

# Configurazione, verifica e risoluzione dei problemi di Callhome in ACI Fabric

## Sommario

---

[Introduzione](#)

[Concetto](#)

[Prerequisiti](#)

[Procedura di configurazione](#)

[Risoluzione dei problemi e verifica](#)

---

## Introduzione

Questo documento descrive la configurazione di Call Home in un ambiente Cisco ACI.

## Concetto

La funzione CallHome ci consente di ricevere notifiche critiche sulla funzionalità dell'infrastruttura tramite e-mail, incluse informazioni di diagnostica e errori o eventi ambientali. Gli avvisi vengono inviati a più destinatari tramite i profili di destinazione CallHome, che possono essere configurati con specifici formati di messaggi e categorie di contenuti.

## Prerequisiti

- Il fabric deve essere su 4.2(1) o superiore.
- Tutti i dispositivi fabric devono disporre di connettività di rete al server SMTP/E-Mail.
- La porta TCP di comunicazione 25 deve essere consentita tra i dispositivi fabric e il server SMTP/E-Mail.

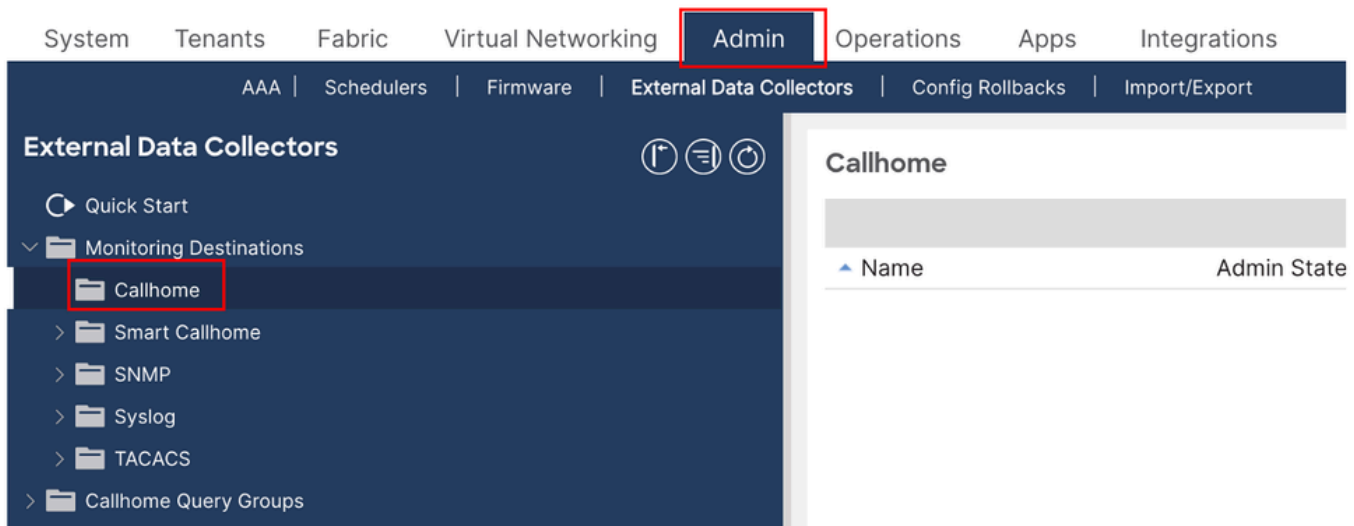
## Procedura di configurazione

Passaggio 1: accedere ad APIC.

