# Configuration et vérification de Syslog en mode géré UCS Intersight

## Table des matières


Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Interconnexions de fabric
- Serveurs

Vérifier

Dépannage

Informations connexes


## Introduction

Ce document décrit le processus de configuration et de vérification du protocole Syslog sur les domaines UCS en mode géré Intersight.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveurs UCS (Unified Computing System)
- Mode géré Intersight (IMM)
- Concepts de base des réseaux
- protocole Syslog

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Intersight en tant que service (SaaS)
- Interconnexion de fabric Cisco UCS 6536, microprogramme 4.3(5.240032)
- Serveur rack C220 M5, microprogramme 4.3(2.240090)
- Alma Linux 9

The information in this document was created from the devices in a specific lab environment. All of

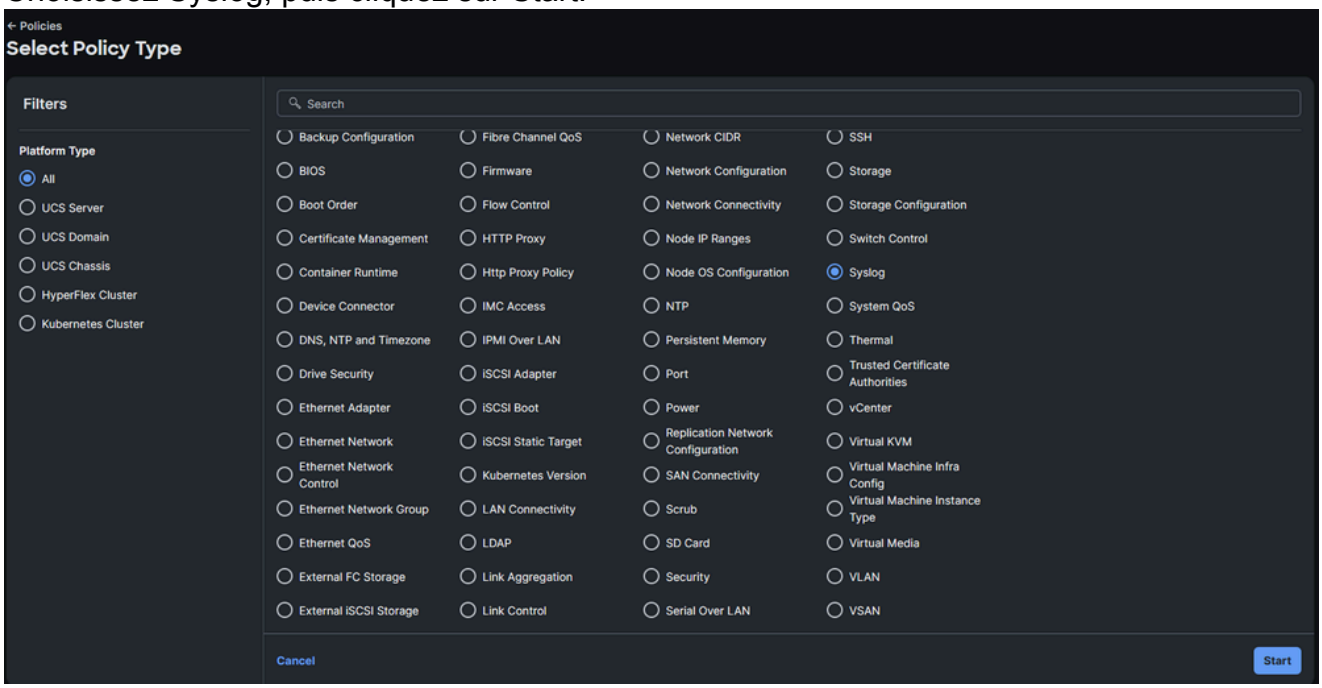
the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Informations générales

Les stratégies Syslog s'appliquent aux interconnexions de fabric et aux serveurs. Ils permettent de configurer la journalisation locale et distante.

