Konfiguration, Verifizierung und Fehlerbehebung von Callhome in der ACI-Fabric

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von Call Home in einer Cisco ACI-Umgebung beschrieben.

Konzept

Die CallHome-Funktion ermöglicht es uns, per E-Mail wichtige Benachrichtigungen über Fabric-Funktionen zu erhalten, einschließlich Diagnoseinformationen und Umgebungsfehlern oder -ereignissen. Diese Warnmeldungen werden über CallHome-Zielprofile, die mit bestimmten Nachrichtenformaten und Inhaltskategorien konfiguriert werden können, an mehrere Empfänger gesendet.

Voraussetzungen

- Die Fabric muss Version 4.2(1) oder höher sein.
- Alle Fabric-Geräte müssen über eine Netzwerkverbindung zum SMTP-/E-Mail-Server verfügen.
- Kommunikation Der TCP-Port 25 muss zwischen den Fabric-Geräten und dem SMTP-/E-Mail-Server zugelassen werden.

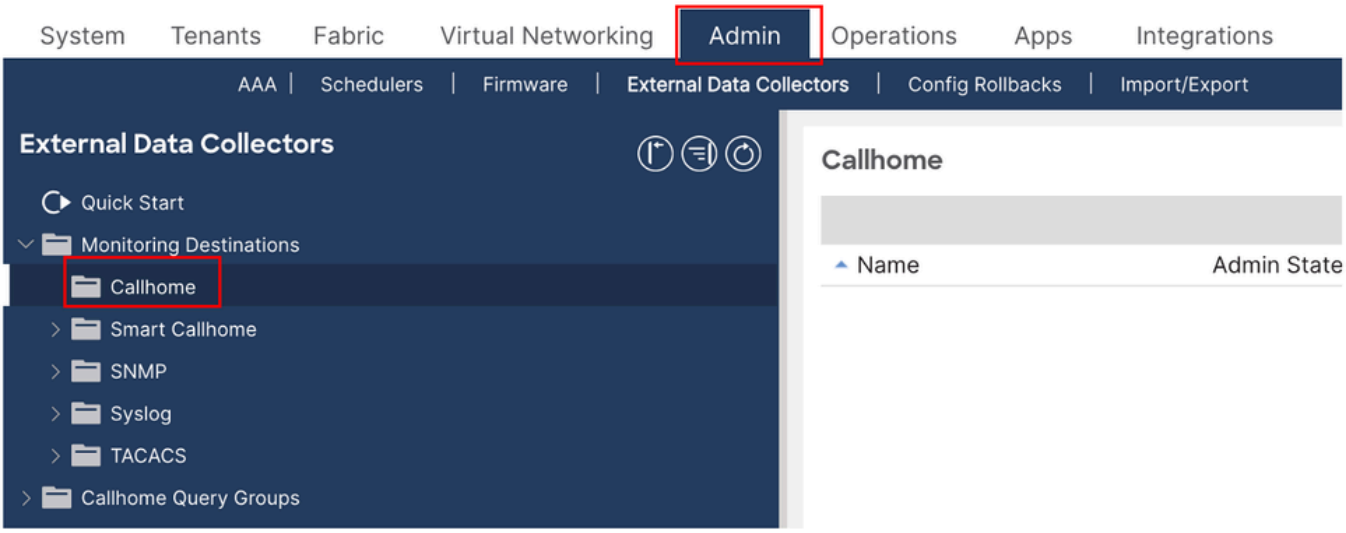
Konfigurationsschritte

Schritt 1: Melden Sie sich beim APIC an.