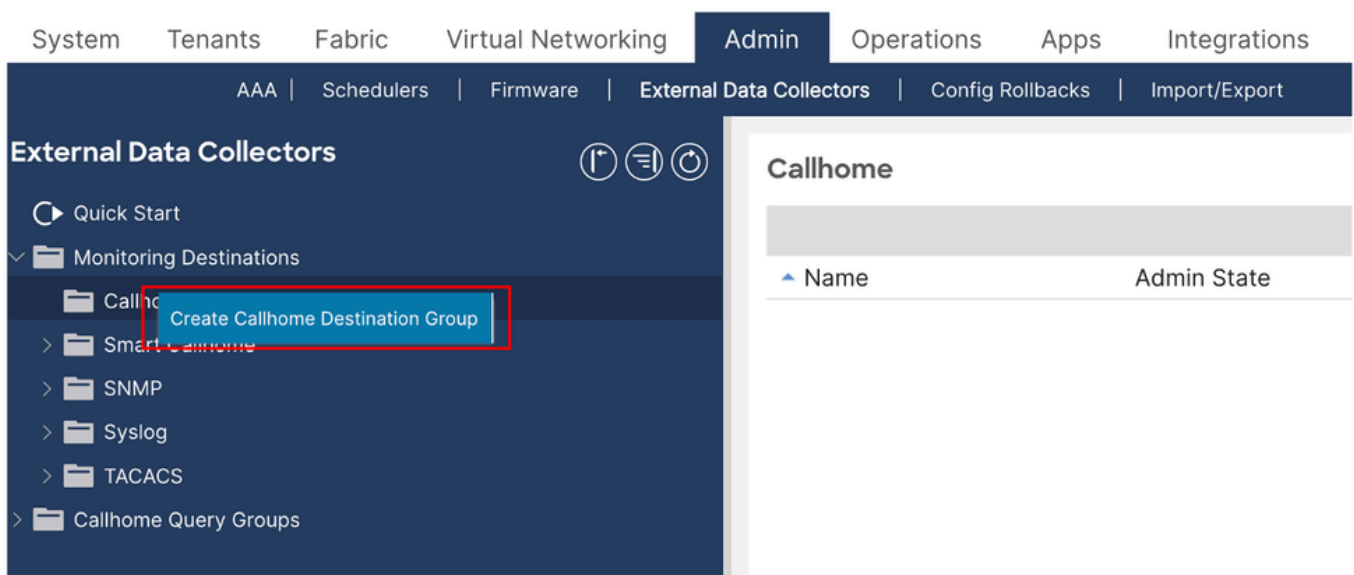
- Accedere ad APIC utilizzando le credenziali di amministratore.

Passaggio 2: creare il gruppo di destinazione CallHome.

- Selezionare APIC > Admin > External Data Collectors > Monitoring Destination



- Fare clic con il pulsante destro del mouse sulla cartella CallHome e selezionare Crea gruppo di destinazione CallHome.



Passaggio 3: Inserire i dettagli richiesti.

I dettagli richiesti sono riportati di seguito

- Nome: nome del gruppo di destinazione di CallHome
- Admin - attiva questa opzione
- Porta - 25 ,Numero di porta su cui il protocollo SMTP comunicherà.
- Server SMTP - Nome DNS o indirizzo IP del server SMTP
- Da e-mail - indirizzo e-mail da cui l'infrastruttura invierà messaggi
- EPG di gestione - oob o inb EPG che ha raggiungibilità al nostro server SMTP
- E-mail di contatto - indirizzo e-mail a cui verranno inviati i messaggi

## Create Callhome Destination Group



1. Profile

2. Destinations

### STEP 1 > Profile

Name:	<input type="text" value="Call_Home_Destination_Group"/>
Description:	<input type="text" value="optional"/>
Admin State:	<input type="text" value="enabled"/> ▾
Port Number:	<input type="text" value="25"/> ▲ ▾
SMTP Server:	<input type="text" value="smtp.cisco.com"/>
Management EPG:	<input type="text" value="default (Out-of-Band)"/> ▾
Secure SMTP:	<input type="checkbox"/>
From Email:	<input type="text" value="frommail@cisco.com"/>
Reply To Email:	<input type="text" value="replaytoemail@cisco.com"/>
Customer Contact Email:	<input type="text" value="customercontactmail@cisco.com"/>
Phone Contact:	<input type="text" value=""/> <small>e.g., +1-011-408-555-1212</small>
Contact Information:	<input type="text"/>
Street Address:	<input type="text"/>
Contract Id:	<input type="text"/>
Customer Id:	<input type="text"/>
Site Id:	<input type="text"/>