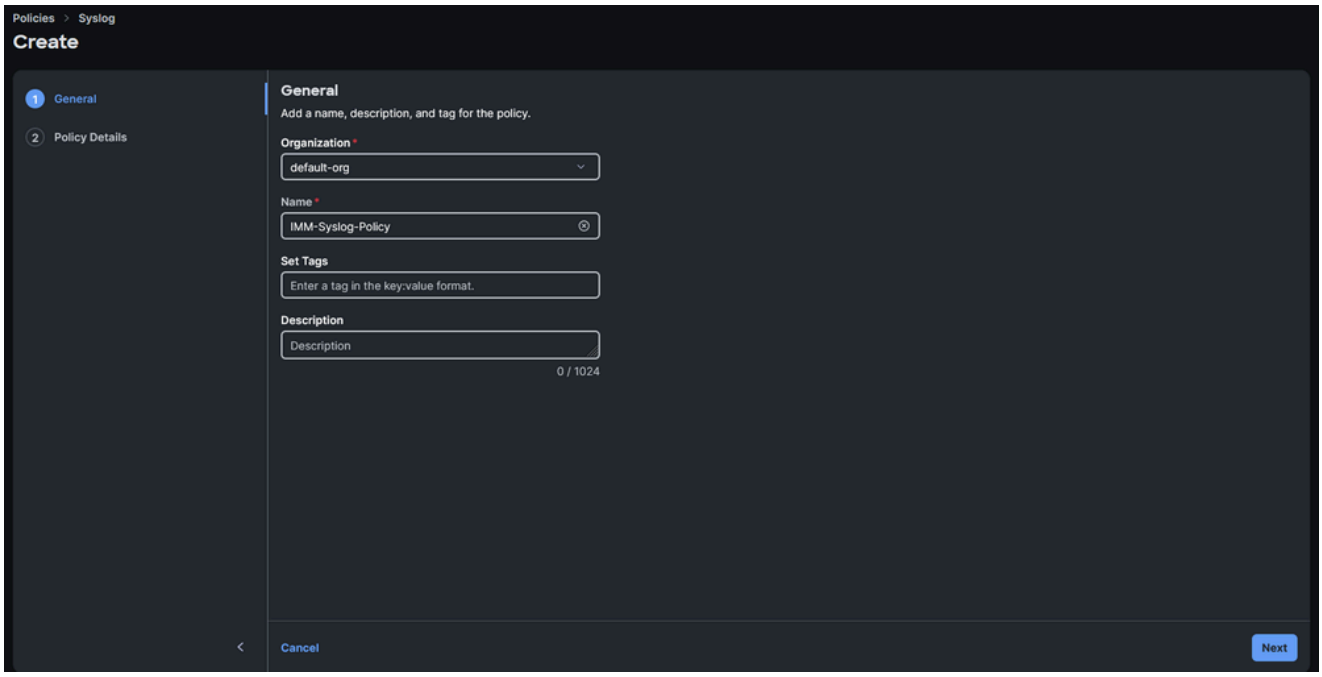
# Configurer

1. Accédez à Politiques > Créer une nouvelle politique.
2. Choisissez Syslog, puis cliquez sur Start.



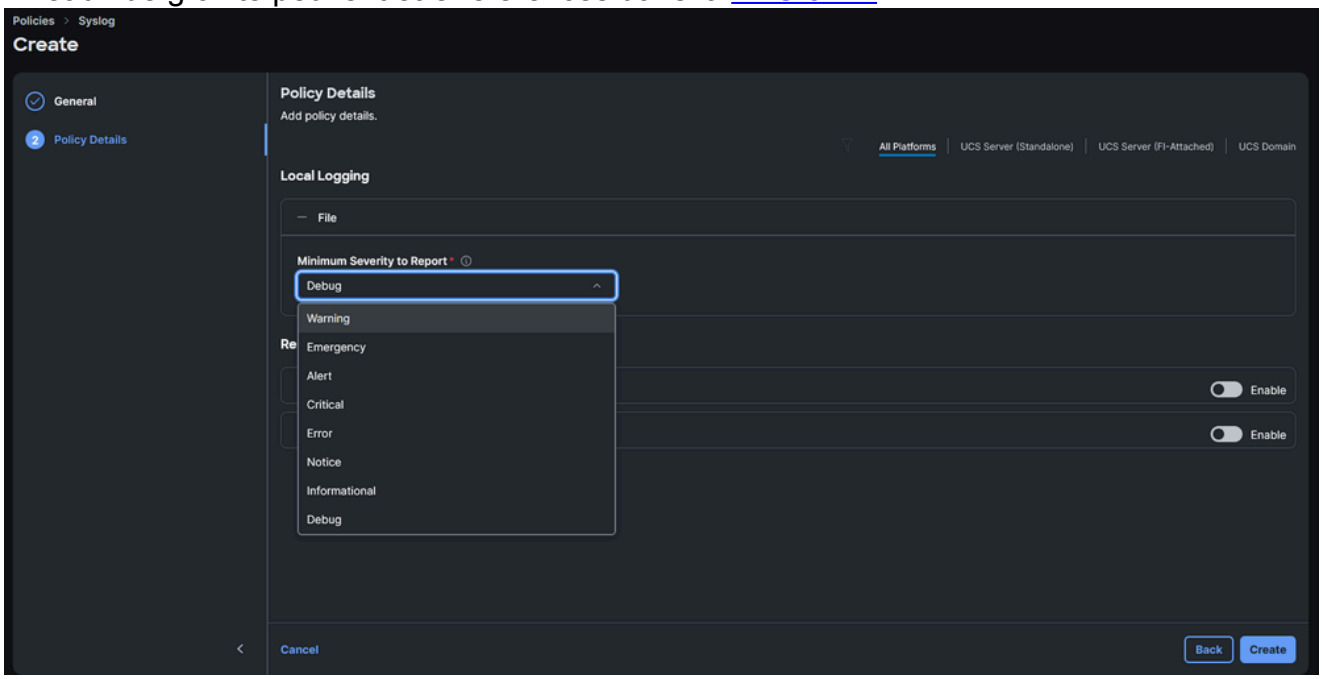

Sélection de stratégie

3. Choisissez l'organisation et choisissez un nom, puis cliquez sur Suivant.




Configurer l'organisation et le nom

4. Sélectionnez le niveau de gravité minimum souhaité pour la journalisation locale. Les