

Configurazione e verifica del syslog sulla modalità gestita di UCS Intersight

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Interconnessioni fabric](#)

[Server](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il processo di configurazione e verifica del protocollo Syslog sui domini UCS in modalità gestita Intersight.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Server Unified Computing System (UCS)
- Intersight Managed Mode (IMM)
- Nozioni di base sulla rete
- Protocollo Syslog

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

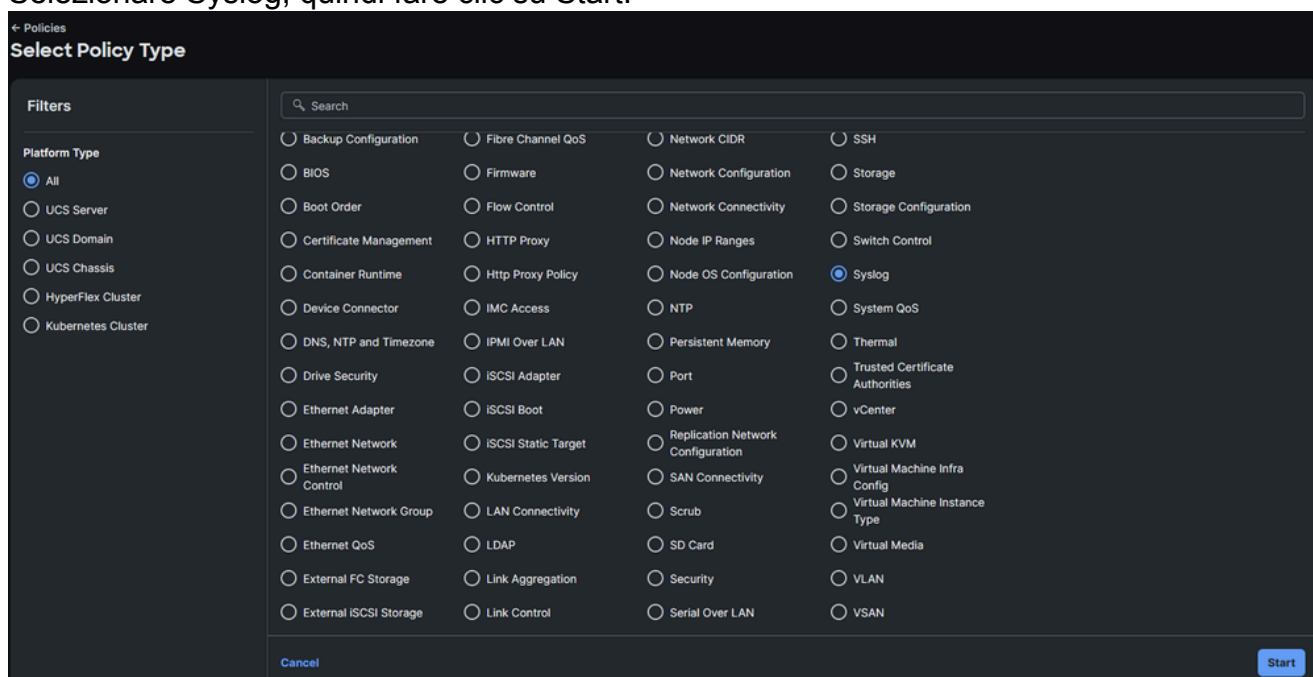
ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I criteri Syslog sono applicabili per interconnessioni fabric e server. Consentono la configurazione della registrazione locale e remota.

Configurazione

1. Passare a Criteri > Crea nuovo criterio.
2. Selezionare Syslog, quindi fare clic su Start.



Selezione criteri

3. Scegliere l'organizzazione e scegliere un nome, quindi fare clic su Avanti.

Policies > Syslog

Create

1 General

2 Policy Details

General

Add a name, description, and tag for the policy.

Organization *
default-org

Name *
IMM-Syslog-Policy

Set Tags
Enter a tag in the key-value format.

Description
Description
0 / 1024

Cancel Next

Configura organizzazione e nome

- Scegliere la severità minima desiderata per il rapporto relativo alla registrazione locale. Per i livelli di gravità, vedere la [RFC 5424](#).