Previous

Cancel

Next

- Nella pagina successiva è possibile creare le destinazioni esatte, ovvero i destinatari dei messaggi CallHome.
- Fare clic sui campi firma e riempimento +.
  - Nome - nome destinazione
  - Stato amministrazione: se disabilitato, la destinazione non riceverà alcun messaggio
  - Livello: il livello di gravità dei messaggi che verranno inviati alla destinazione. Consiglierei a questo set di errori o superiore. La tabella dei livelli di gravità verrà fornita di seguito.
  - E-mail - Indirizzo e-mail effettivo a cui inviare i messaggi
  - Formato: se non si prevede di analizzare automaticamente i messaggi in ingresso, impostare questa opzione su short-txt. Possiamo sperimentare per vedere le differenze tra di loro.
  - Dimensione massima (byte) - la dimensione massima di un singolo messaggio e-mail. Se Format viene impostato su aml o xml, i messaggi possono essere molto grandi, pertanto il numero di 100-200 KB è corretto. Possiamo sperimentare con questo numero per determinare la dimensione richiesta. Per il formato di testo breve è sufficiente impostare questo valore su 10KB.
  - Conforme RFC - È meglio dire che non consente questa operazione.

# Create Callhome Destination Group



STEP 2 > Destinations

1. Profile

2. Destinations



If you enable the RFC Compliant flag, messages will not be backward compatible and might have issues with Microsoft Outlook on OSX.



Name	Admin State	Level	Email	Format	Maximum Size (Bytes)	RFC Compliant
------	-------------	-------	-------	--------	----------------------	---------------

# Create Callhome Destination Group



STEP 2 > Destinations

1. Profile

2. Destinations



If you enable the RFC Compliant flag, messages will not be backward compatible and might have issues with Microsoft Outlook on OSX.



Name	Admin State	Level	Email	Format	Maximum Size (Bytes)	RFC Compliant
------	-------------	-------	-------	--------	----------------------	---------------

Destination1	enabled	alerts	actualmail@cisco.com	xml	1000000	<input type="checkbox"/>
--------------	---------	--------	----------------------	-----	---------	--------------------------

Update

Cancel

Previous

Cancel

Finish

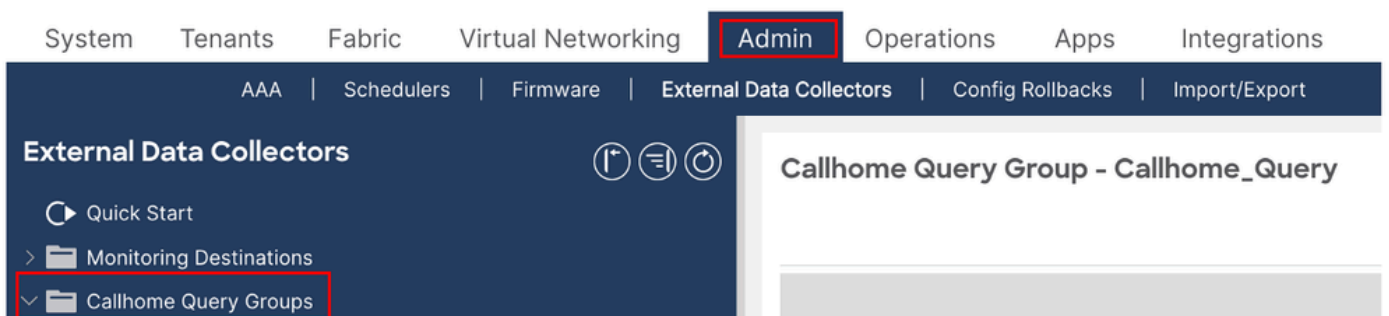
- Possiamo creare tutte le destinazioni che ci servono e possiamo anche creare di più facendo clic con il pulsante destro del mouse sul nostro gruppo di destinazione CallHome e selezionando Crea destinazione CallHome.