niveaux de gravité peuvent être référencés dans la RFC 5424.




Sélectionnez le niveau de gravité minimal à signaler pour la journalisation locale

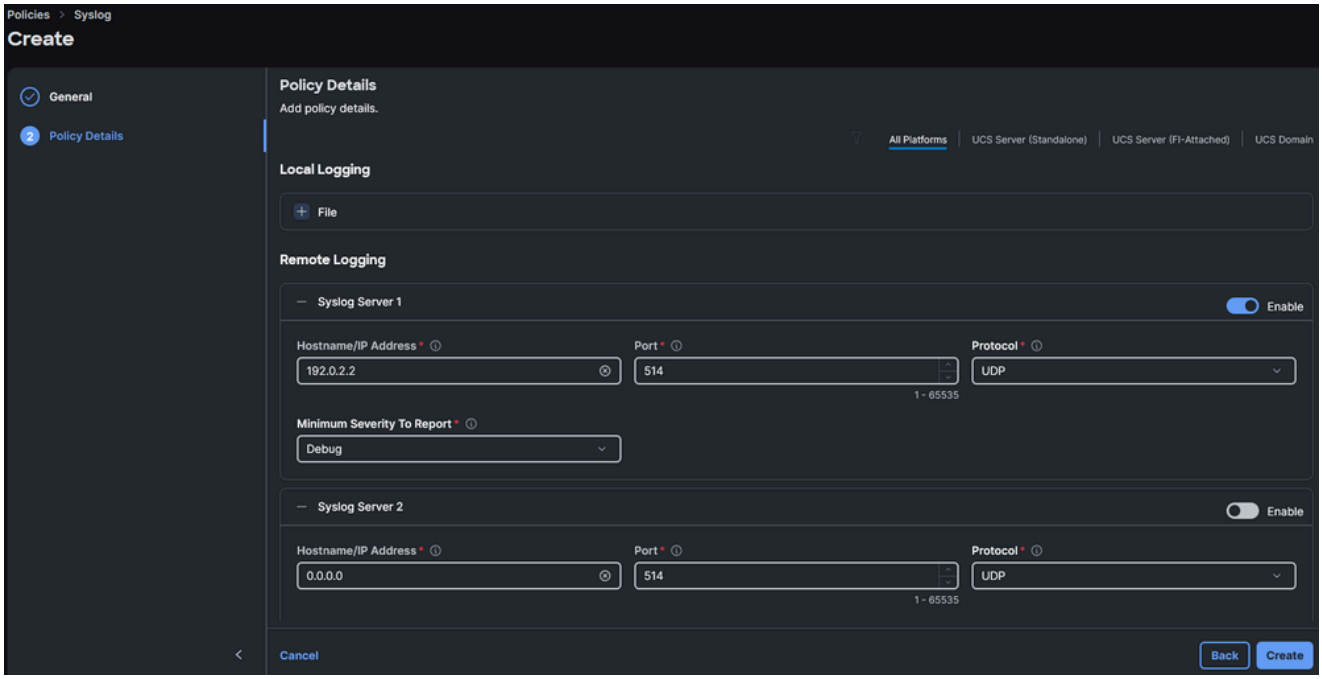
5. Sélectionnez le niveau de gravité minimum souhaité pour la journalisation à distance et les paramètres requis. Il s'agit de l'adresse IP ou du nom d'hôte du ou des serveurs distants, du numéro de port et du protocole de port (TCP ou UDP).

