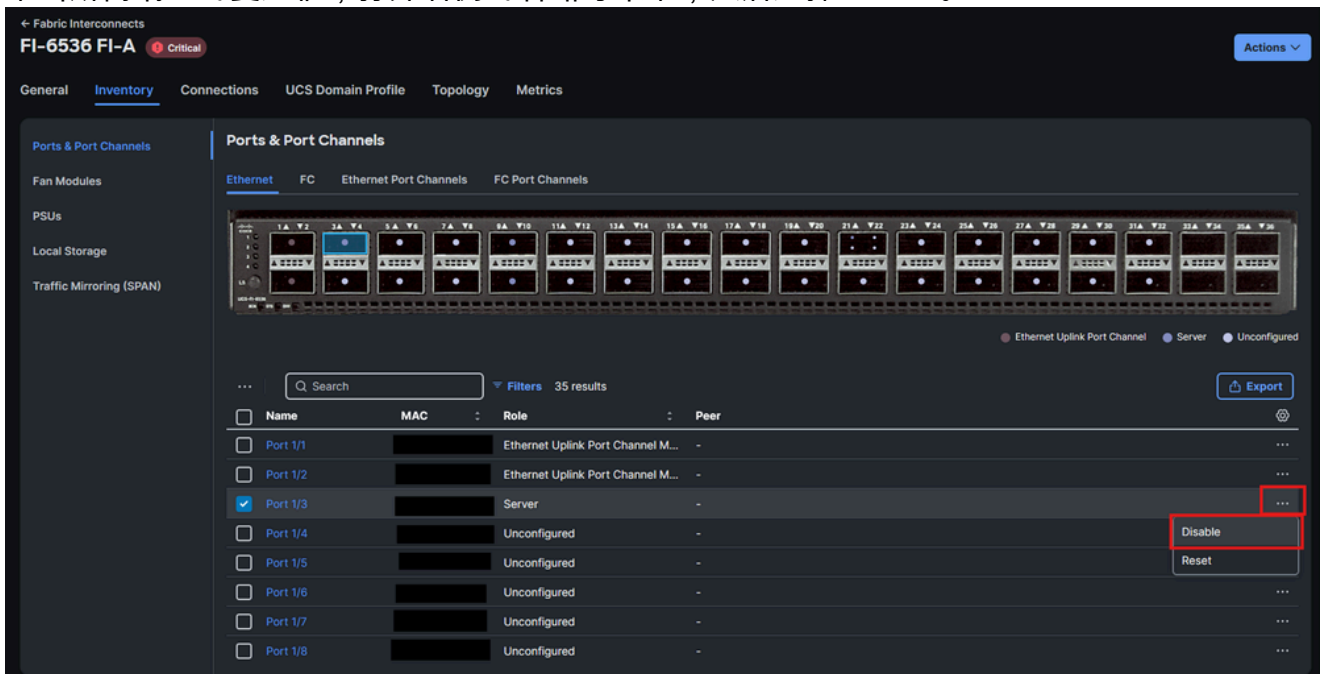
可以在交换矩阵互联上执行数据包捕获，以确认是否正确转发了Syslog数据包。将报告的最低严重性更改为debug。确保系统日志报告尽可能多的信息。

从命令行界面，在管理端口上开始数据包捕获，并按端口514 ( 系统日志端口 ) 过滤：

```
<#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，交换矩阵互联A上的服务器端口被交换以生成系统日志流量。

1. 导航到交换矩阵互联>资产。
2. 单击所需端口的复选框，打开右侧的省略号菜单，然后选择disable。



关闭交换矩阵互联上的接口以生成用于测试的系统日志流量

3. 交换矩阵互联上的控制台必须捕获系统日志数据包：

```
<#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. 消息必须记录在远程服务器中：

<#root>

```
[root@alma jormarqu]# tail -n 1 /var/log/remote/msg/192.0.2.3/_.log
```