# Severity levels

LEVEL KEYWORD	LEVEL	DESCRIPTION
emergencies	0	System unstable
alerts	1	Immediate action needed
critical	2	Critical conditions
errors	3	Error conditions
warning	4	Warning conditions
notifications	5	Normal but significant condition
informational	6	Informational messages only
debugging	7	Debugging messages

## Passo 4: creazione dei gruppi di query di callhome

- Selezionare APIC > Admin > External Data Collector > CallHome Query Groups (APIC > Amministratore > Agenti di raccolta dati esterni > Gruppi di query CallHome)





- Fare clic con il pulsante destro del mouse sulla cartella CallHome Query Group (Gruppi di query CallHome) e selezionare Create CallHome Query Group (Crea gruppo di query CallHome).

## Create Callhome Query Group

Name:

### Add Queries

Name	Query Type	DN or Class Name	Query Target	Response Subtree	Response Subtree Include
 					

Cancel

Submit

- Definire il nome del gruppo di query e fare clic sul segno+per creare la definizione della query.
  - Nome: nome della query
  - Tipo: il selettore del tipo di oggetto che verrà monitorato per rilevare le modifiche. Ho selezionato qui che significa "nome distinto".
  - DN o Nome classe: nome dell'oggetto monitorato. Ed è qui che la magia entra in azione! Non è disponibile alcuna descrizione del tipo di nome dell'oggetto o di qualsiasi altro elemento da inserire in questo campo. In APIC versione precedente 4 questo campo non era obbligatorio. Dalla versione 4 è obbligatorio. Se abbiamo selezionato dnforType, allora possiamo mettere qui letteralmente che significa "Intero universo" o in altre parole - "Tutti gli oggetti di tessuto".
  - Destinazione: seleziona se è necessario includere le informazioni della sottostruttura per l'oggetto restituito dalla query. Ho selezionato il sottotree.
  - Struttura secondaria: seleziona gli oggetti della struttura secondaria che devono essere restituiti dalla query. Io ho completamente selezionato qui.
  - Include - tipo di oggetti che verranno restituiti dalla query. Io ho selezionato tutti.

# Create Query



Name:

Type:  class  dn

DN or Class Name:

Target:  children  self  subtree

Response Subtree:  children  full  no

Response Subtree Include:

- add-mo-list
- audit-logs
- config-only
- count
- custom-path-hop
- deployment
- deployment-records
- ep-records
- event-logs
- fault-count
- fault-records
- faults
- full-deployment
- health
- health-records
- local-prefix
- no-scoped
- pending-deployment
- port-deployment
- record-subtree
- relations
- relations-with-parent
- required
- state
- stats
- tags
- tasks

