Configure and Verify Syslog on UCS Intersight Managed Mode

Contents

Introduction

This document describes the process to setup and verify the Syslog protocol on Intersight Managed Mode UCS Domains.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Unified Computing System (UCS) Servers
- Intersight Managed Mode (IMM)
- Networking basic concepts
- Syslog protocol

Components Used

The information in this document is based on these software versions:

- Intersight software as a service (SaaS)
- Cisco UCS 6536 Fabric Interconnect, firmware 4.3(5.240032)
- Rack Server C220 M5, firmware 4.3(2.240090)
- Alma Linux 9

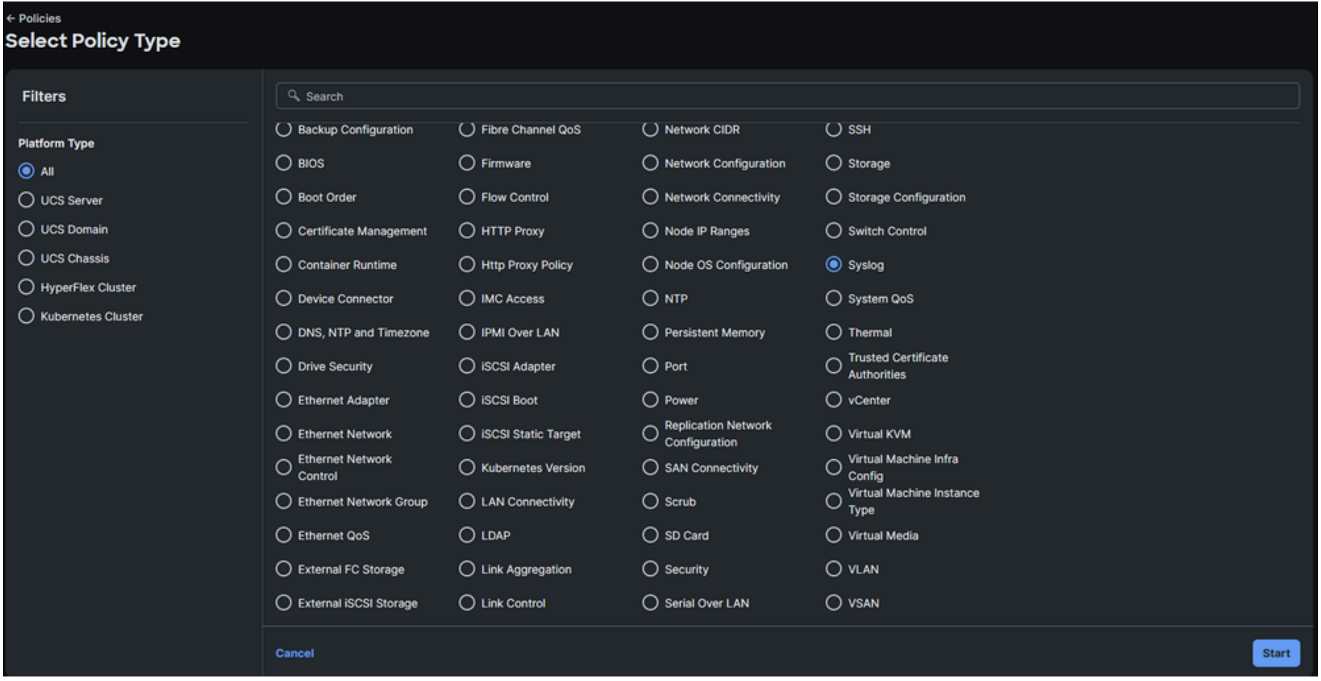
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Syslog policies are applicable for Fabric Interconnects and Servers. They allow for configuration of local and remote logging.

