

# Callhome configureren, verifiëren en problemen oplossen in ACI Fabric

## Inhoud

---

[Inleiding](#)

[begrip](#)

[Voorwaarden](#)

[Configuratiestappen](#)

[Problemen oplossen en verificatie](#)

---

## Inleiding

Dit document beschrijft de configuratie van Call home in een Cisco ACI-omgeving.

## begrip

De CallHome-functie stelt ons in staat om via e-mail kritische meldingen te ontvangen over de functionaliteit van de fabric, inclusief diagnostische informatie en omgevingsfouten of -gebeurtenissen. Het levert deze waarschuwingen aan meerdere ontvangers via CallHome-bestemmingsprofielen, die kunnen worden geconfigureerd met specifieke berichtformaten en inhoudscategorieën.

## Voorwaarden

- De stof moet op 4.2(1) of hoger staan.
- Alle fabric-apparaten moeten een netwerkverbinding hebben met de SMTP/E-mailserver.
- Communicatie TCP-poort 25 moet zijn toegestaan tussen fabric-apparaten en SMTP/E-mailserver.

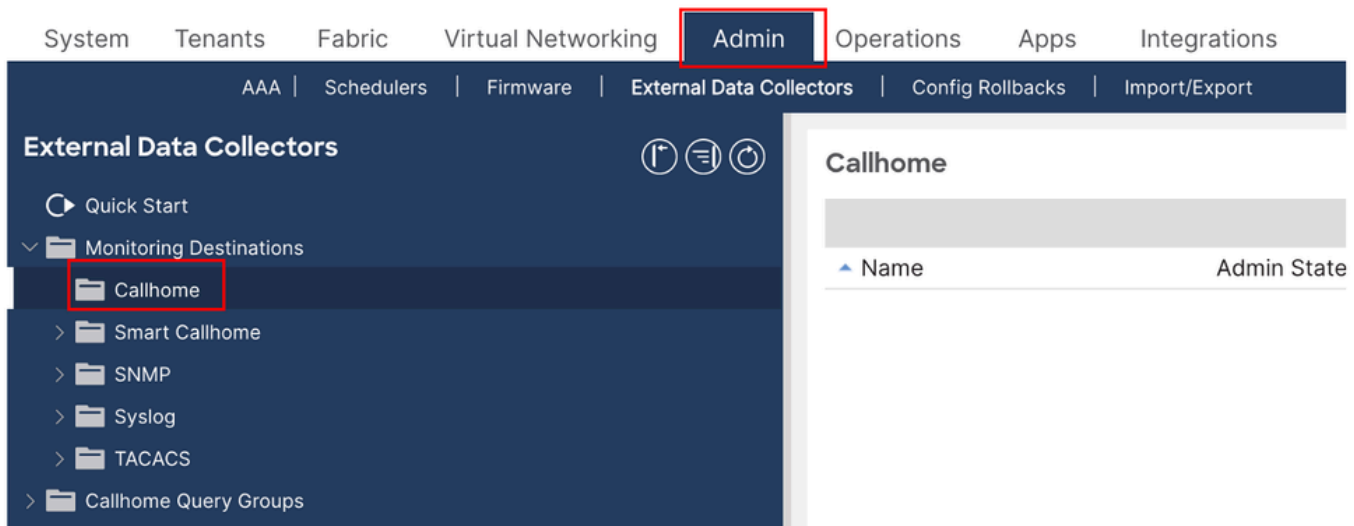
## Configuratiestappen

Stap 1: Log in bij APIC.