---

Remarque : Cet exemple utilise le paramètre par défaut UDP port 514. Bien que le numéro de port puisse être modifié, cela ne s'applique qu'aux serveurs. Les

---

interconnexions de fabric utilisent le port par défaut 514 par conception.

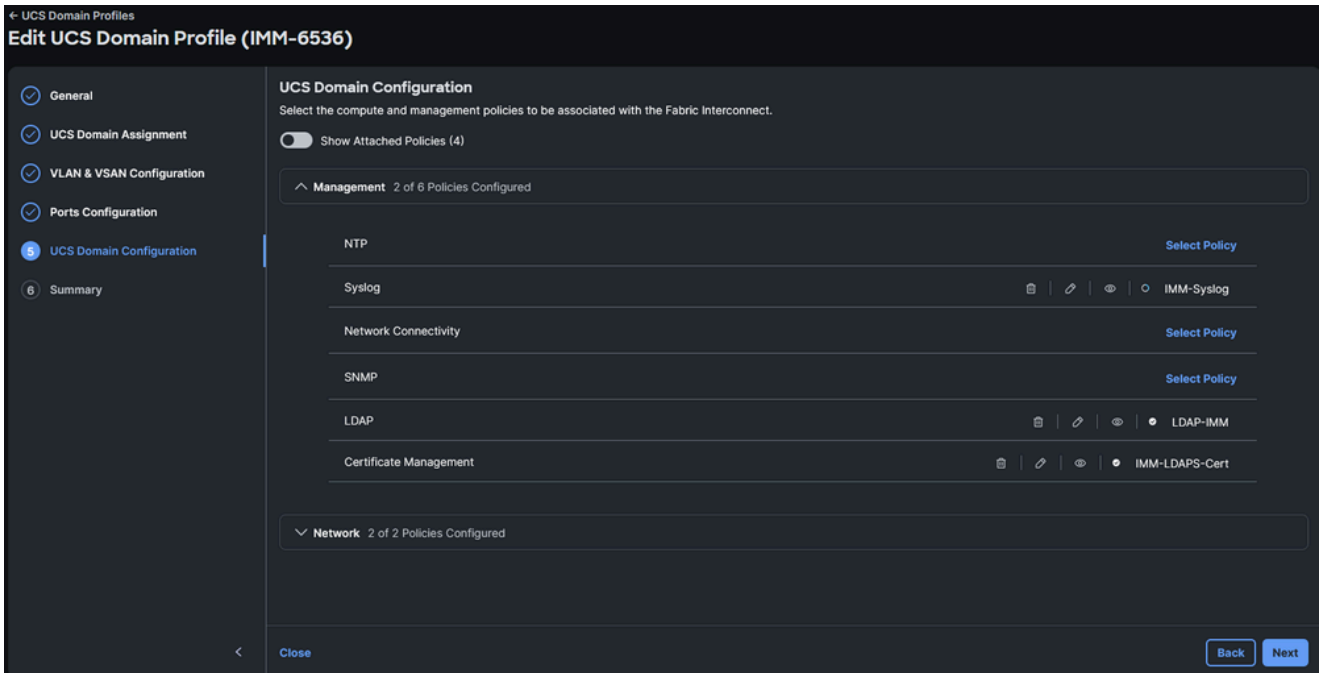



Configurer les paramètres de journalisation à distance

6. Cliquez sur Create.
7. Attribuez la stratégie aux périphériques souhaités.

## Interconnexions de fabric

1. Accédez au profil de domaine, cliquez sur Edit, puis sur Next jusqu'à l'étape 4 de la configuration du domaine UCS.
2. Sous Management > Syslog, sélectionnez la politique Syslog souhaitée.