Policies > Syslog

Create

1 General

2 Policy Details

Policy Details

Add policy details.

All Platforms | UCS Server (Standalone) | UCS Server (FI-Attached) | UCS Domain

Local Logging

File

Minimum Severity to Report * ⓘ
Debug

Warning

Emergency

Alert

Critical

Error

Notice

Informational

Debug

Enable

Enable


Cancel Back Create

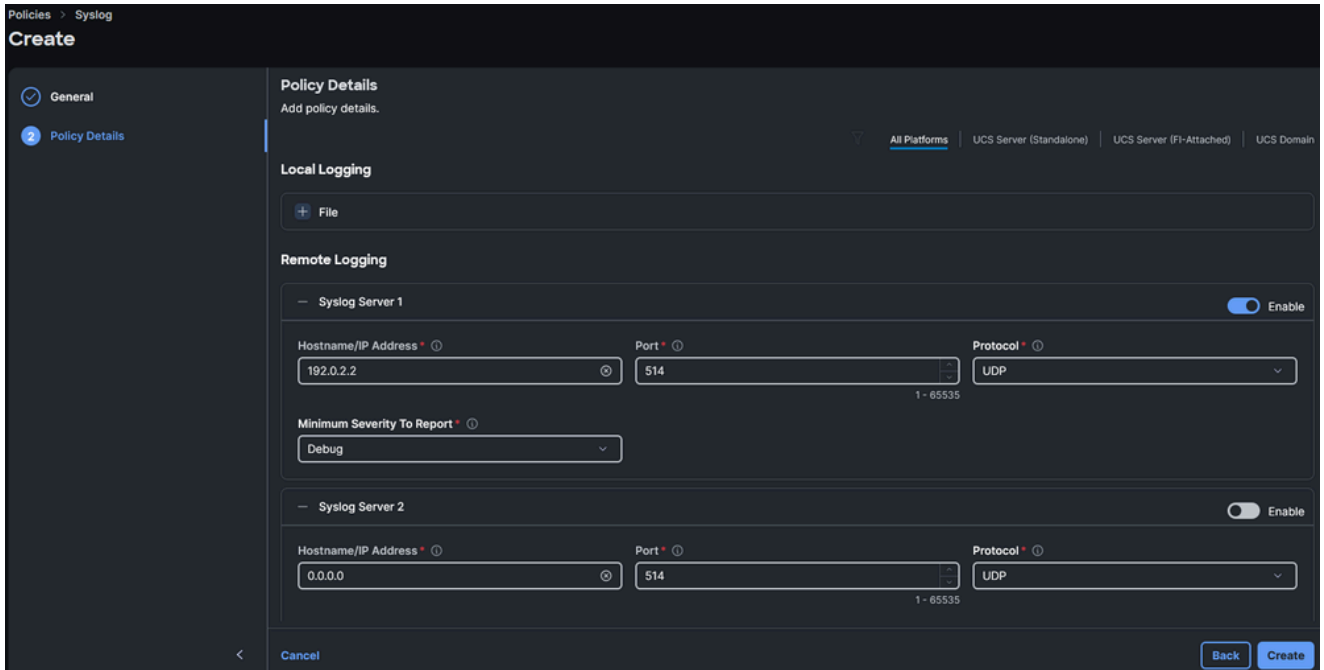
Scegliere la gravità minima da includere nel rapporto per la registrazione locale

- Scegliere il livello di gravità minimo desiderato per il rapporto relativo alla registrazione remota e le impostazioni necessarie. Si tratta dell'indirizzo IP o del nome host del server remoto, del numero di porta e del protocollo della porta (TCP o UDP).



Nota: In questo esempio viene utilizzata l'impostazione predefinita per la porta UDP 514. Sebbene sia possibile modificare il numero di porta, questa impostazione è valida

 solo per i server. Le interconnessioni fabric utilizzano la porta predefinita 514.



Policies > Syslog
Create

General
Policy Details

Policy Details
Add policy details.