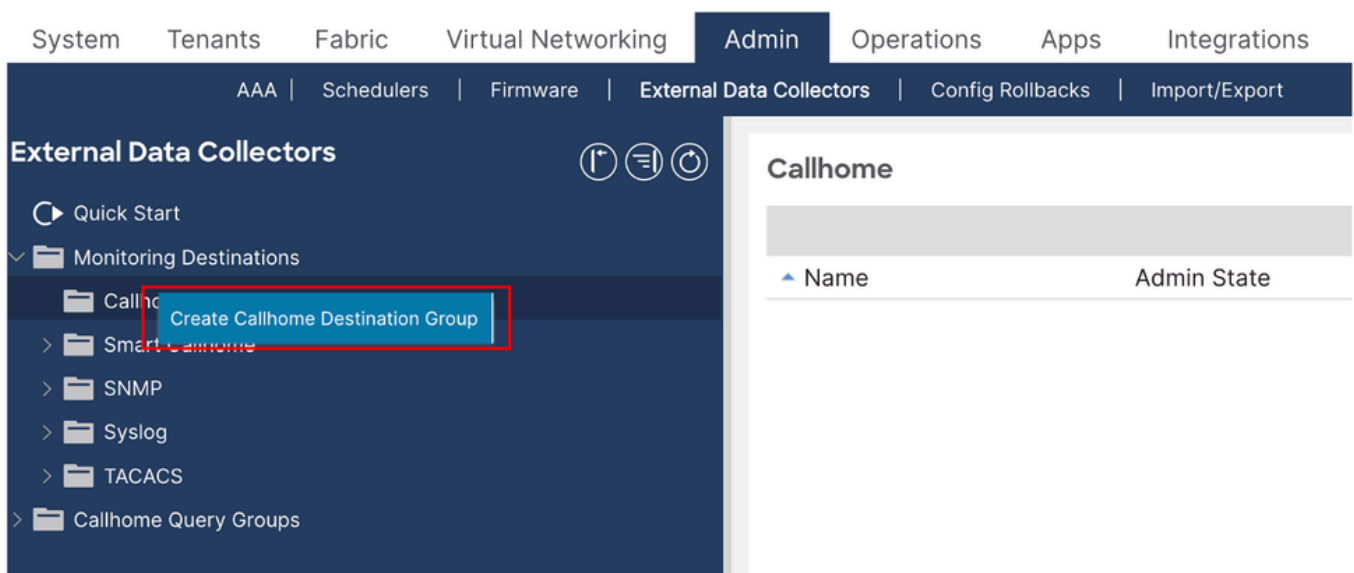
- Toegang tot APIC met beheerdersreferenties.

Stap 2: Maak een CallHome-bestemmingsgroep aan.

- Navigeer naar APIC > Beheer > Externe gegevensverzamelaars > Bestemming bewaken



- Klik met de rechtermuisknop op CallHomeFolder en selecteer Create CallHome Destination Group.



Stap 3: Voer de gewenste gegevens in.

Vereiste details worden hieronder vermeld

- Naam - Naam van bestemmingsgroep CallHome
- Admin - schakel deze optie in
- Poort - 25, Poortnummer waarop SMTP zal communiceren.
- SMTP-server - DNS-naam of IP-adres van SMTP-server
- Van E-mail - e-mailadres van welke stof ons berichten zal sturen
- EPG-beheer - oob of inb EPG die bereikbaar is voor onze SMTP-server
- Contact E-mail - e-mailadres waarop berichten worden ontvangen


## 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"/> <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

- Op de volgende pagina kunnen we exacte bestemmingen maken (dat wil zeggen ontvangers van CallHome-berichten).
- Klik op + teken en vul velden in
  - Naam- bestemmingsnaam
  - Beheerdersstatus - als deze is uitgeschakeld, ontvangt de bestemming geen berichten
  - Niveau - prioriteitsniveau van berichten die naar de bestemming worden verzonden. Ik zou aanraden deze optie in te stellen op fout of hoger. De tabel met ernstniveaus wordt hieronder weergegeven.
  - E-mail - Huidig e-mailadres waar berichten moeten worden verzonden
  - Formaat - als we niet van plan zijn om inkomende berichten automatisch te ontleden, stel dit dan in op short-txt. We kunnen experimenteren om de verschillen tussen hen te zien.
  - Maximale grootte (bytes) - maximale grootte van één e-mailbericht. In het geval dat we Format instellen op aml of xml dan kunnen berichten vrij groot zijn, dus aantal 100-200KB zijn ok. We kunnen experimenteren met dit aantal om de vereiste grootte te bepalen. Voor short-txt formaat moet het voldoende zijn om dit in te stellen op 10KB.
  - RFC Compliant - Beter te zeggen maakt dit niet mogelijk.