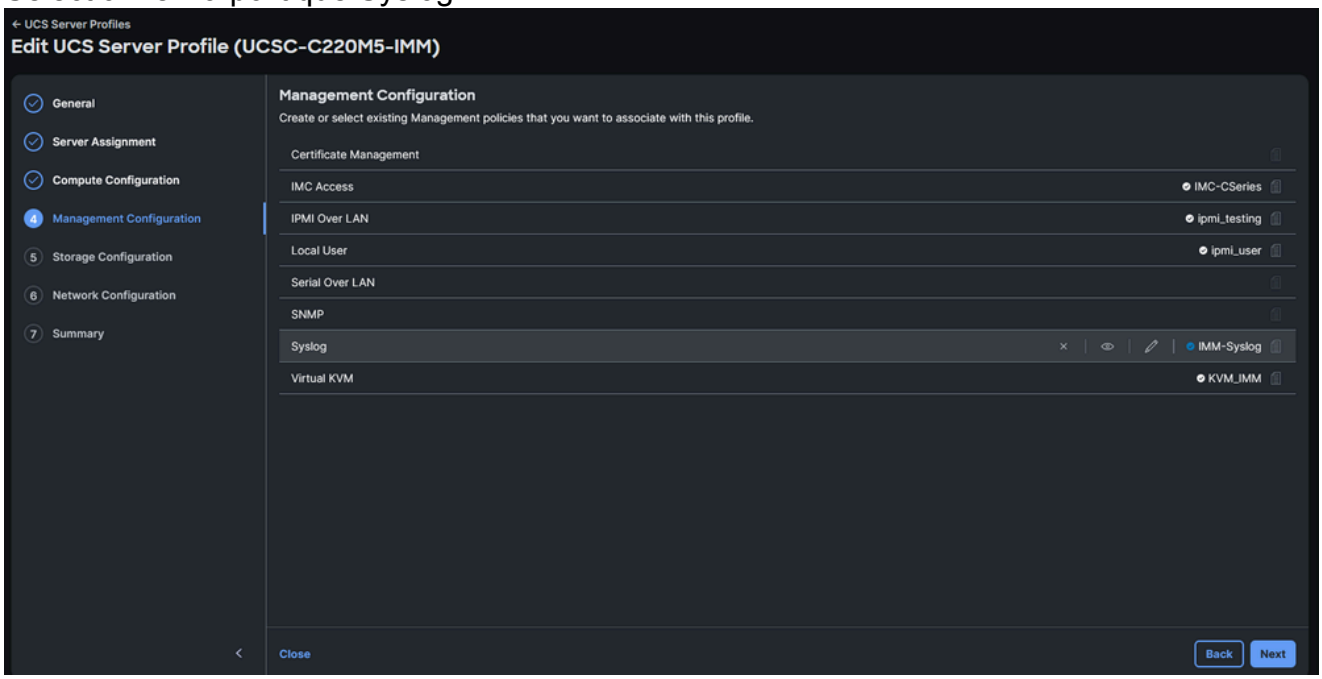



Sélectionnez la stratégie Syslog sur un profil de domaine Fabric Interconnect

3. Cliquez sur Next, puis sur Deploy. Le déploiement de cette stratégie n'est pas perturbateur.

## Serveurs

1. Accédez au profil de serveur, cliquez sur Edit, puis passez à Next jusqu'à l'étape 4 Management Configuration.
2. Sélectionnez la politique Syslog.




Choisir la stratégie Syslog sur un profil de service de serveur

3. Continuez jusqu'à la dernière étape et Déployez.

# Vérifier

À ce stade, les messages Syslog doivent être consignés sur le ou les serveurs distants Syslog. Dans cet exemple, le serveur Syslog a été déployé sur un serveur Linux avec la bibliothèque rsyslog.