All Platforms | UCS Server (Standalone) | UCS Server (FI-Attached) | UCS Domain

Local Logging

+ File

Remote Logging

— Syslog Server 1 Enable

Hostname/IP Address * ① 192.0.2.2 Port * ① 514 Protocol * ① UDP

Minimum Severity To Report * ① Debug

— Syslog Server 2 Enable

Hostname/IP Address * ① 0.0.0.0 Port * ① 514 Protocol * ① UDP

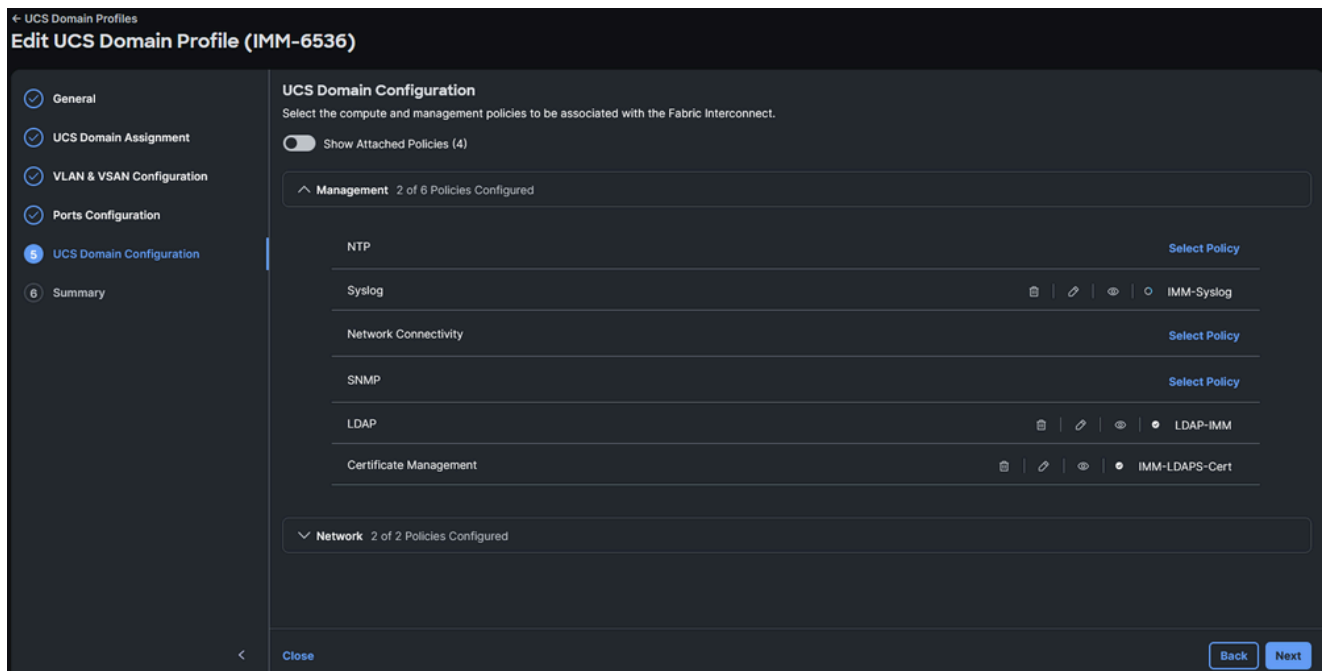
Cancel Back Create

Configura parametri di registrazione remota

6. Fare clic su Crea.
7. Assegnare il criterio ai dispositivi desiderati.

Interconnessioni fabric

1. Passare al Profilo di dominio, fare clic su Modifica, quindi su Avanti fino al passaggio 4 Configurazione del dominio UCS.
2. In Gestione > Syslog, scegliere il criterio Syslog desiderato.