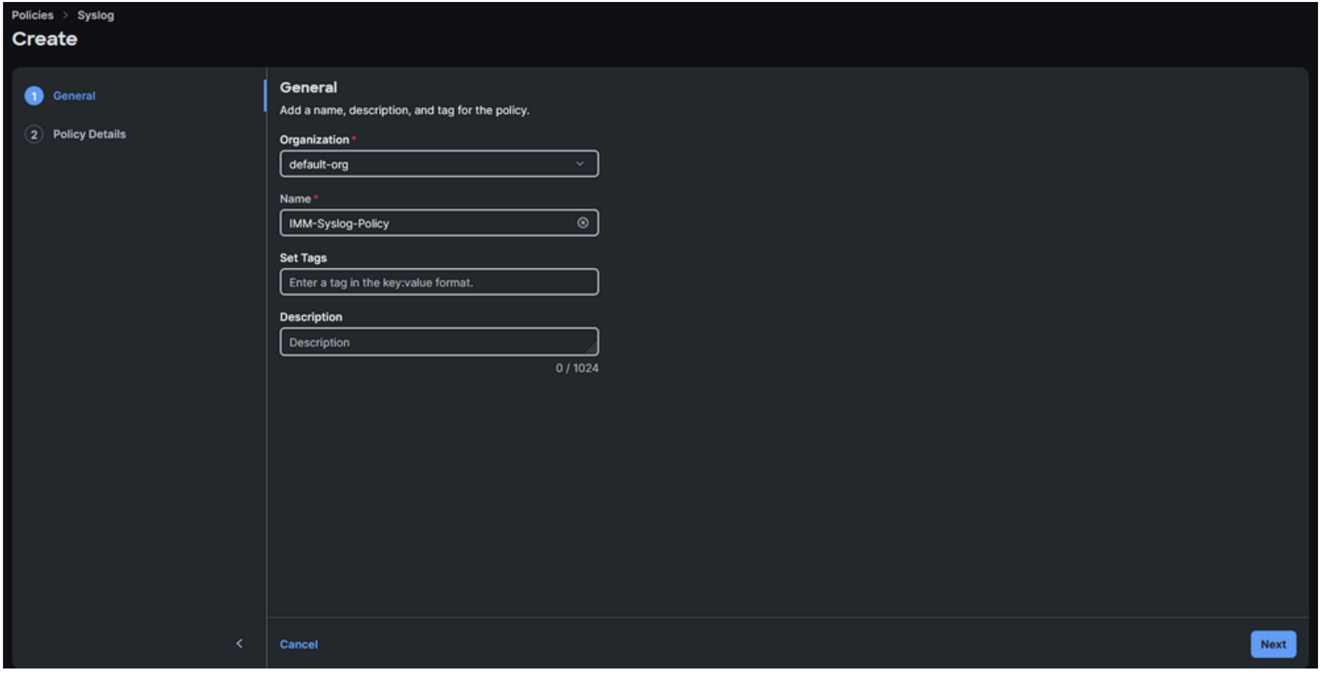
Configure

1. Navigate to **Policies** > **Create new policy**.
2. Choose **Syslog**, then click **Start**.



Policy selection

3. Choose the Organization and choose a name, then click **Next**.

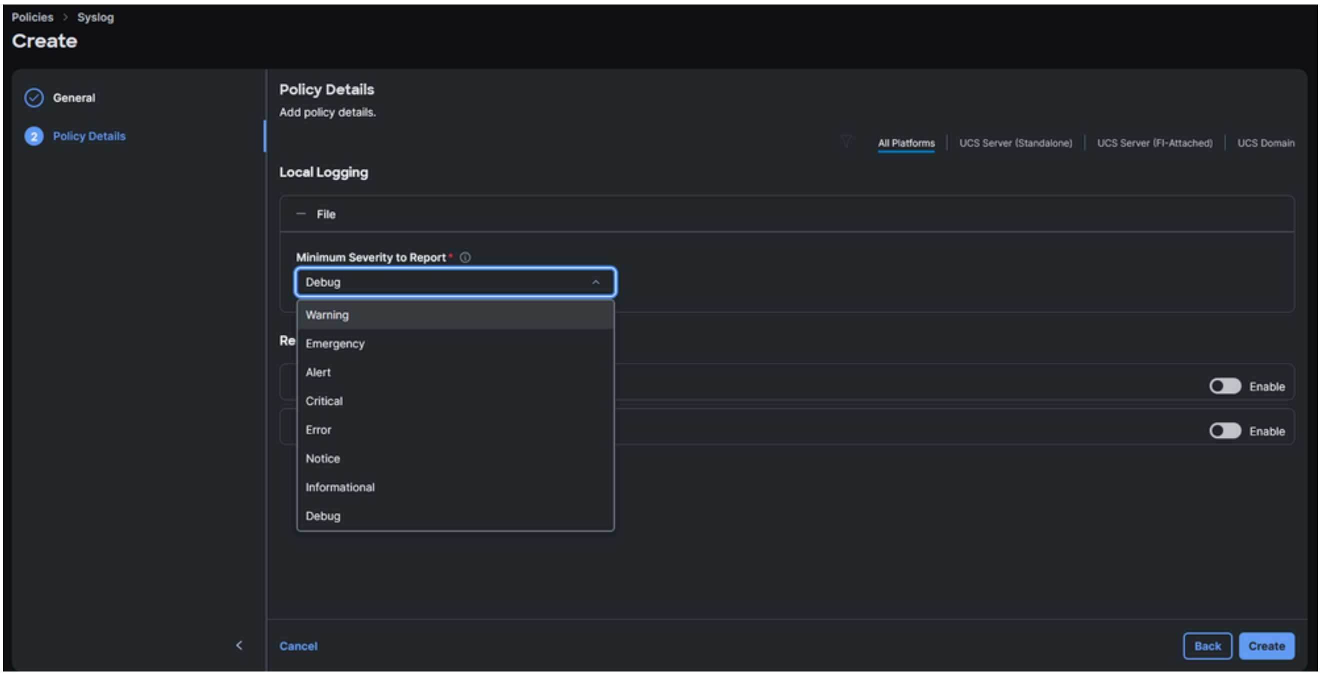


Organization * default-org

Name * IMM-Syslog-Policy

Configure organization and name