## 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

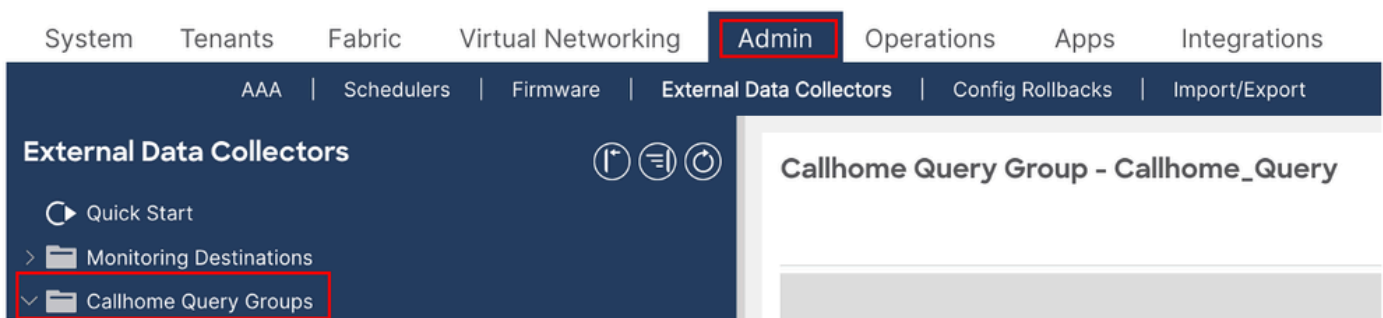
- We kunnen zoveel bestemmingen maken als we nodig hebben en kunnen er ook meer maken door met de rechtermuisknop op onze CallHome-bestemmingsgroep te klikken en CallHome-bestemming maken te selecteren.

# 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

## Stap 4: Callhome-querygroepen maken

- Navigeer naar APIC > Beheer > Externe gegevensverzamelaars > CallHome-querygroepen



- Klik met de rechtermuisknop op de map CallHome Query Groups en selecteer CallHome

Query Group maken.

## Create Callhome Query Group

Name:

Add Queries

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

- Definieer de naam van de querygroep en klik op + teken om een querydefinitie te maken.
  - Naam- querynaam
  - Type- selector van objecttype dat wordt gecontroleerd op wijzigingen. Ik heb gekozen voor wat "voornaam naam" betekent.
  - DN- of klassenaam- naam van bewaakt object. En dat is waar de magie in actie komt! We zullen nergens een beschrijving vinden van wat voor soort objectnaam of wat dan ook in dit veld moet worden ingevoegd. In APIC eerdere versie 4 was dit veld niet vereist. Vanaf versie 4 is het verplicht. Als we hebben gekozen voorType, dan kunnen we hier zetten wat letterlijk betekent "Hele universum" of met andere woorden - "Alle stoffen objecten".
  - Doel- Hiermee wordt geselecteerd of substructuurinformatie moet worden opgenomen voor object dat door query wordt geretourneerd. Ik heb hier een substraat geselecteerd.
  - Subtree - selecteert subboomobjecten die moeten worden geretourneerd uit de query. Ik heb hier volledig voor gekozen.
  - Inclusief - type objecten dat per query wordt geretourneerd. Ik heb ze allemaal geselecteerd.