Jan 16 17:15:03

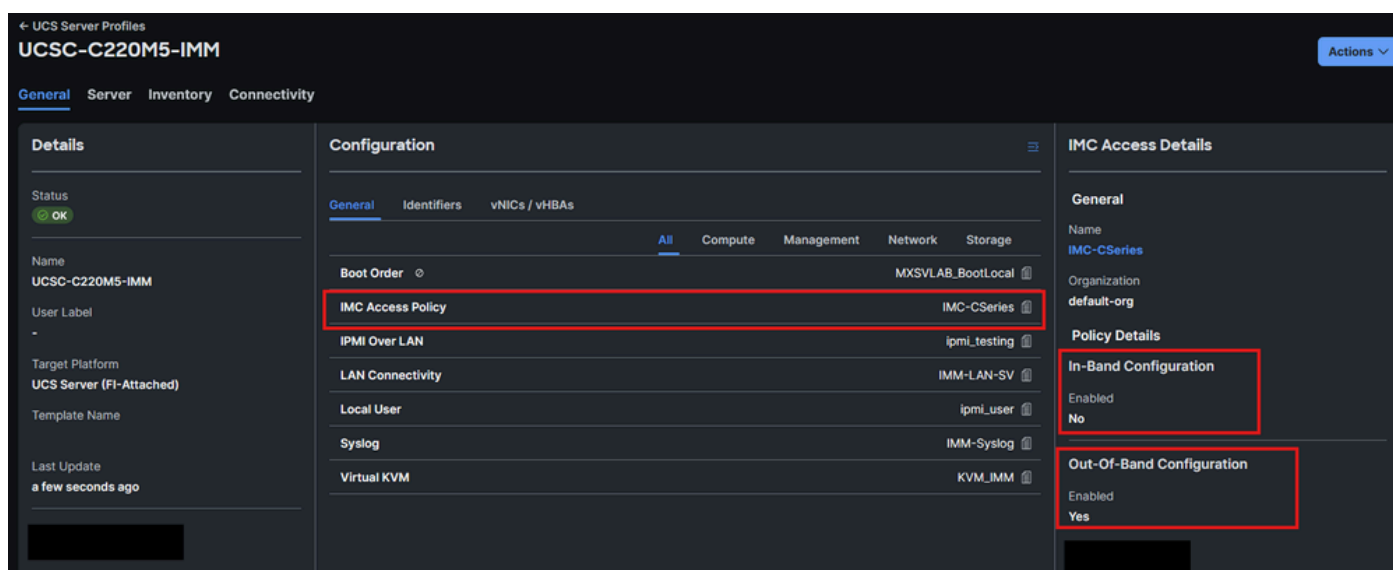
192.0.2.3

: 2025 Jan 16 22:17:40 UTC:

%ETHPORT-5-IF\_DOWN\_NONE: Interface Ethernet1/3 is down (Transceiver Absent)

可以在服务器上运行相同的测试：

 注意：此过程仅适用于在IMC访问策略中配置带外服务器。如果使用带内，请在远程系统日志服务器上执行数据包捕获，或联系TAC使用内部debug命令执行数据包捕获。



The screenshot displays the configuration page for a UCS Server Profile named UCSC-C220M5-IMM. The page is divided into several sections:

- Details:** Shows the status as OK, name as UCSC-C220M5-IMM, and target platform as UCS Server (FI-Attached).
- Configuration:** Contains a table of settings for various components. The 'IMC Access Policy' row is highlighted with a red box, showing it is set to 'IMC-CSeries'. Other rows include 'IPMI Over LAN' (ipmi\_testing), 'LAN Connectivity' (IMM-LAN-SV), 'Local User' (ipmi\_user), 'Syslog' (IMM-Syslog), and 'Virtual KVM' (KVM\_IMM).
- IMC Access Details:** Contains sub-sections for 'General' (Name: IMC-CSeries, Organization: default-org), 'Policy Details' (In-Band Configuration: No), and 'Out-Of-Band Configuration' (Enabled: Yes).