4. Choose the desired minimum severity to report for Local Logging. Severity levels can be referenced on RFC 5424.

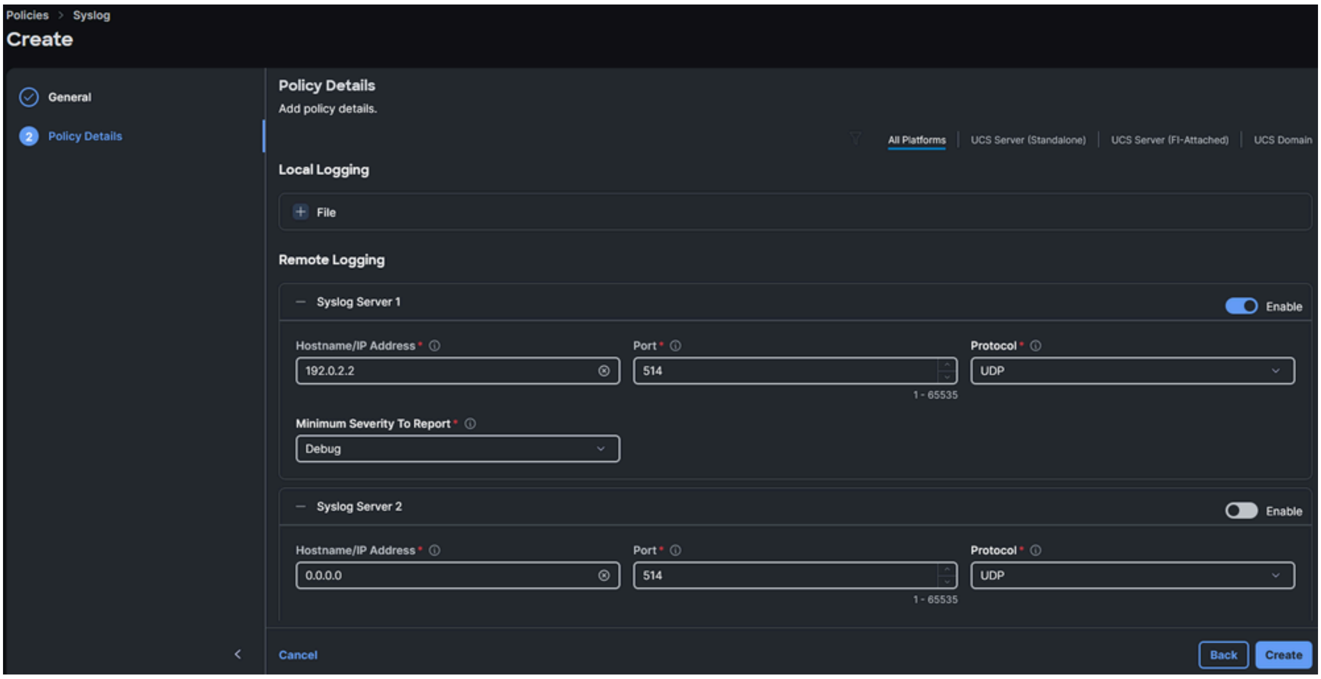


Minimum Severity to Report * Debug

Choose the minumum severity to report for Local Logging

5. Choose the desired minimum severity to report for Remote Logging, and the required settings. These are the remote server(s) IP address or hostname, the port number, and the port protocol (TCP or UDP).