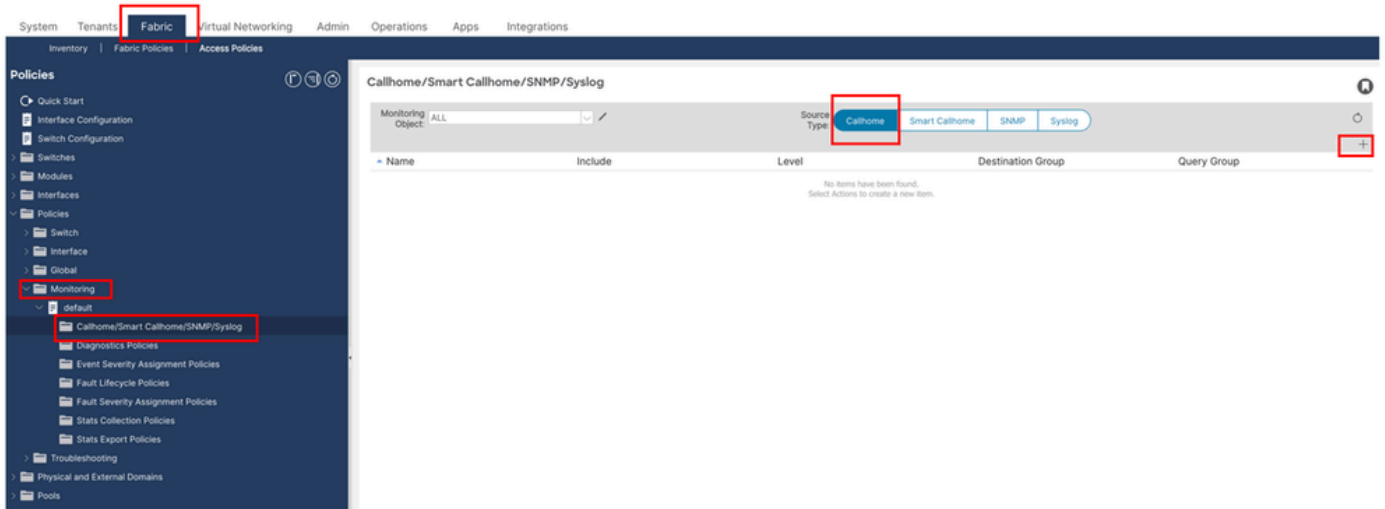
Cancel

OK

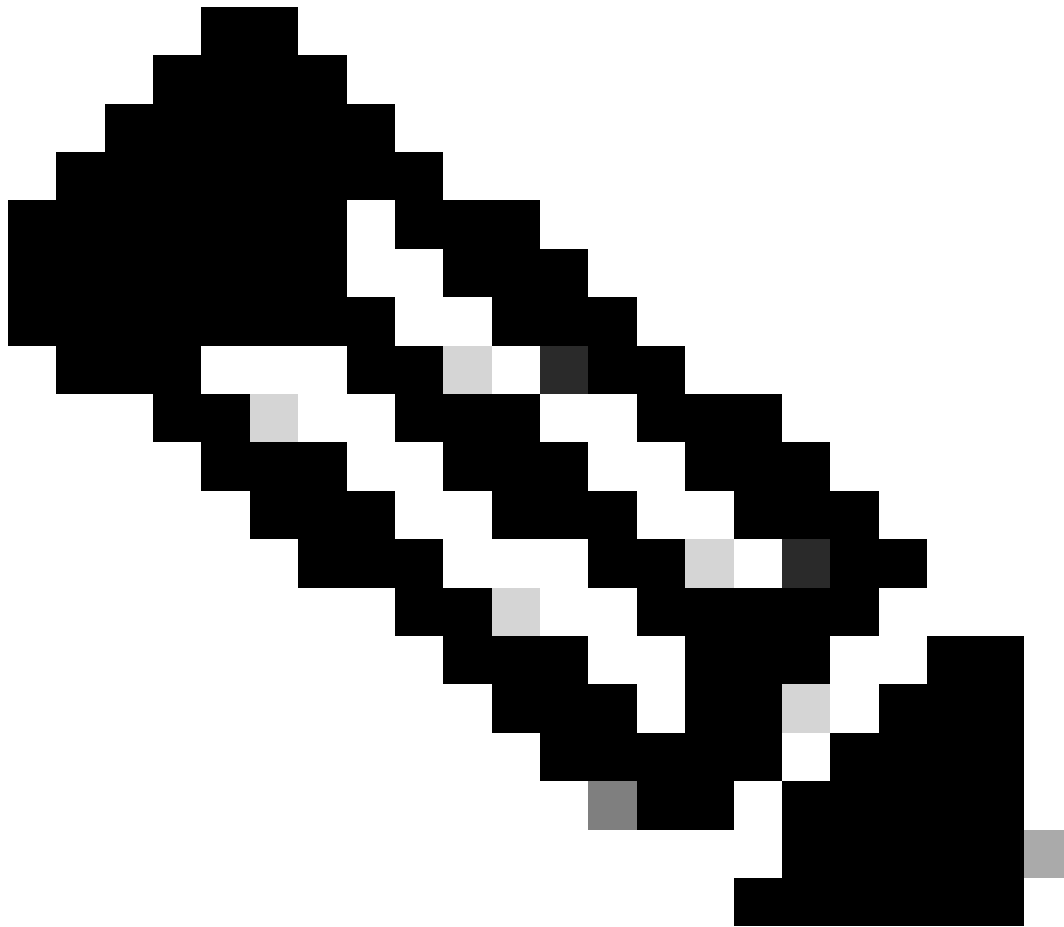
Passaggio 5: criteri di monitoraggio fabric e creazione di origini CallHome

Ora che le destinazioni CallHome e le query sono state configurate, è possibile passare alla modifica dei criteri di monitoraggio.