---

Remarque : La vérification de la journalisation des messages Syslog peut varier en fonction du serveur Syslog distant utilisé.

---

Vérifiez que les messages Syslog Fabric Interconnects ont été consignés sur le serveur distant :

```
[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
```

Vérifiez que les messages Syslog des serveurs ont été consignés sur le serveur distant :

```
[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
```

# Dépannage

Une capture de paquets peut être effectuée sur les interconnexions de fabric pour confirmer que les paquets Syslog ont été transférés correctement. Modifiez le niveau de gravité minimum à rapporter au débogage. Assurez-vous que les rapports Syslog contiennent autant d'informations que possible.

À partir de l’interface de ligne de commande, lancez une capture de paquets sur le port de gestion et filtrez par port 514 (port Syslog) :

<#root>

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

**local interface mgmt**

```
 capture-filter "
```

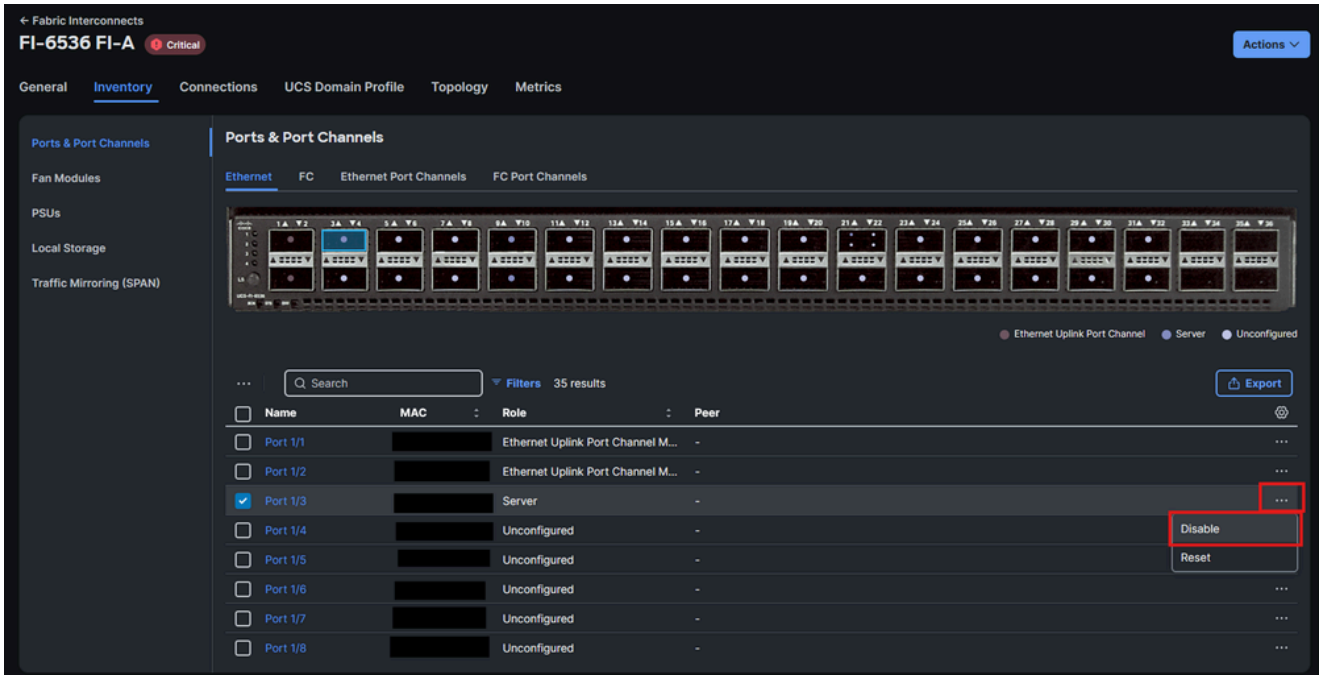
**port 514**

```
" limit-captured-frames 0
```

```
Capturing on mgmt0
```

Dans cet exemple, un port de serveur sur Fabric Interconnect A a été mis à l'écart pour générer du trafic Syslog.

1. Accédez à Fabric Interconnects > Inventory.
2. Cochez la case correspondant au port souhaité, ouvrez le menu de sélection à droite et choisissez disable.