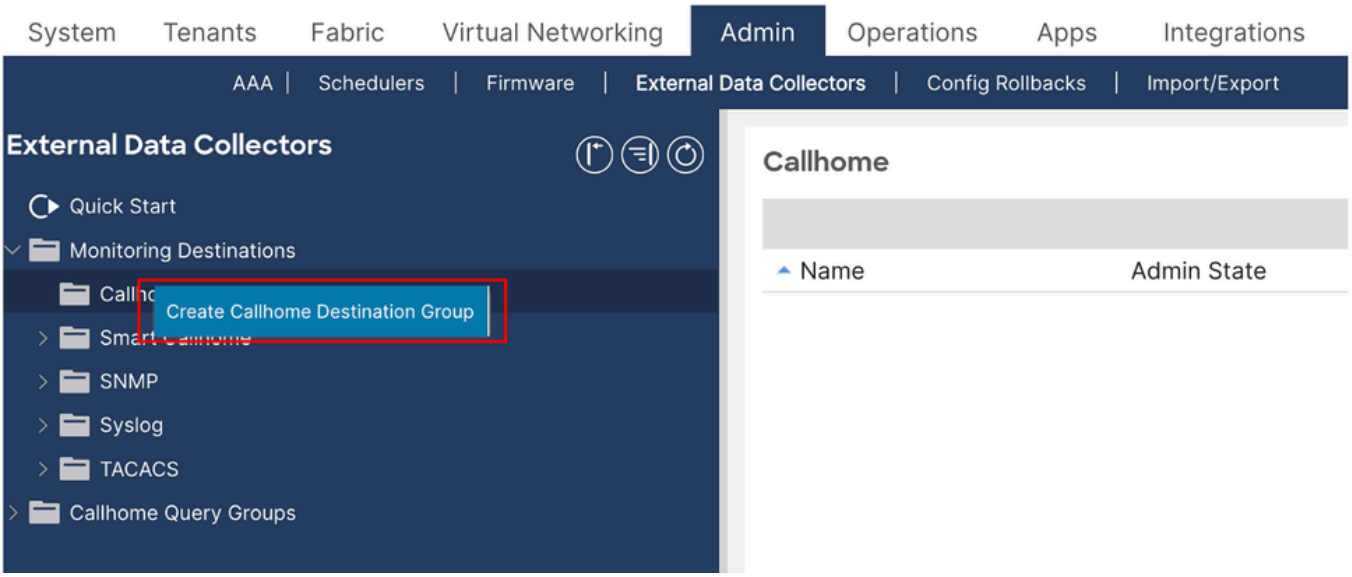
- Zugreifen auf den APIC mit Administratoranmeldeinformationen

Schritt 2: Erstellen einer CallHome-Zielgruppe

- Navigieren Sie zu APIC > Admin > External Data Collectors > Monitoring Destination.



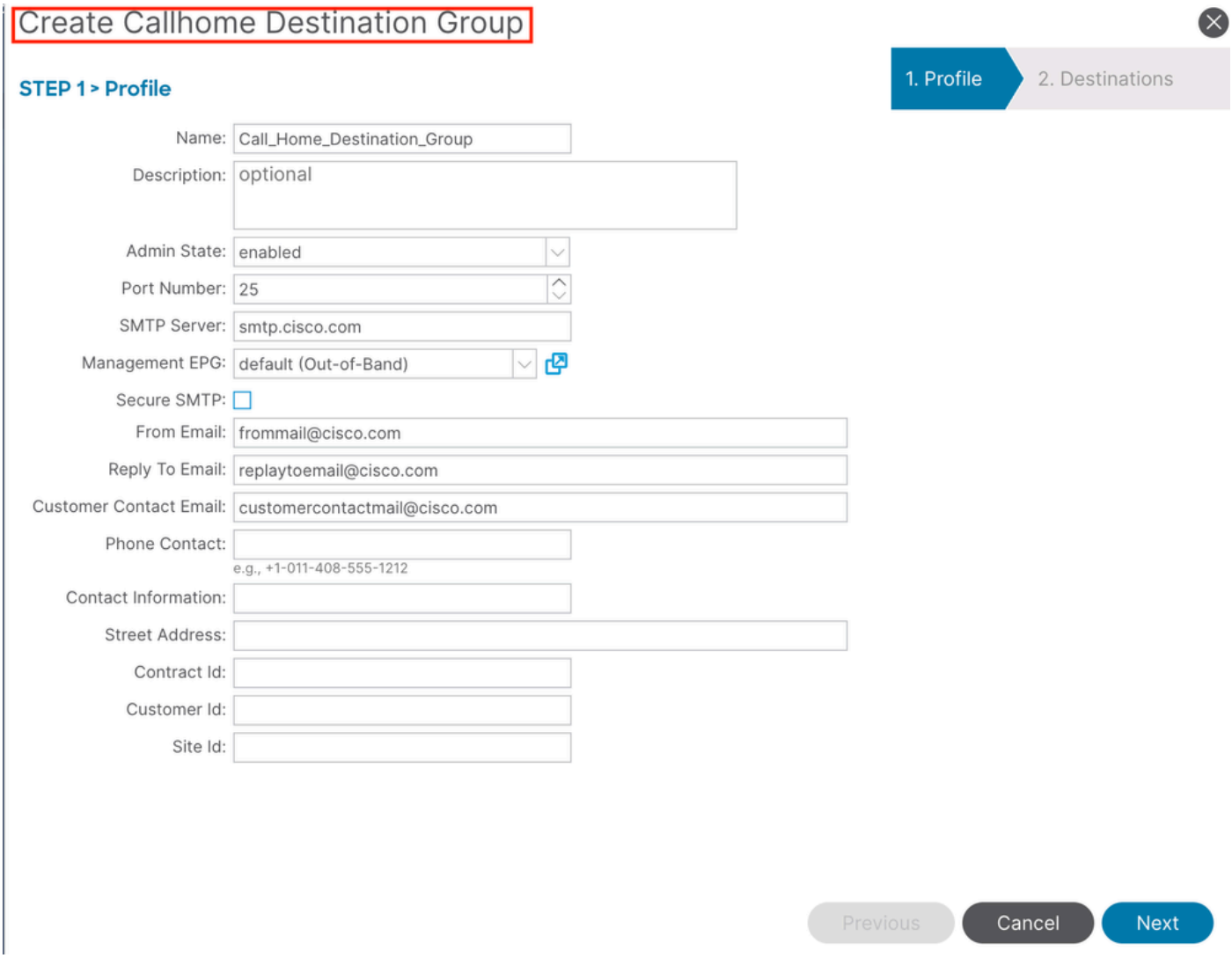
- Klicken Sie mit der rechten Maustaste auf CallHome-Ordner, und wählen Sie Create CallHome Destination Group (CallHome-Zielgruppe erstellen).