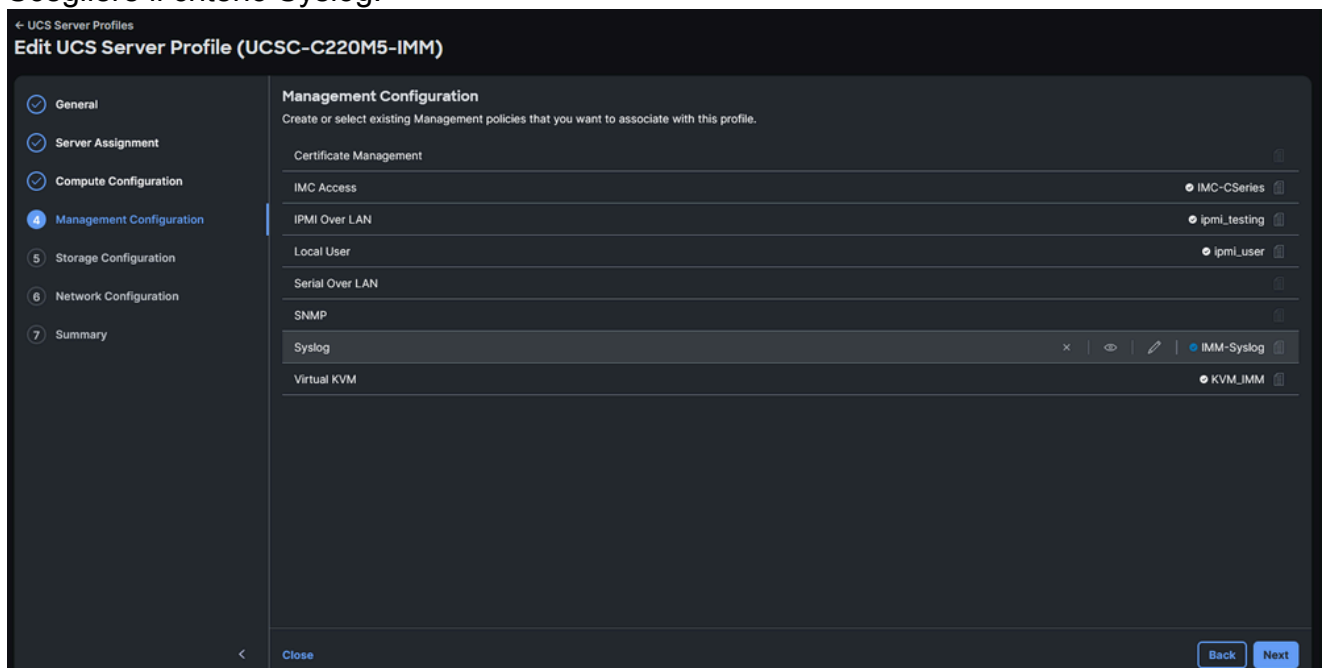


Scegliere il criterio syslog in un profilo di dominio di interconnessione fabric

3. Fare clic su Avanti, quindi su Distribuisci. La distribuzione di questo criterio non comporta interruzioni.

Server

1. Passare al profilo del server, fare clic su Modifica, quindi su Avanti fino al passaggio 4 Configurazione gestione.
2. Scegliere il criterio Syslog.




Scegliere il criterio syslog in un profilo di servizio del server

3. Continuare fino all'ultimo passaggio e Distribuire.

Verifica

A questo punto, i messaggi Syslog devono essere registrati sui server remoti Syslog. Per questo esempio, il server Syslog è stato distribuito su un server Linux con la libreria rsyslog.

 Nota: La verifica della registrazione dei messaggi Syslog può variare in base al server Syslog remoto in uso.

Confermare che i messaggi Syslog delle interconnessioni Fabric siano stati registrati sul server remoto:

```
[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
```

Confermare che i messaggi del syslog del server siano stati registrati sul server remoto:

```
[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 level:3)
Jan 16 20:16:23 192.0.2.5 AUDIT[2257]: Local User Management (strong password policy :disabled) by User:(null)
Jan 16 20:16:23 192.0.2.5 AUDIT[2257]: Password Expiration Parameters (password_history:5,password_expiry:90)
Jan 16 20:16:26 192.0.2.5 AUDIT[2257]: Local Syslog Severity changed to "Debug" by User:(null) from Info
Jan 16 20:16:27 192.0.2.5 AUDIT[2257]: Secured Remote Syslog with(serverId =1, secure_enabled =0) by User:(null)
```

Risoluzione dei problemi

È possibile acquisire un pacchetto sulle interconnessioni Fabric per verificare che i pacchetti Syslog siano stati inoltrati correttamente. Modificare il livello di gravità minimo per il report di cui eseguire il debug. Accertarsi che Syslog fornisca il maggior numero di informazioni possibile.