Note: This example uses the default setting UDP port 514. While the port number can be changed, **this only applies to Servers**. Fabric Interconnects use the default port 514 by design.



Syslog Server 1 — Enable

Hostname/IP Address * 192.0.2.2

Port * 514 (1 - 65535)

Protocol * UDP

Minimum Severity To Report * Debug

Syslog Server 2 — Enable

Hostname/IP Address * 0.0.0.0

Port * 514 (1 - 65535)

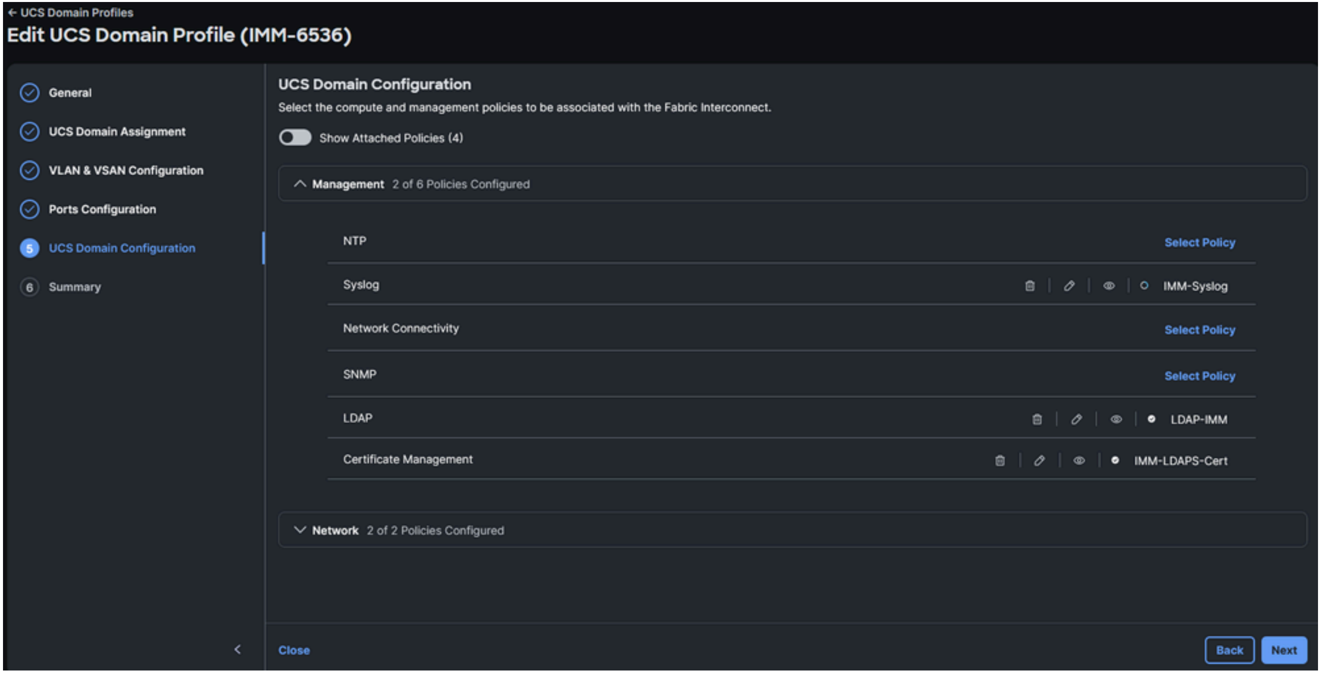
Protocol * UDP

Configure Remote Logging parameters

6. Click **Create**.
7. Assign the Policy to the desired devices.

Fabric Interconnects

1. Navigate to the Domain Profile, click **Edit**, then click **Next** until step 4 **UCS Domain Configuration**.
2. Under **Management > Syslog,** choose the desired Syslog Policy.



Edit UCS Domain Profile (IMM-6536)

UCS Domain Configuration

Select the compute and management policies to be associated with the Fabric Interconnect.