Schritt 3: Geben Sie die erforderlichen Details ein.

Die erforderlichen Details sind unten aufgeführt.

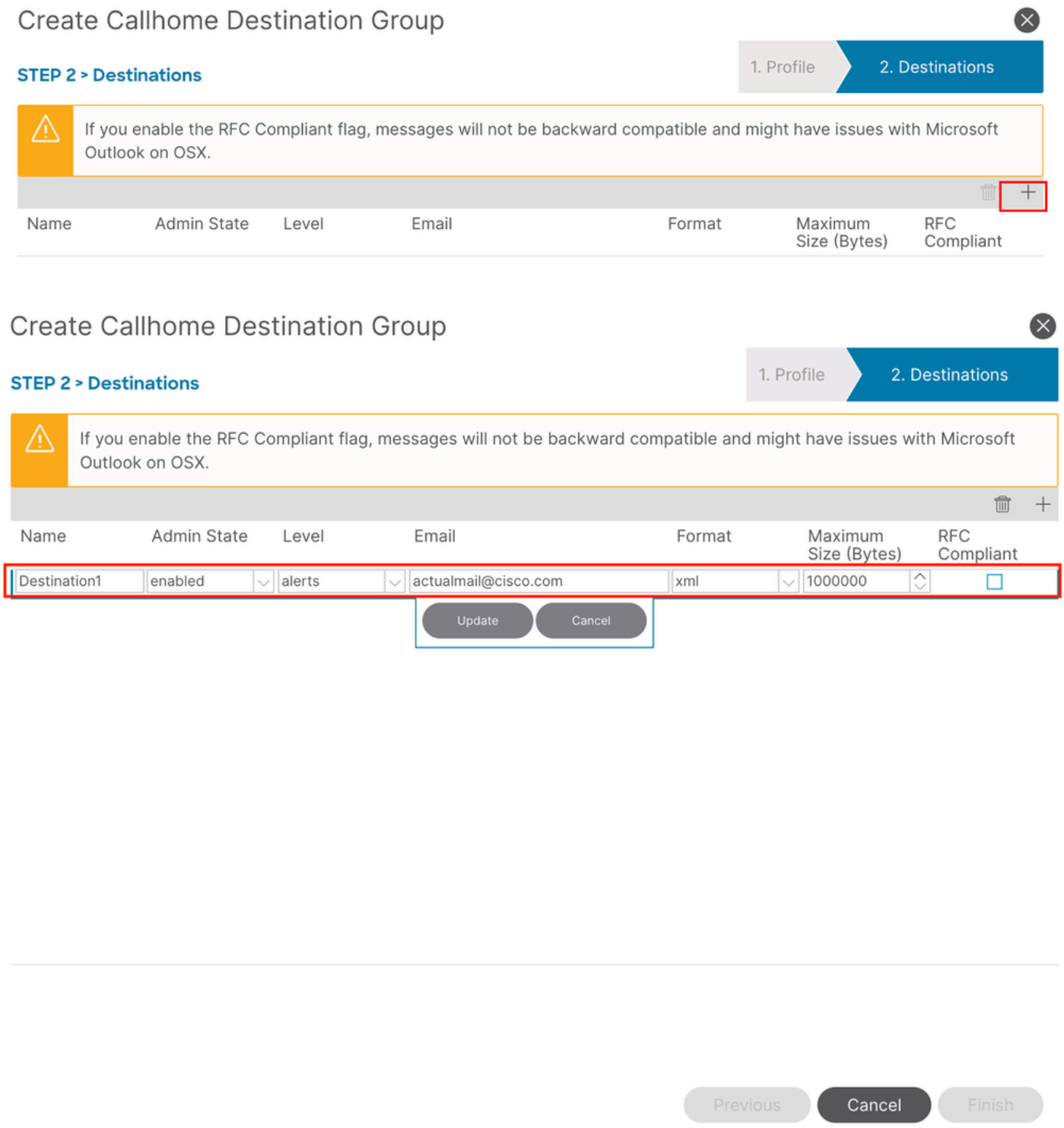
- Name - Name der CallHome-Zielgruppe
- Admin: Aktivieren Sie diese Option.
- Port - 25, Portnummer, über die SMTP kommuniziert.
- SMTP-Server - DNS-Name oder IP-Adresse des SMTP-Servers
- Von E-Mail - E-Mail-Adresse, von der die Fabric uns Nachrichten sendet
- Management-EPG - OOB- oder INB-EPG mit Erreichbarkeit unseres SMTP-Servers
- E-Mail-Adresse des Kontakts - E-Mail-Adresse, an die die Nachrichten empfangen werden