Dall'interfaccia della riga di comando, avviare l'acquisizione di un pacchetto sulla porta di gestione e filtrare in base alla porta 514 (porta Syslog):

```
<#root>
```

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

```
local interface mgmt
```

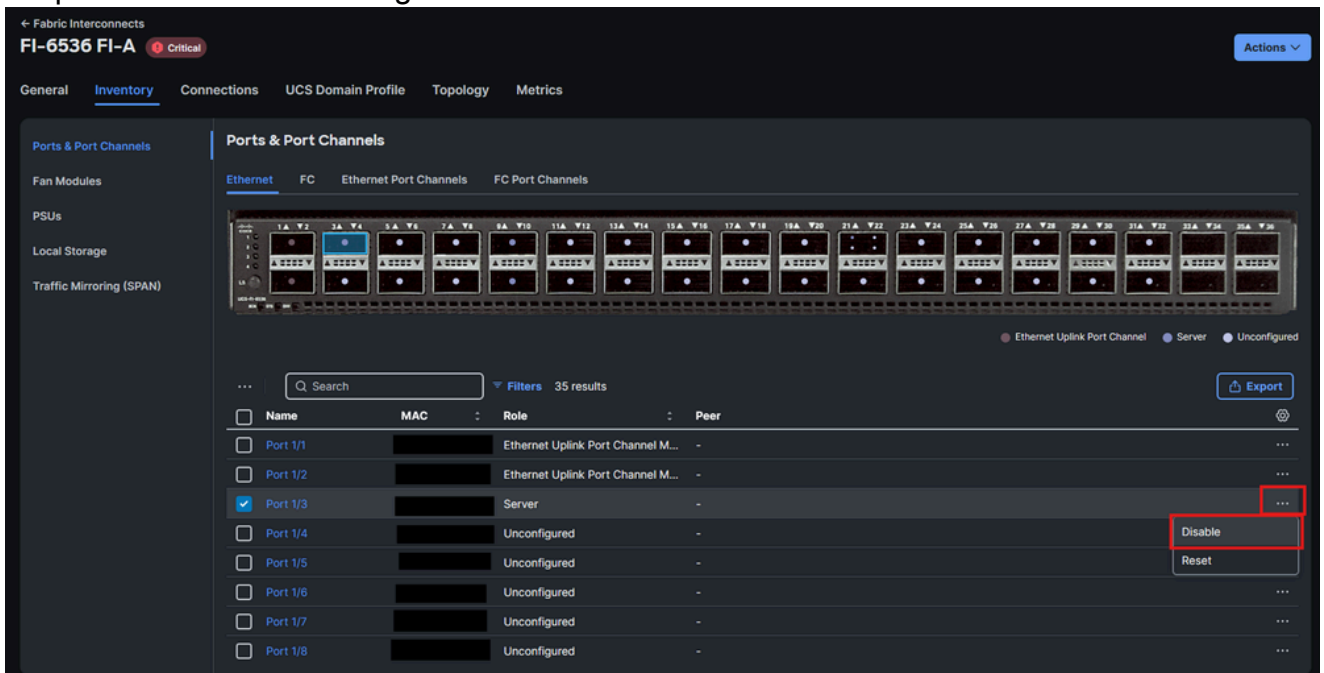
```
capture-filter "
```

```
port 514
```

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

Nell'esempio, una porta server sull'interfaccia Fabric A è stata disabilitata per generare il traffico Syslog.

1. Passare a Interconnessioni fabric > Inventario.
2. Fare clic sulla casella di controllo della porta desiderata, aprire il menu con i puntini di sospensione a destra e scegliere Disattiva.