Show Attached Policies (4)

Management 2 of 6 Policies Configured

NTP	Select Policy
Syslog	IMM-Syslog
Network Connectivity	Select Policy
SNMP	Select Policy
LDAP	LDAP-IMM
Certificate Management	IMM-LDAPS-Cert

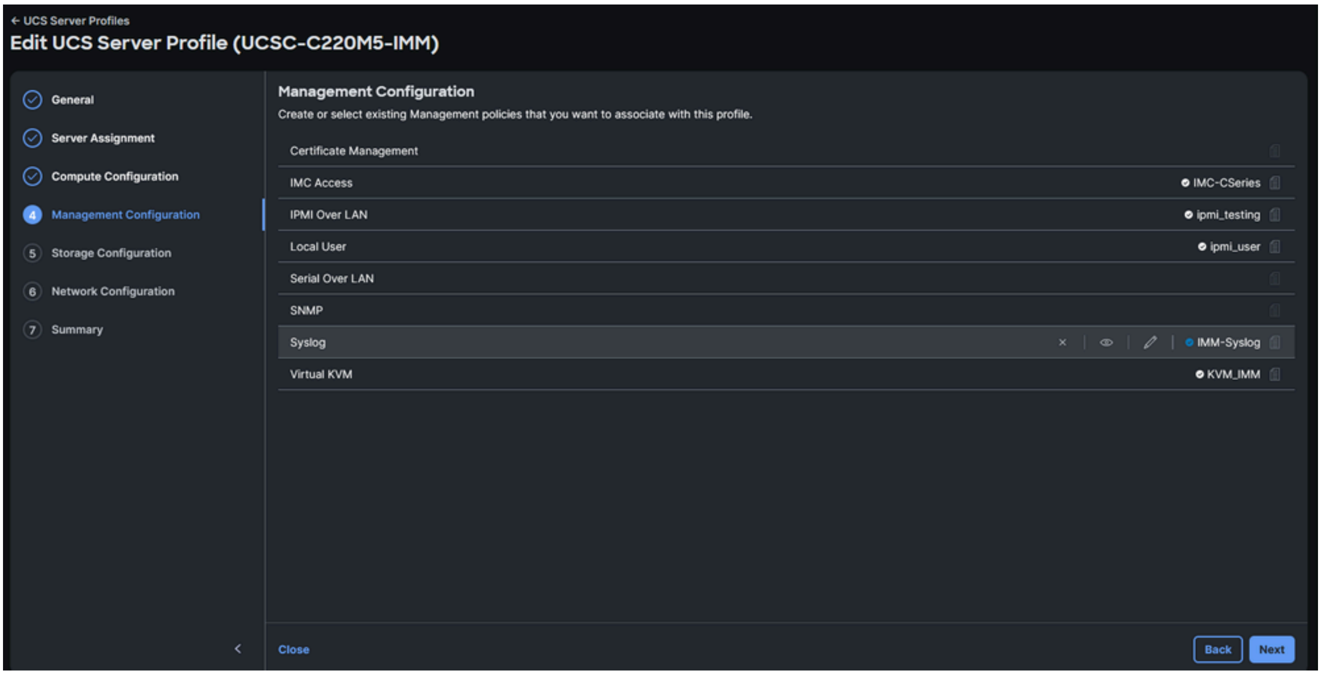
Network 2 of 2 Policies Configured

Choose the syslog policy on a Fabric Interconnect Domain Profile

3. Click **Next,** then **Deploy.** The deployment of this policy is not disruptive.

Servers

1. Navigate to the Server Profile, click **Edit**, then go **Next** until step 4 **Management Configuration**.
2. Choose the Syslog Policy.



Edit UCS Server Profile (UCSC-C220M5-IMM)

Management Configuration

Create or select existing Management policies that you want to associate with this profile.

Certificate Management

IMC Access: IMC-CSeries

IPMI Over LAN: ipmi_testing

Local User: ipmi_user

Serial Over LAN

SNMP

Syslog: IMM-Syslog

Virtual KVM: KVM_IMM

Choose the syslog policy on a Server Service Profile

3. Continue until the last step and **Deploy**.

Verify

At this point, Syslog messages must be logged on the Syslog remote server(s). For this example, the Syslog server was deployed on a Linux server with the rsyslog library.

Note: Verification of the Syslog messages logging can differ depending based on the remote Syslog server in use.