- Selezionare APIC > Fabric > Fabric Policies > Policies > Monitoring (Policy di infrastruttura)
- Assicurarsi che il valore "ALL" sia selezionato nella casella di riepilogo a discesa "Oggetto di monitoraggio" e che "Tipo di origine" sia impostato su "CallHome".



- Fai clic su +accedi nella parte destra del riquadro di destra
  - Nome: nome origine CallHome (Callhome\_Source)
  - Includi: selezionare il tipo di notifiche da ricevere
  - Livello: gravità dell'evento che attiva l'azione (livello selezionato o superiore)
  - Gruppo di destinazione - qui , selezionare il gruppo di destinazione CallHome creato in precedenza
  - Gruppo di query: selezionare qui il gruppo di query CallHome creato prima
- Fare clic su Invia.



Nota: Al termine dell'installazione, è possibile ottimizzare i criteri di monitoraggio creando origini CallHome separate per oggetti di monitoraggio diversi e utilizzando più gruppi di destinazione e query CallHome

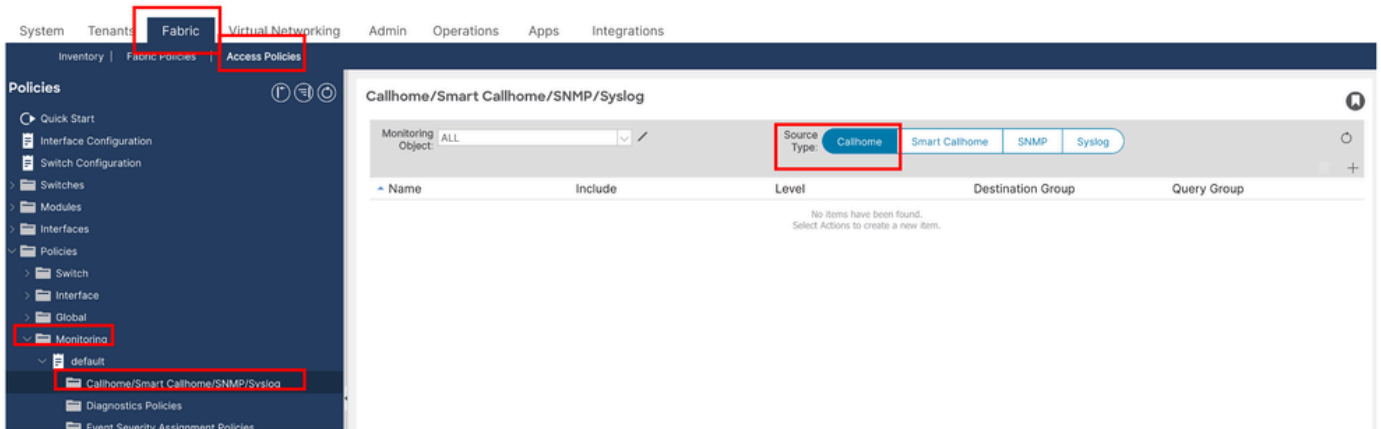
---

#### Passaggio 6: origini CallHome dei criteri di accesso

In questa sezione verranno configurati i criteri di accesso all'infrastruttura per creare origini CallHome.

Selezionare APIC > Fabric > Criteri di accesso > Criteri > Monitoraggio

- Nella cartella Monitoraggio sono disponibili i criteri di monitoraggio predefiniti. Aprire il criterio predefinito, fare clic sulla cartella CallHome/Smart CallHome/SNMP/Syslog/TACACS.
- Verificare che ALL sia selezionato nell'elenco a discesa Oggetto di monitoraggio e che Source Type sia impostato su CallHome.



- Fare clic su+accedi nella parte più a destra del riquadro di destra:
  - Nome: immettere il nome dell'origine CallHome (`Access_CallHome`)
  - Includi: selezionare il tipo di notifiche da ricevere
  - Livello: gravità dell'evento che attiva l'azione (livello selezionato o superiore)
  - Gruppo di destinazione: selezionare il gruppo di destinazione CallHome creato in precedenza
  - Gruppo di query: selezionare il gruppo di query CallHome creato in precedenza

# Create Callhome Source



Name:

Include:

- Audit logs
- Events
- Faults
- Session logs

Level:

Destination Group:

Query Group:

Passaggio 7: Dopo aver apportato queste modifiche, dobbiamo ricevere avvisi e-mail sull'ID e-mail configurato.