Arrestare un'interfaccia su un'interconnessione fabric per generare traffico syslog per il test

3. La console sull'interconnessione fabric deve acquisire il pacchetto Syslog:

```
<#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. Il messaggio deve essere registrato nel server remoto:

```
<#root>
```

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


```
Jan 16 17:15:03
```

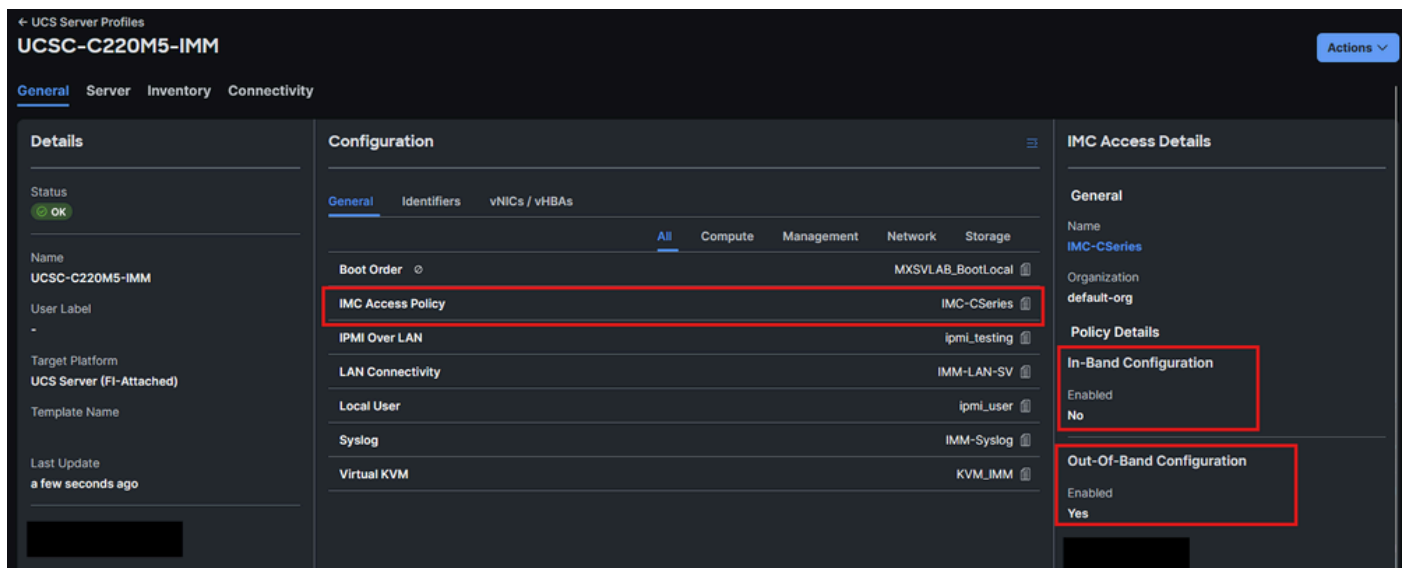
```
192.0.2.3
```

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

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

Lo stesso test può essere eseguito sui server:

 Nota: Questa procedura è valida solo per i server con configurazione fuori banda nei criteri di accesso IMC. Se il protocollo Inband è in uso, eseguire l'acquisizione dei pacchetti sul server Syslog remoto oppure raggiungere il server TAC per eseguirla con i comandi interni di debug.



The screenshot displays the UCS Server Profiles configuration interface for a server named UCSC-C220M5-IMM. The interface is divided into several sections: Details, Configuration, and IMC Access Details. The Configuration section is further divided into tabs for General, Identifiers, and vNICs / vHBAs. The IMC Access Details section shows the following configuration:

Section	Property	Value
General	Name	IMC-CSeries
	Organization	default-org
Policy Details	In-Band Configuration	No
	Out-Of-Band Configuration	Yes

Verificare la configurazione nei criteri di accesso IMC

In questo esempio, è stato attivato il localizzatore LED su un server integrato C220 M5. Ciò non richiede tempi di inattività.

1. Verificare quale interconnessione fabric invia il traffico fuori banda per il server. L'IP del server è 192.0.2.5, quindi l'interconnessione Fabric A inoltra il traffico di gestione (il termine "route secondaria" indica che l'interconnessione Fabric funge da proxy per il traffico di gestione del server):