Confirm that the Fabric Interconnects Syslog messages were logged on the remote server:

```
[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
```

Confirm that the Servers Syslog messages were logged on the remote server:

```
[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) f
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 Inte
Jan 16 20:16:27 192.0.2.5 AUDIT[2257]: Secured Remote Syslog with(serverId =1, secure_enabled =0) by Use
```

Troubleshoot

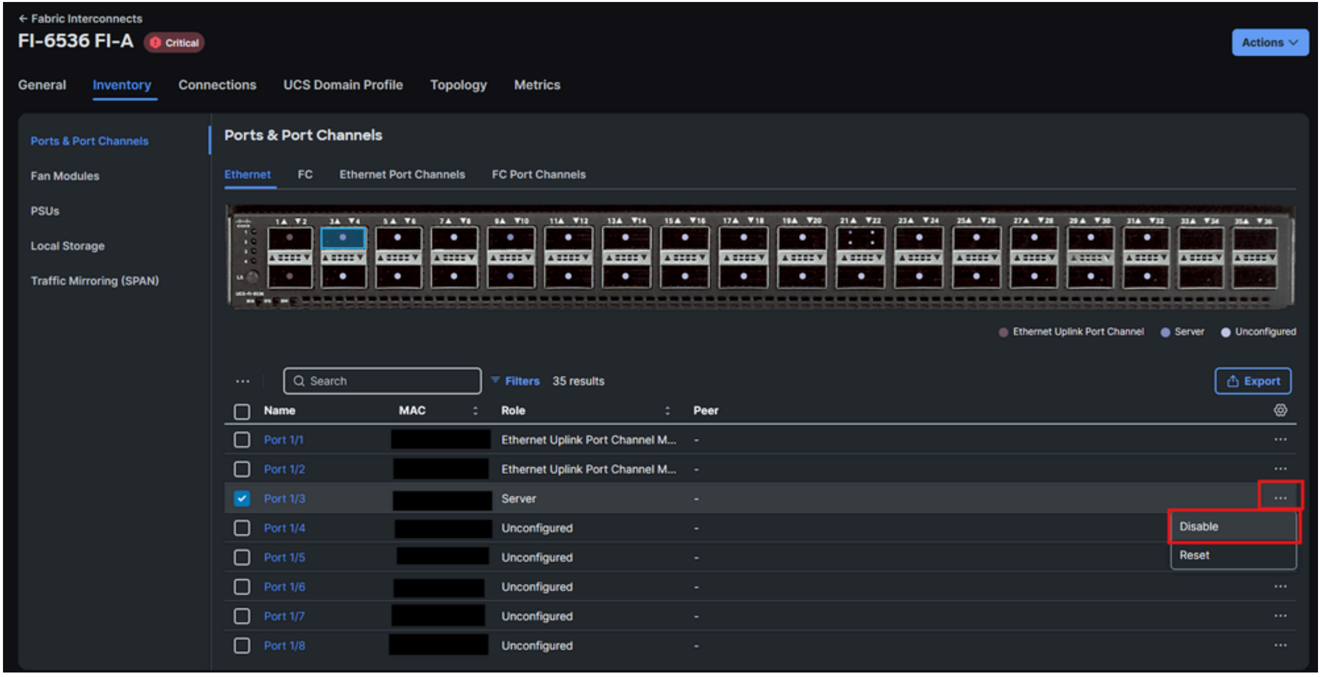
A packet capture can be performed on the Fabric Interconnects to confirm if the Syslog packets were forwarded correctly. Change the minimum severity to report to **debug**. Ensure Syslog reports as much information as possible.

From the command line interface, start a packet capture on the management port and filter by port 514 (Syslog port):

```
<#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 this example, a server port on Fabric Interconnect A was flapped to generate Syslog traffic.

1. Navigate to **Fabric Interconnects > Inventory**.
2. Click the checkbox for the desired port, open the ellipsis menu on the right, and choose **disable**.



☐	Name	MAC	Role	Peer
☐	Port 1/1	[redacted]	Ethernet Uplink Port Channel M...	-
☐	Port 1/2	[redacted]	Ethernet Uplink Port Channel M...	-
☑	Port 1/3	[redacted]	Server	-
☐	Port 1/4	[redacted]	Unconfigured	-
☐	Port 1/5	[redacted]	Unconfigured	-
☐	Port 1/6	[redacted]	Unconfigured	-
☐	Port 1/7	[redacted]	Unconfigured	-
☐	Port 1/8	[redacted]	Unconfigured	-

Shut down an interface on an Fabric Interconnect to generate syslog traffic for testing

3. The console on the Fabric Interconnect must capture the Syslog packet:

```
<#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)
```

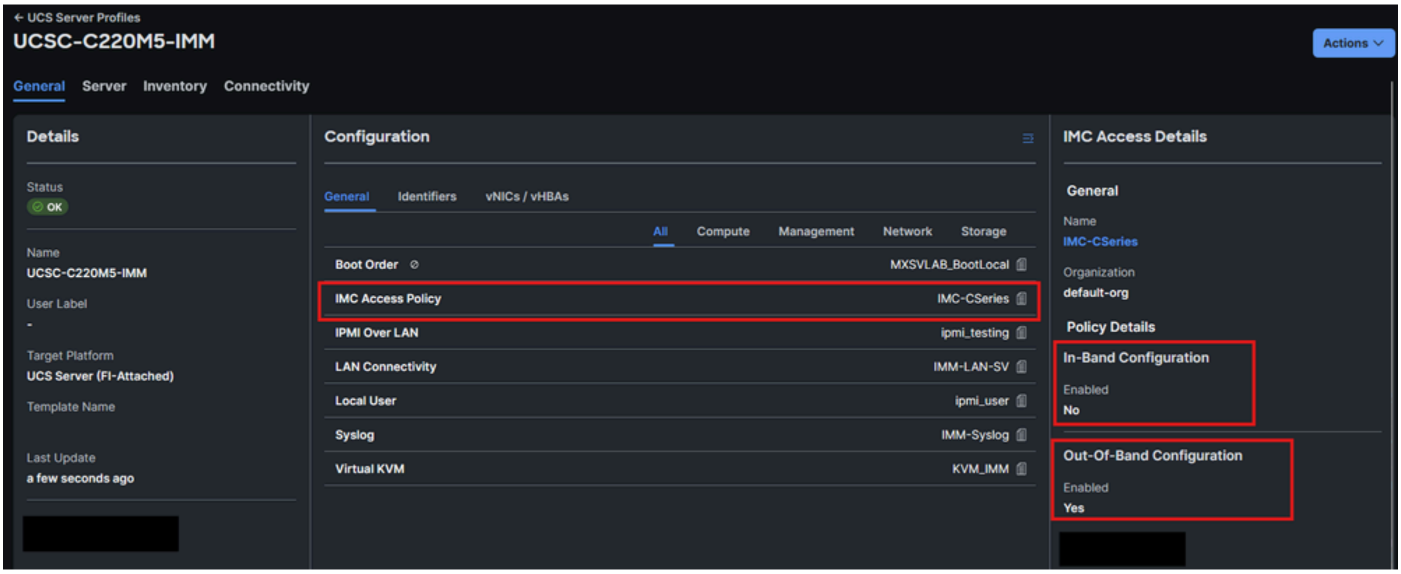
4. The message must be logged in your remote server:

<#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)
```

The same test can be run on servers:

Note: This procedure only works for servers with out-of-band configuration on their IMC Access Policy. If Inband is in use, perform the packet capture on the remote Syslog server instead, or reach out to TAC to perform it with internal debug commands.



UCSC-C220M5-IMM

Details

Status: OK

Name: UCSC-C220M5-IMM

User Label: -

Target Platform: UCS Server (FI-Attached)

Template Name

Last Update: a few seconds ago

[redacted]

Configuration

Boot Order	MXSVLAB_BootLocal
IMC Access Policy	IMC-CSeries
IPMI Over LAN	ipmi_testing
LAN Connectivity	IMM-LAN-SV
Local User	ipmi_user
Syslog	IMM-Syslog
Virtual KVM	KVM_IMM

IMC Access Details

General

Name: IMC-CSeries

Organization: default-org

Policy Details

In-Band Configuration

Enabled: No

Out-Of-Band Configuration

Enabled: Yes

[redacted]

Verify the configuration on the IMC access policy

In this example, the LED locator on a C220 M5 Integrated Server was enabled. This does not require downtime.