- Auf der nächsten Seite können wir genaue Ziele erstellen (d. h. Empfänger von CallHome-Nachrichten).
- Klicken Sie auf + Vorzeichen und füllen Sie Felder

    - Name - Zielname

    - Admin-Status - Wenn deaktiviert, erhält das Ziel keine Nachrichten.
    - Ebene: Der Schweregrad der Nachrichten, die an das Ziel gesendet werden. Ich würde empfehlen, diese Einstellung auf error oder höher zu setzen. Die Tabelle mit den Schweregraden finden Sie unten.
    - E-Mail - Die tatsächliche E-Mail-Adresse, an die Nachrichten gesendet werden müssen
    - Formatieren: Wenn keine automatische Analyse eingehender Nachrichten geplant ist, legen Sie "short-text" fest. Wir können experimentieren, um die Unterschiede zwischen ihnen zu sehen.
    - Maximale Größe (Byte): Die maximale Größe einer einzelnen E-Mail-Nachricht. Falls wir Format auf aml oder xml setzen, dann können Nachrichten ziemlich groß sein, sodass die Anzahl von 100-200KB in Ordnung ist. Wir können mit dieser Zahl experimentieren, um die erforderliche Größe zu bestimmen. Für die Kurztextformatierung muss es ausreichen, diesen Wert auf 10KB zu setzen.
    - RFC-konform - besser gesagt, aktiviert dies nicht.



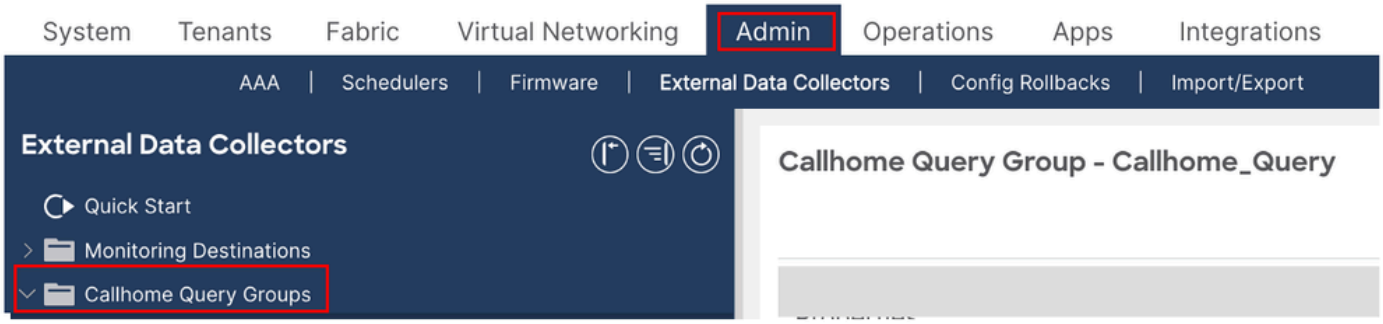
- Sie können beliebig viele Ziele erstellen. Sie können auch weitere Ziele erstellen, indem Sie mit der rechten Maustaste auf die CallHome-Zielgruppe klicken und CallHome-Ziel erstellen auswählen.