# 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

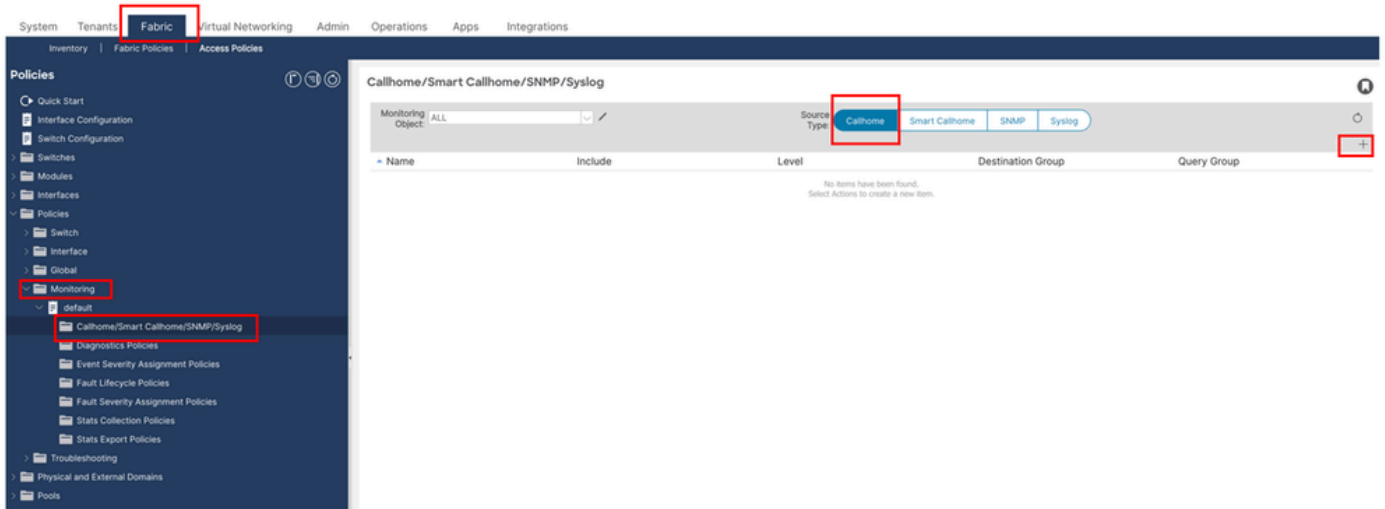
Cancel

OK

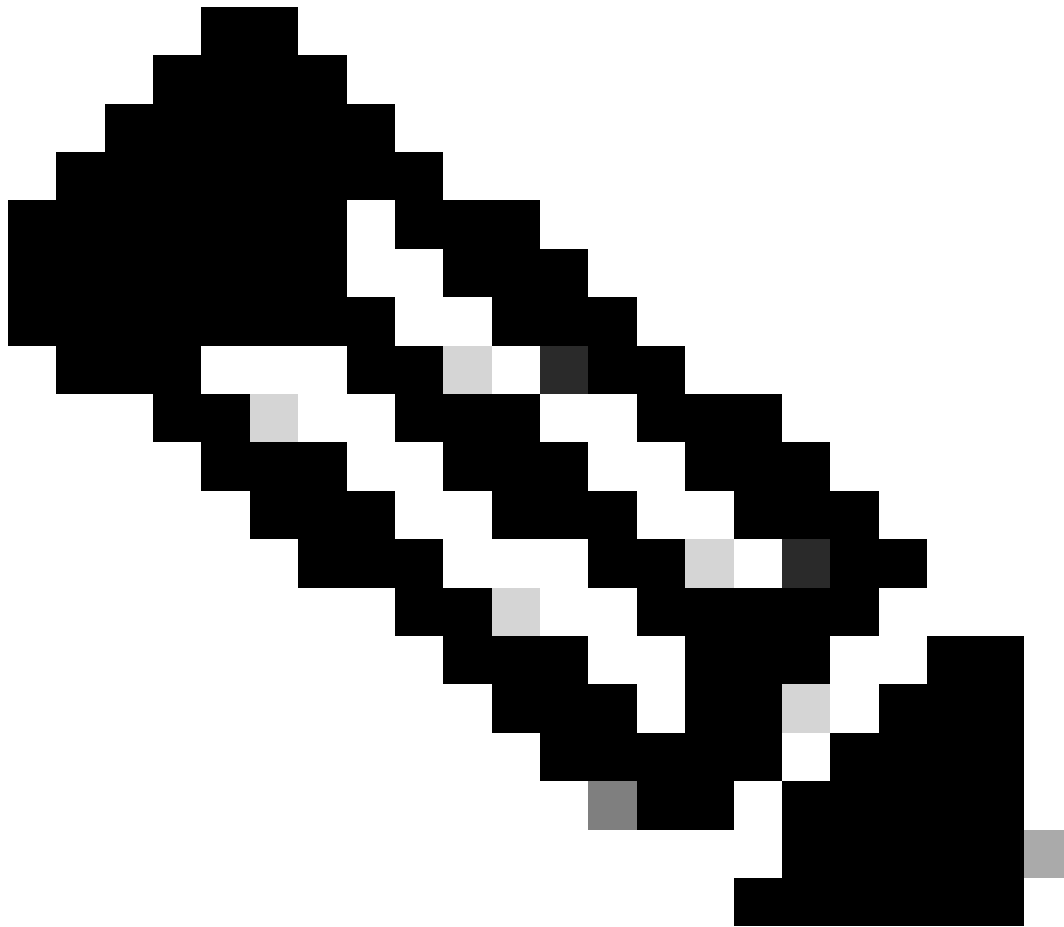
## Stap 5: Fabric Monitoring-beleid en CallHome-bronnen maken