1. Verify which Fabric Interconnect sends out-of-band traffic for your server. The server IP is 192.0.2.5, so Fabric Interconnect A forwards its management traffic ("secondary route" means that the Fabric Interconnect acts as a proxy for the server management traffic):

   <#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
   ```

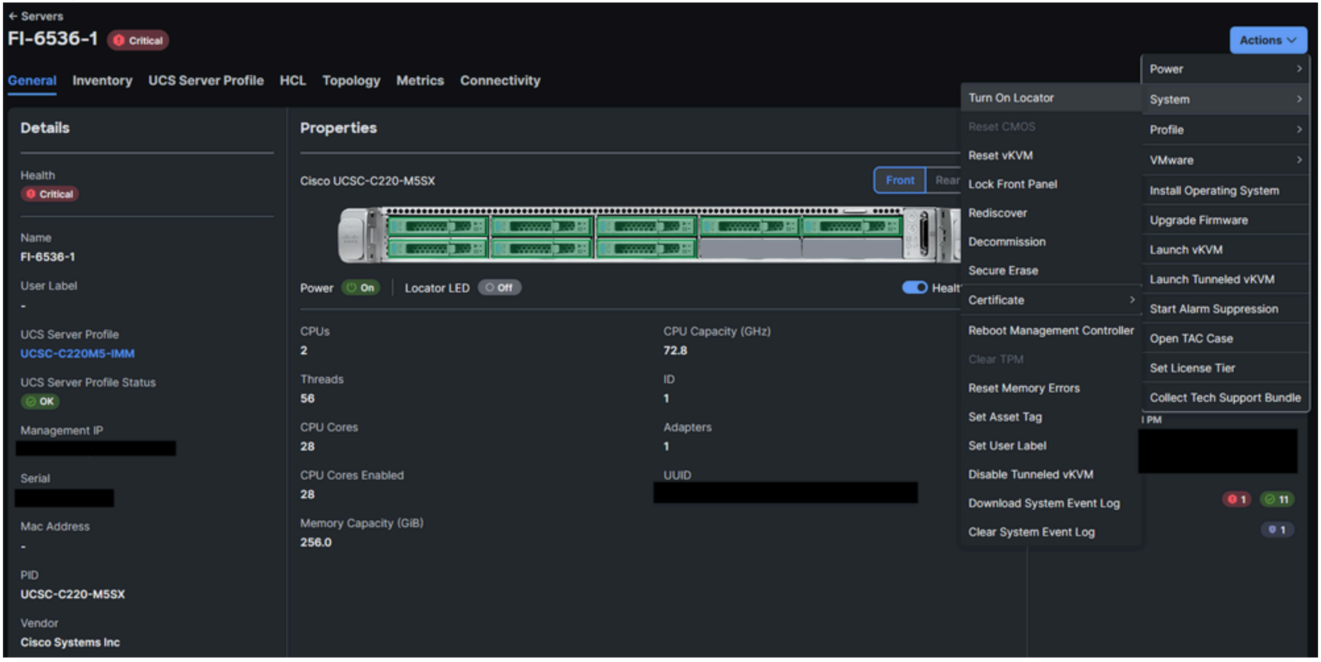
   `secondary route-preference`

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

2. Start a packet capture on the appropriate Fabric Interconnect:

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

3. Navigate to **Servers** > **Actions** > **System** and choose **Turn On Locator**:



Details

Health
Critical

Name
FI-6536-1

User Label
-

UCS Server Profile
UCSC-C220M5-IMM

UCS Server Profile Status
OK

Management IP
[redacted]

Serial
[redacted]

Mac Address
-

PID
UCSC-C220-M5SX

Vendor
Cisco Systems Inc

Properties

Cisco UCSC-C220-M5SX

Power On | Locator LED Off

CPUs
2

Threads
56

CPU Cores
28

CPU Cores Enabled
28

Memory Capacity (GiB)
256.0

CPU Capacity (GHz)
72.8

ID
1

Adapters
1

UUID
[redacted]

[redacted]

Turn on LED locator in a Server

4. The console on the Fabric Interconnect must show the Syslog packet captured:

   <#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. The Syslog message must be logged in your remote server AUDIT.log file:

   <#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:
   ```

If Syslog packets were generated by UCS, but the Syslog server did not log them:

1. Confirm that the packets arrived at the remote Syslog server with a packet capture.
2. Verify the configuration of your remote Syslog server (including but not limited to: configured syslog port and firewall settings).

Related Information

- RFC 5424 - The Syslog Protocol
- Intersight IMM Expert Series - Syslog Policy
- Cisco Intersight Help Center - Configure UCS Domain Profile Policies
- Cisco Intersight Help Center - Configure Server Policies

If the Server has Inband configured on its IMC Access Policy, load CIMC debug shell and perform a packet capture on the bond0 interface for Racks, or bond0.x interface (where x is the VLAN) for Blades.

```
[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
```

- The Syslog port number **cannot** be changed on Fabric Interconnects, only in Servers. This is by design and was documented on