```
<#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

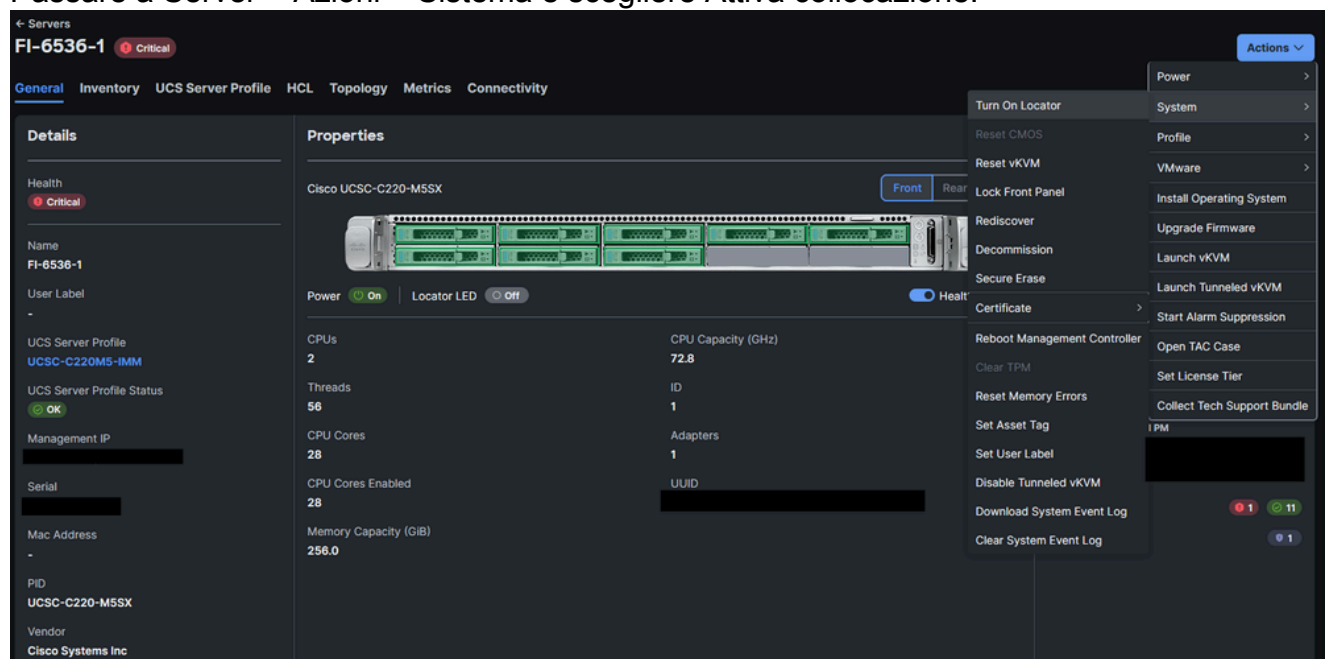
secondary route-preference

: 0, tag: 0

2. Avviare l'acquisizione di un pacchetto sull'interconnessione fabric appropriata:

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

3. Passare a Server > Azioni > Sistema e scegliere Attiva collocazione:



Attivare il localizzatore LED in un server

4. La console sull'interconnessione fabric deve visualizzare il pacchetto Syslog acquisito:

```
<#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. Il messaggio Syslog deve essere registrato nel file AUDIT.log del server remoto:

```
<#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:
```

Se i pacchetti Syslog sono stati generati da UCS, ma il server Syslog non li ha registrati:

1. Confermare che i pacchetti siano arrivati al server Syslog remoto con un'acquisizione.
2. Verificare la configurazione del server Syslog remoto (inclusi, ma non limitati a: configurate (impostazioni del firewall e della porta syslog).

Informazioni correlate

- [RFC 5424 - Protocollo Syslog](#)
- [Intersight IMM serie Expert - Syslog Policy](#)
- [Cisco Intersight Help Center - Configurazione dei criteri dei profili di dominio UCS](#)
- [Cisco Intersight Help Center - Configurazione dei criteri server](#)

Se per il server è stato configurato Inband sulla policy di accesso IMC, caricare la shell di debug CIMC ed eseguire un'acquisizione dei pacchetti sull'interfaccia **bond0** per i rack o sull'interfaccia **bond0.x** (dove x è la VLAN) per i blade.

```
[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)
```

- Impossibile modificare il numero di porta Syslog nelle interconnessioni Fabric, solo nei server. Questo è il progetto ed è stato documentato su

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).