Arrêter une interface sur une interconnexion de fabric pour générer du trafic syslog à des fins de test

3. La console de Fabric Interconnect doit capturer le paquet 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. Le message doit être connecté à votre serveur distant :

<#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:
```

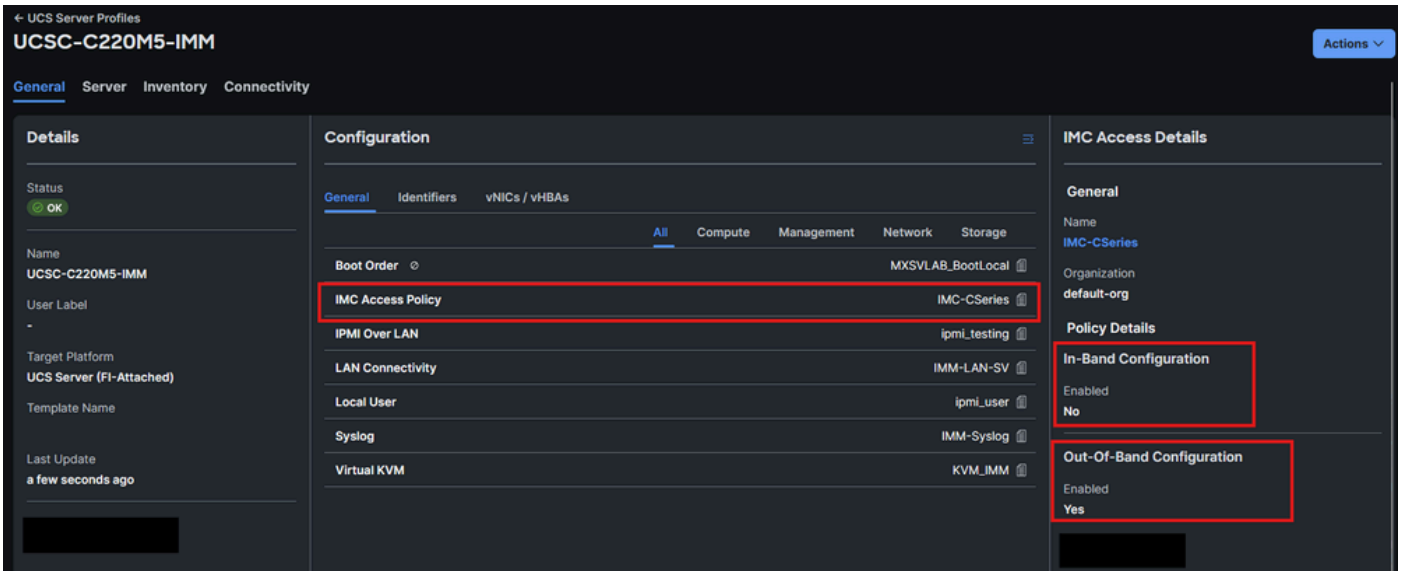
**%ETHPORT-5-IF_DOWN_NONE: Interface Ethernet1/3 is down (Transceiver Absent)**

Le même test peut être exécuté sur les serveurs :

---

Remarque : Cette procédure ne fonctionne que pour les serveurs avec une configuration hors bande sur leur politique d'accès IMC. Si Inband est en cours d'utilisation, effectuez plutôt la capture de paquets sur le serveur Syslog distant, ou contactez le TAC pour l'effectuer avec les commandes debug internes.

---




Vérifier la configuration de la stratégie d'accès IMC

Dans cet exemple, l'indicateur LED d'un serveur intégré C220 M5 a été activé. Cela ne nécessite pas de temps d'arrêt.

1. Vérifiez quel Fabric Interconnect envoie le trafic hors bande pour votre serveur. L'adresse IP du serveur est 192.0.2.5, de sorte que Fabric Interconnect A transfère son trafic de gestion (« route secondaire » signifie que Fabric Interconnect agit comme un proxy pour le trafic de gestion du serveur) :

   <#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
```