## Risoluzione dei problemi e verifica

### 1. Verifica connettività server SMTP

Per verificare che i dispositivi APIC e Leaf possano raggiungere il server SMTP tramite la porta TCP 25, eseguire i test ping e telnet.

#### 1.1 Test Ping

Utilizzare i comandi seguenti per verificare la raggiungibilità di base della rete all'host SMTP:

Su APIC:

```
<#root>
```

```
APIC # ping x.x.x.x
```

Su interruttore foglia:

```
<#root>
```

```
Leaf# iping x.x.x.x
```

## 1.2 Test Telnet (porta 25)

Eseguire i comandi seguenti per verificare che la porta SMTP 25 sia aperta e raggiungibile:

Su APIC:

```
APIC # curl -v telnet://smtp_server_ip:port
```

Example :

```
APIC# curl -v telnet://x.x.x.x:25
```

Su interruttore foglia:

```
Leaf# icurl -v telnet://smtp_server_ip:port
```

Example:

```
Leaf# icurl -v telnet://x.x.x.x:25
```

## 2. Convalida della configurazione CallHome

Verificare che CallHome sia configurato correttamente su entrambi gli switch APIC e foglia.

### 2.1 Convalida del profilo CallHome

Verificare che il profilo sia configurato con la porta e i parametri corretti:

Su APIC:

```
<#root>
```

```
Apic# moquery -c callhomeProf
```

Su interruttore foglia:

```
<#root>
```

```
Leaf# moquery -c callhomeProf
```

## 2.2 Convalida destinazione CallHome

Verificare che la porta e il server SMTP di destinazione siano impostati correttamente:

Su APIC:

```
<#root>
```

```
Apic# moquery -c callhomeDest
```

Su interruttore foglia:

```
<#root>
```

```
Leaf# moquery -c callhomeDest
```

## 3. Verifica della trasmissione della posta elettronica CallHome

In una struttura ACI tipica, i messaggi CallHome vengono avviati da APIC2 in un cluster a tre nodi. Se APIC2 non è disponibile, questi messaggi possono provenire da uno switch foglia. Per confermare l'origine e la trasmissione dei messaggi CallHome, usare `tcpdump` sulle interfacce interessate.

### 3.1 Da APIC (accesso root richiesto)

Se è configurata la gestione in banda, sostituire `bond0.330` con la VLAN utilizzata per la gestione in banda:

```
Apic# tcpdump -i bond0.330 port 25
```

Da Interruttore foglia:

Utilizzare l'interfaccia kpm\_inb per monitorare il traffico SMTP in uscita:

```
Leaf# tcpdump -i kpm_inb port 25
```

4. In alcuni casi, anche dopo la corretta configurazione e verifica di CallHome, della connettività SMTP e delle policy di monitoraggio, non possiamo ricevere avvisi di guasto dell'interfaccia via e-mail.

Per risolvere il problema, procedere come segue:

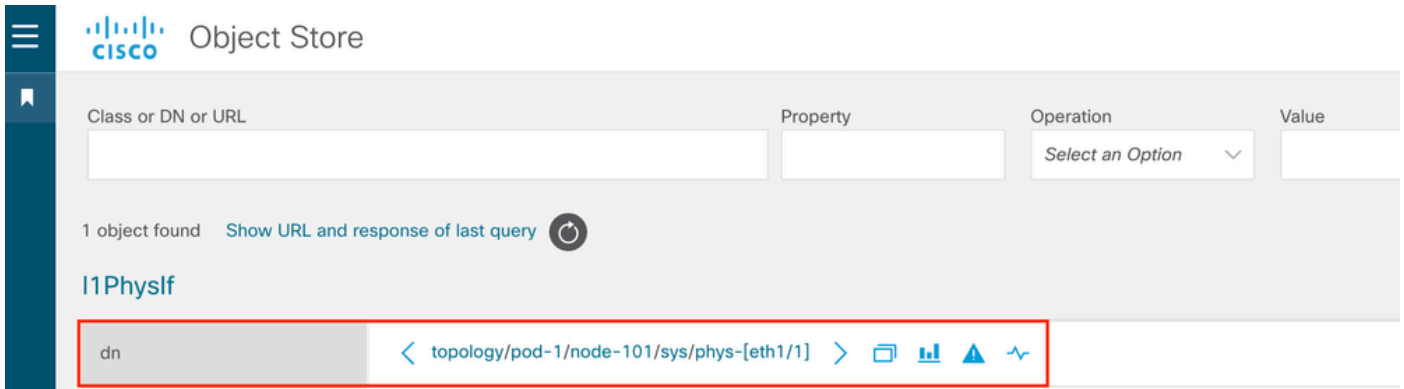
Utilizzare il browser dell'archivio oggetti per esaminare l'errore.

4.1 Passare all'interfaccia interessata nell'interfaccia utente di Cisco ACI.

4.2 Fare clic con il pulsante destro del mouse sull'interfaccia e selezionare "Open in Object Store Browser" (fare riferimento alla schermata seguente per una guida visiva).

The screenshot displays the Cisco ACI web interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Fabric' tab is active, and the 'Inventory' section is expanded to show 'Fabric Policies' and 'Access Policies'. The left sidebar shows a tree view of the network inventory, with 'Physical Interfaces' expanded to show a list of interfaces from eth1/1 to eth1/12. A context menu is open over the 'eth1/1' interface, listing various actions such as 'Enable', 'Disable', 'Turn On Locator LED', 'Turn Off Locator LED', 'Reset', 'Deploy Static EPG', 'Save as ...', 'Post ...', and 'Share'. The 'Open in Object Store Browser' option is highlighted with a red rectangular box. The main content area shows the configuration page for 'Layer 1 Physical Interface Configuration - 101/eth1/1', which is currently in an 'Operational' state. A small status card for the interface shows a green '100' and several colored icons.

4.3 Nel Visualizzatore archivio oggetti, individuare il Nome distinto (DN) associato all'oggetto di errore.



4.4 Dopo aver identificato il DN, accedere alla CLI di APIC ed eseguire il seguente comando per eseguire una query sui dettagli dell'oggetto:

Esempio:-

```
apic# moquery -d "topology/pod-1/node-101/sys/phys-[eth1/1]"
```

4.5. Nell'output del comando precedente, individuare il campo `monPo1Dn`.

Ad esempio:

```
monPo1Dn : uni/infra/moninfra-default
```

Questo campo indica il nome distinto (DN) del criterio di monitoraggio applicato all'oggetto interfaccia.

4.6 In questo esempio, la politica di monitoraggio è la seguente: `uni/infra/moninfra-default`

Ciò indica che il criterio di monitoraggio predefinito nel tenant Infra viene applicato all'interfaccia.

4.7 Per garantire che CallHome generi e invii avvisi in caso di guasti all'interfaccia:

Verificare che la configurazione CallHome sia presente nel tenant Infra.

Verificare che il criterio di monitoraggio (`moninfra-predefinito` in questo caso) sia collegato a un profilo CallHome configurato correttamente.

System **Tenants** Fabric Virtual Networking Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or desc | common | Test | **infra** | rjl\_repro | mgmt

**infra**

- Quick Start
- infra
  - Application Profiles
  - Networking
  - Contracts
  - Policies
    - Protocol
    - Troubleshooting
    - Host Protection
    - Monitoring
      - default
        - Stats Collection Policies
        - Stats Export Policies
        - Callhome/Smart Callhome/SNMP/Syslog**
        - Event Severity Assessment Policies

**Callhome/Smart Callhome/SNMP/Syslog**

Monitoring Object: ALL Source Type: Callhome Smart Callhome SNMP Syslog

Name	Include	Level	Destination Group	Query Group
No items have been found. Select Actions to create a new item.				

## 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).