Nu CallHome-bestemmingen en -query's zijn geconfigureerd, kunnen we doorgaan met het bewerken van het bewakingsbeleid.

- Navigeer naar APIC > Fabric > Fabric Policies > Policies > Monitoring
- Zorg ervoor dat de waarde "ALL" is geselecteerd in de vervolgkeuzelijst "Object bewaken" en dat "Brontype" is ingesteld op "CallHome".



- Klik op +inloggen rechts in het grootste deel van het rechterdeelvenster
  - Naam - Naam CallHome Bronnaam (Callhome\_Source)
  - Inclusief: selecteer welk soort meldingen u wilt ontvangen
  - Niveau - ernst van de gebeurtenis die actie zal activeren (geselecteerd niveau of hoger)
  - Bestemmingsgroep - selecteer hier de CallHome-bestemmingsgroep die eerder is gemaakt
  - Querygroep- selecteer hier de groep CallHome Query die eerder is gemaakt
- Klik op Indienen.



Opmerking: Als de installatie is voltooid, kunnen we ons monitoringbeleid verfijnen door afzonderlijke CallHome-bronnen te maken voor verschillende monitoringobjecten en meerdere CallHome-doelgroepen en -query's te gebruiken

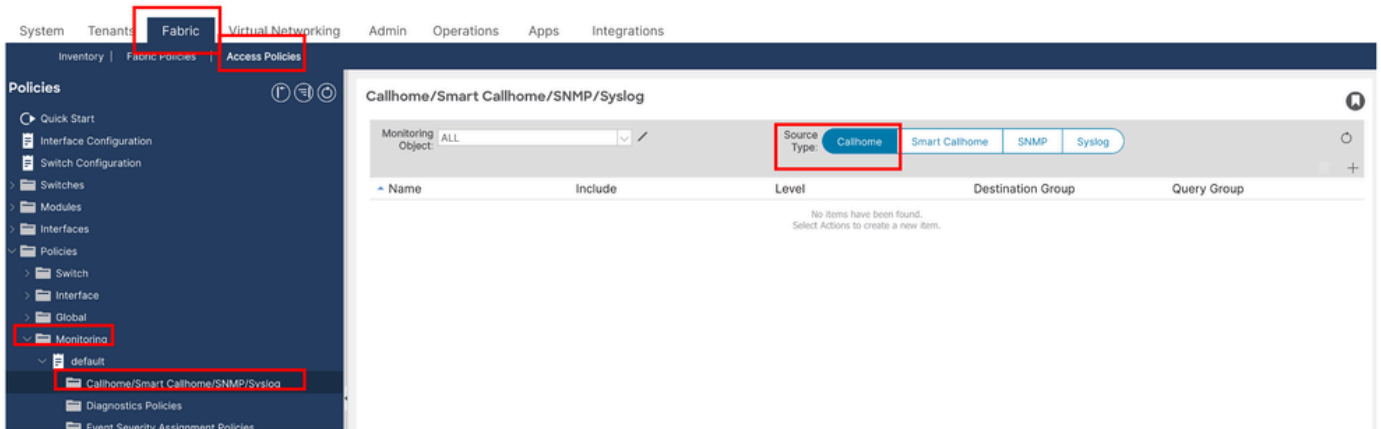
---

## Stap 6: Toegangsbeleid CallHome bronnen

In deze sectie zullen we het toegangsbeleid voor verbindingen configureren om CallHome-bronnen te maken.

Navigeer naar APIC > Fabric > Access Policies > Policies > Monitoring

- In de map Monitoring vinden we het standaardcontrolebeleid. Open het standaardbeleid en klik op de map CallHome/Smart CallHome/SNMP/Syslog/TACACS.
- Zorg ervoor dat ALL is geselecteerd in de vervolkeuzelijst Object bewaken en dat het brontype is ingesteld op CallHome.



- Klik op +aanmelden rechts in het grootste deel van het rechterdeelvenster:
  - Naam - Voer de bronnaam van CallHome in (`Access_CallHome`)
  - Opnemen - selecteer welk soort meldingen moeten worden ontvangen
  - Niveau - ernst van de gebeurtenis die actie zal activeren (geselecteerd niveau of hoger)
  - Bestemmingsgroep - hier selecteren we de CallHome-bestemmingsgroep die we eerder hebben gemaakt
  - Querygroep - hier selecteren we de CallHome-querygroep die we eerder hebben gemaakt

# Create Callhome Source



Name:

Include:

- Audit logs
- Events
- Faults
- Session logs

Level:

Destination Group:

Query Group:

Cancel

Submit

Stap 7: Nadat u deze wijzigingen hebt aangebracht, moeten we e-mailberichten ontvangen op de geconfigureerde e-mail-ID.

## Problemen oplossen en verificatie

### 1. Verificatie van de connectiviteit van de SMTP-server

Om te bevestigen dat zowel APIC- als Leaf-apparaten de SMTP-server kunnen bereiken via TCP-poort 25, voert u ping- en telnet-tests uit.

#### 1.1 Ping-test

Gebruik de onderstaande opdrachten om de bereikbaarheid van het basisnetwerk voor de SMTP-

host te controleren:

Over APIC:

```
<#root>
```

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

Op Leaf Switch:

```
<#root>
```

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

## 1.2 Telnet-test (poort 25)

Voer de volgende opdrachten uit om te controleren of SMTP-poort 25 open en bereikbaar is:

Over APIC:

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

Example :

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

Op Leaf Switch:

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

Example:

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

## 2. Validatie van de CallHome-configuratie

Controleer of CallHome correct is geconfigureerd op zowel de APIC- als de leaf-switch.

### 2.1 Validatie van het CallHome-profiel

Controleer of het profiel is geconfigureerd met de juiste poort en parameters:

Over APIC:

<#root>

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

Op Leaf Switch:

<#root>

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

## 2.2 Validatie van de bestemming van de oproep naar huis

Controleer of de SMTP-bestemmingsserver en -poort nauwkeurig zijn ingesteld:

Over APIC:

<#root>

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

Op Leaf Switch:

<#root>

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

## 3. Verificatie van e-mailverzending van CallHome

In een typische ACI-structuur worden CallHome-berichten geïnitieerd vanuit APIC2 in een cluster met drie knooppunten. Als APIC2 niet beschikbaar is, kunnen deze berichten afkomstig zijn van een switch. Om de bron en verzending van CallHome-berichten te bevestigen, gebruikt u `tcpdump` op de relevante interfaces.