验证IMC访问策略上的配置

在本示例中，C220 M5集成服务器上的LED定位器已启用。这不需要停机。

1. 验证哪个交换矩阵互联为服务器发送带外流量。服务器IP为192.0.2.5，因此交换矩阵互联A会转发其管理流量（“辅助路由”意味着交换矩阵互联充当服务器管理流量的代理）：

```
<#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
```

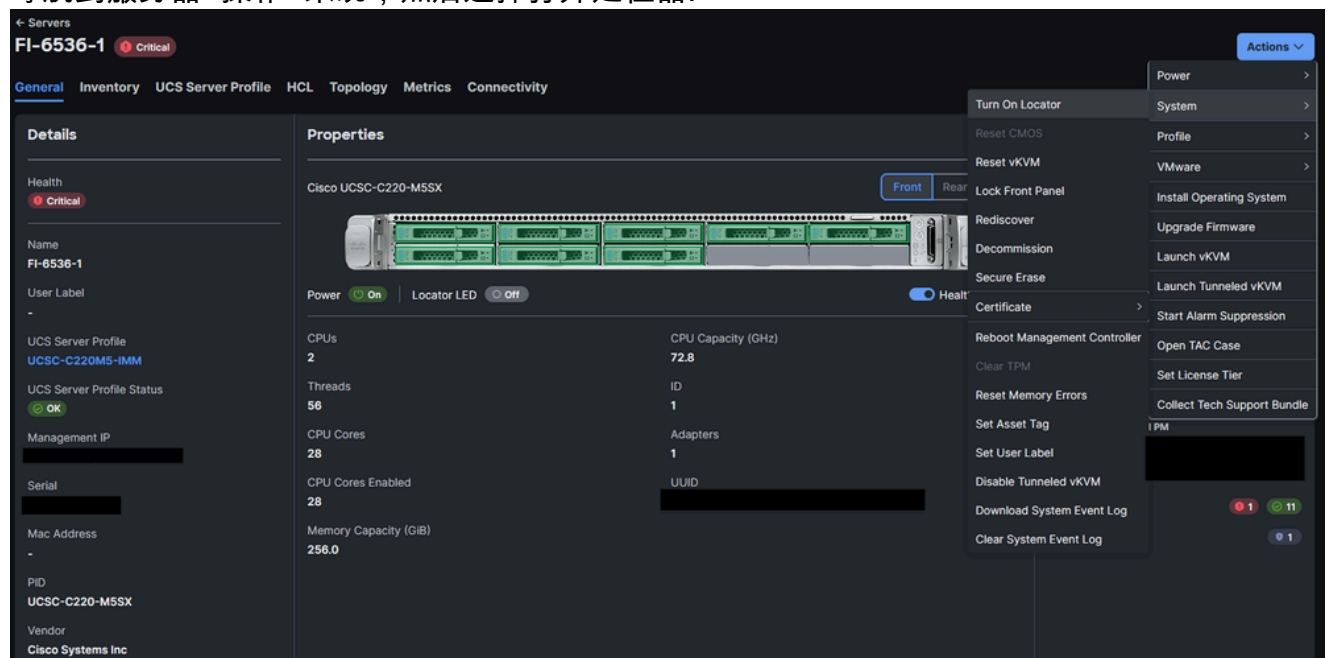
```
secondary route-preference
```

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

2. 在适当的交换矩阵互联上开始数据包捕获：

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

3. 导航到服务器>操作>系统，然后选择打开定位器：



打开服务器中的LED定位器

4. 交换矩阵互联上的控制台必须显示捕获的系统日志数据包：

```
<#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. 必须在远程服务器AUDIT.log文件中记录系统日志消息:

<#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数据包由UCS生成，但Syslog服务器未记录这些数据包：

1. 确认数据包通过数据包捕获到达远程系统日志服务器。
2. 验证远程系统日志服务器的配置(包括但不限于：已配置系统日志端口和防火墙设置)。

## 相关信息

- [RFC 5424 — 系统日志协议](#)
- [Intersight IMM专家系列 — 系统日志策略](#)
- [Cisco Intersight帮助中心 — 配置UCS域配置文件策略](#)
- [Cisco Intersight帮助中心 — 配置服务器策略](#)

如果服务器在其IMC访问策略上配置了带内，请加载CIMC debug shell并在机架的bond0接口或刀片的bond0.x接口（其中x是VLAN）上执行数据包捕获。

```
[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)
```

- 只能在服务器中更改交换矩阵互联上的系统日志端口号。这是根据设计进行的，记录在

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。