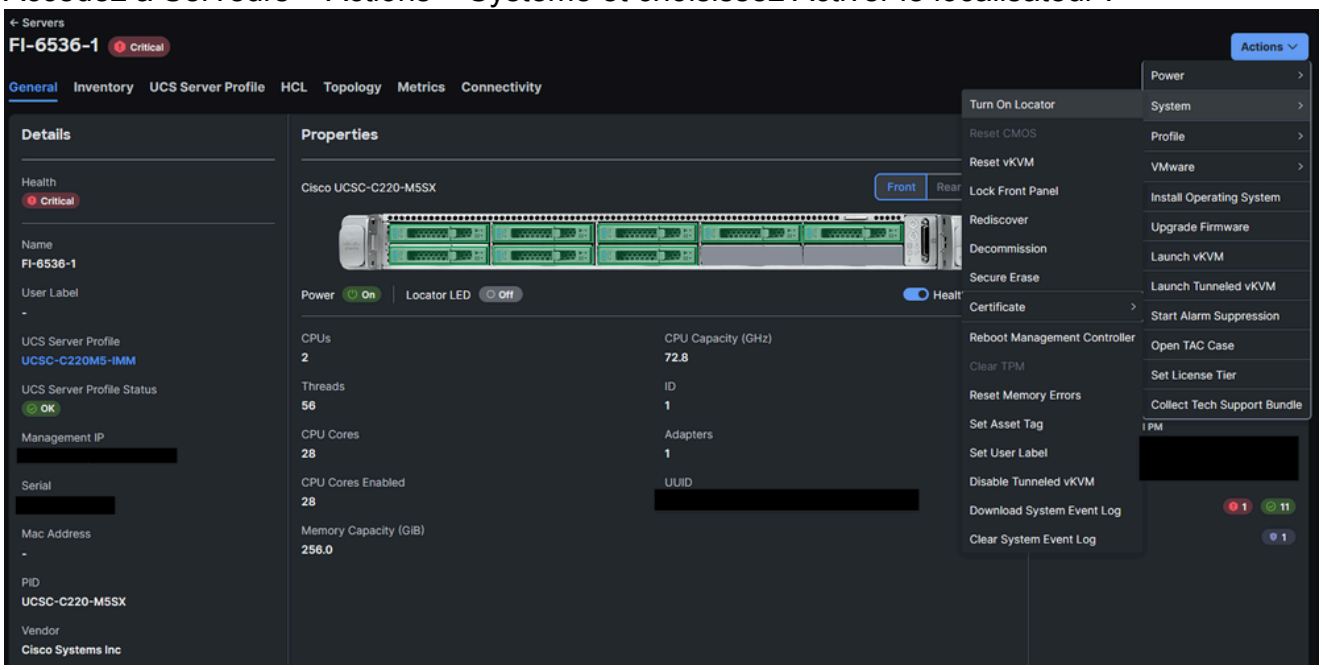
**secondary route-preference**

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

2. Démarrez une capture de paquets sur l'interconnexion de fabric appropriée :

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

3. Accédez à Serveurs > Actions > Système et choisissez Activer le localisateur :




Allumer le voyant de localisation d'un serveur

4. La console de Fabric Interconnect doit afficher le paquet Syslog capturé :

<#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. Le message Syslog doit être consigné dans le fichier AUDIT.log de votre serveur distant:

<#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:
```

Si des paquets Syslog ont été générés par UCS, mais que le serveur Syslog ne les a pas consignés :

1. Vérifiez que les paquets sont arrivés sur le serveur Syslog distant avec une capture de paquets.
2. Vérifiez la configuration de votre serveur Syslog distant (y compris, mais sans s'y limiter : configuration du port syslog et des paramètres de pare-feu).

## Informations connexes

- RFC 5424 - Protocole Syslog
- Série Intersight IMM Expert - Politique Syslog
- Centre d'aide Cisco Intersight - Configuration des stratégies de profil de domaine UCS
- Centre d'aide Cisco Intersight - Configuration des stratégies de serveur

Si le serveur est configuré en intrabande sur sa politique d'accès IMC, chargez l'interpréteur de commandes de débogage CIMC et effectuez une capture de paquets sur l'interface bond0 pour les racks, ou l'interface bond0.x (où x est le VLAN) pour les lames.

```
[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
```

- Le numéro de port Syslog ne peut pas être modifié sur les interconnexions de fabric, uniquement sur les serveurs. Ceci est par conception et a été documenté sur

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.