### 3.1 Van APIC (Root Access vereist)

Als inbandbeheer is geconfigureerd, vervangt u `bond0.330` door het VLAN dat wordt gebruikt voor inbandbeheer:

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

Van Leaf Switch:

Gebruik de interface `kpm_inb` om het uitgaande SMTP-verkeer te controleren:

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

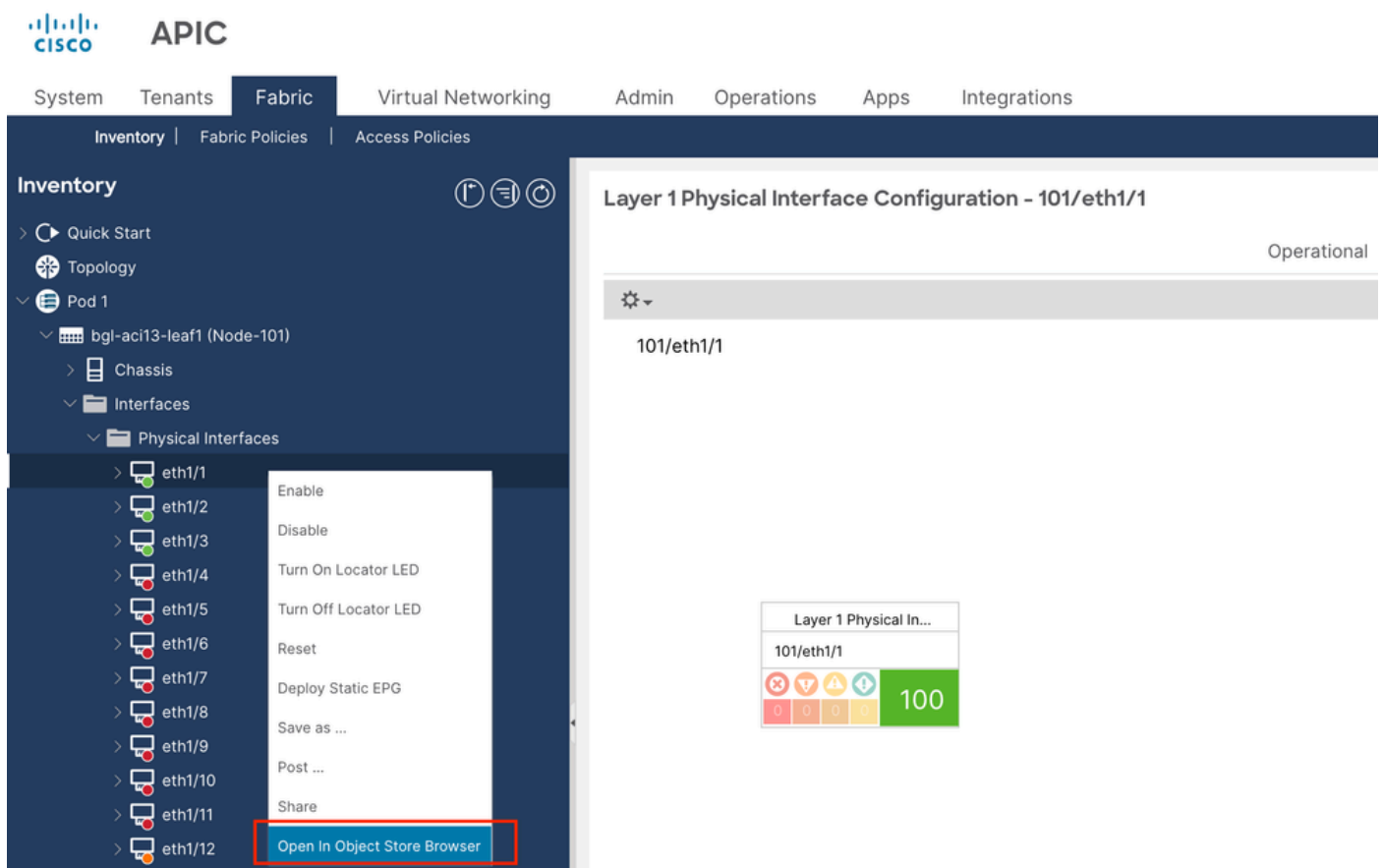
4. In bepaalde gevallen, zelfs na succesvolle configuratie en verificatie van CallHome, SMTP-connectiviteit en monitoringbeleid, kunnen we geen foutmeldingen van de interface via e-mail ontvangen.

Gebruik de onderstaande stappen om problemen op te lossen:

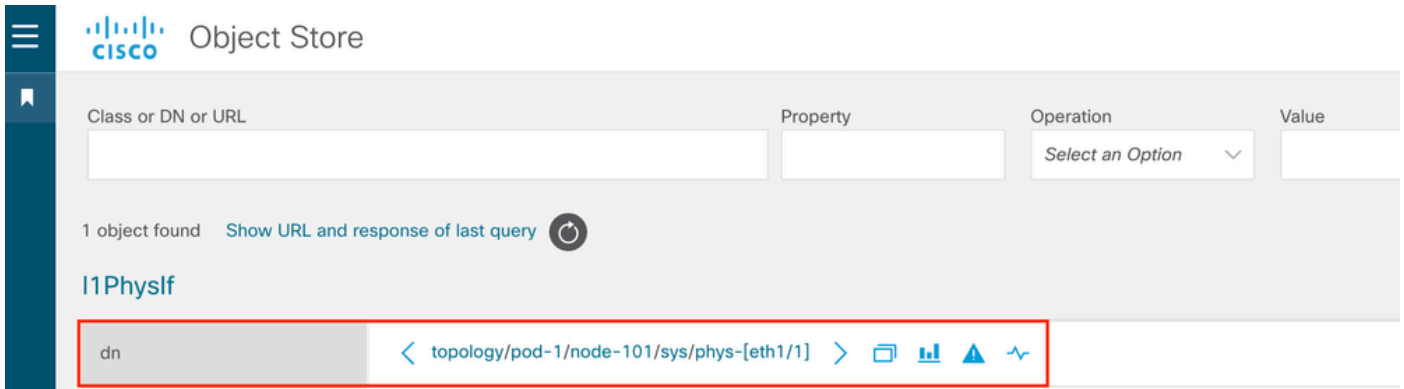
Gebruik de Object Store Browser om de fout te inspecteren.

4.1 Navigeer naar de betreffende interface in de Cisco ACI GUI.

4.2 Klik met de rechtermuisknop op de interface en selecteer "Open in Object Store Browser" (raadpleeg de onderstaande schermafbeelding voor visuele begeleiding).



4.3 Zoek in de Object Store Browser de DN (Distinguished Name) die aan het object met de fout is gekoppeld.



4.4 Nadat u de DN hebt geïdentificeerd, opent u de APIC CLI en voert u de volgende opdracht uit om gegevens voor het object op te vragen:

Voorbeeld: -

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

4.5. Zoek in de uitvoer van de vorige opdracht het veld `monPo1Dn`.

Voorbeeld:

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

Dit veld geeft de onderscheidende naam (DN) voor het bewakingsbeleid aan die op het interfaceobject is toegepast.

4.6 In dit voorbeeld is het monitoringbeleid: `uni/infra/moninfra-default`

Hieruit blijkt dat het standaardcontrolebeleid onder de Infra-tenant wordt toegepast op de interface.

4.7 Om ervoor te zorgen dat CallHome waarschuwingen voor interfacefouten genereert en verzendt:

Bevestig dat de CallHome-configuratie aanwezig is onder de Infra-tenant.

Zorg ervoor dat het controlebeleid (`moninfra-standaard` in dit geval) is gekoppeld aan een correct geconfigureerd CallHome-profiel.

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.				

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.