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

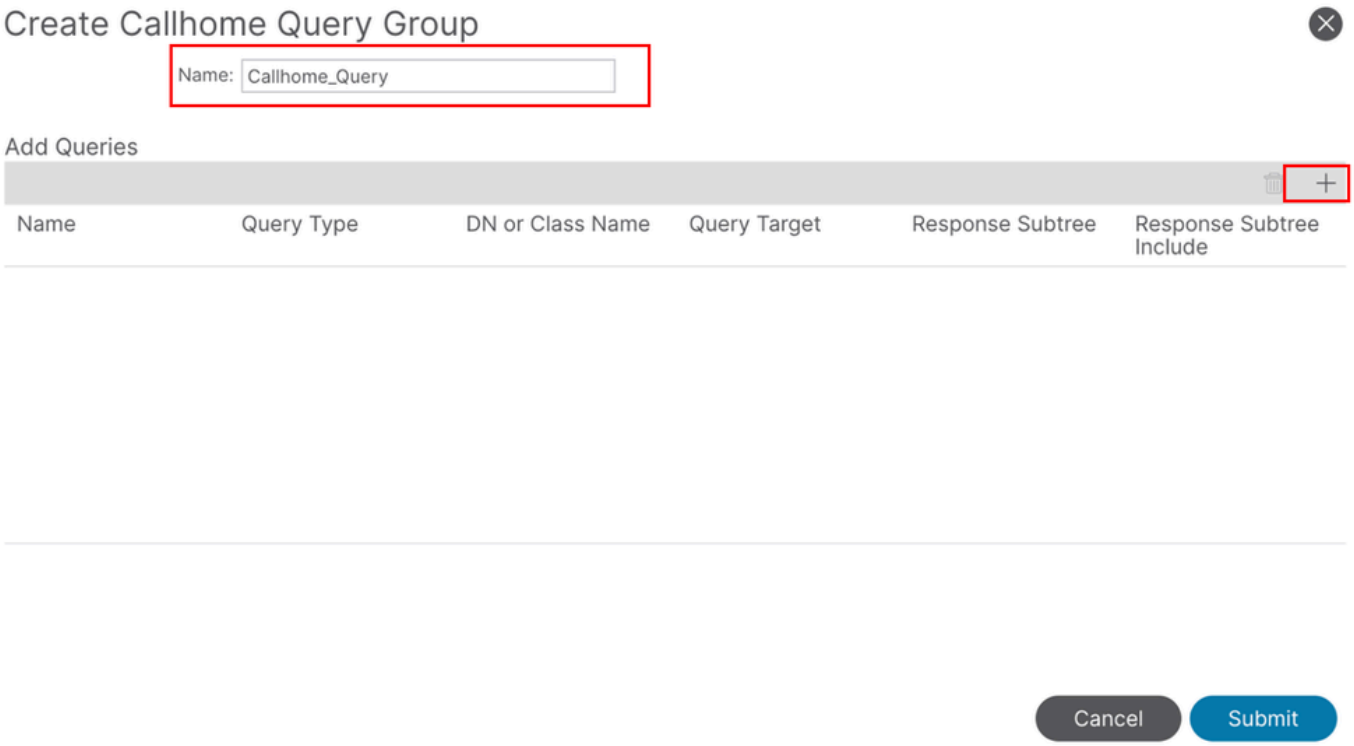
Schritt 4: Erstellen von CallHome-Abfragruppen

- Navigieren Sie zu APIC > Admin > External Data Collectors > CallHome-Abfragegruppen.

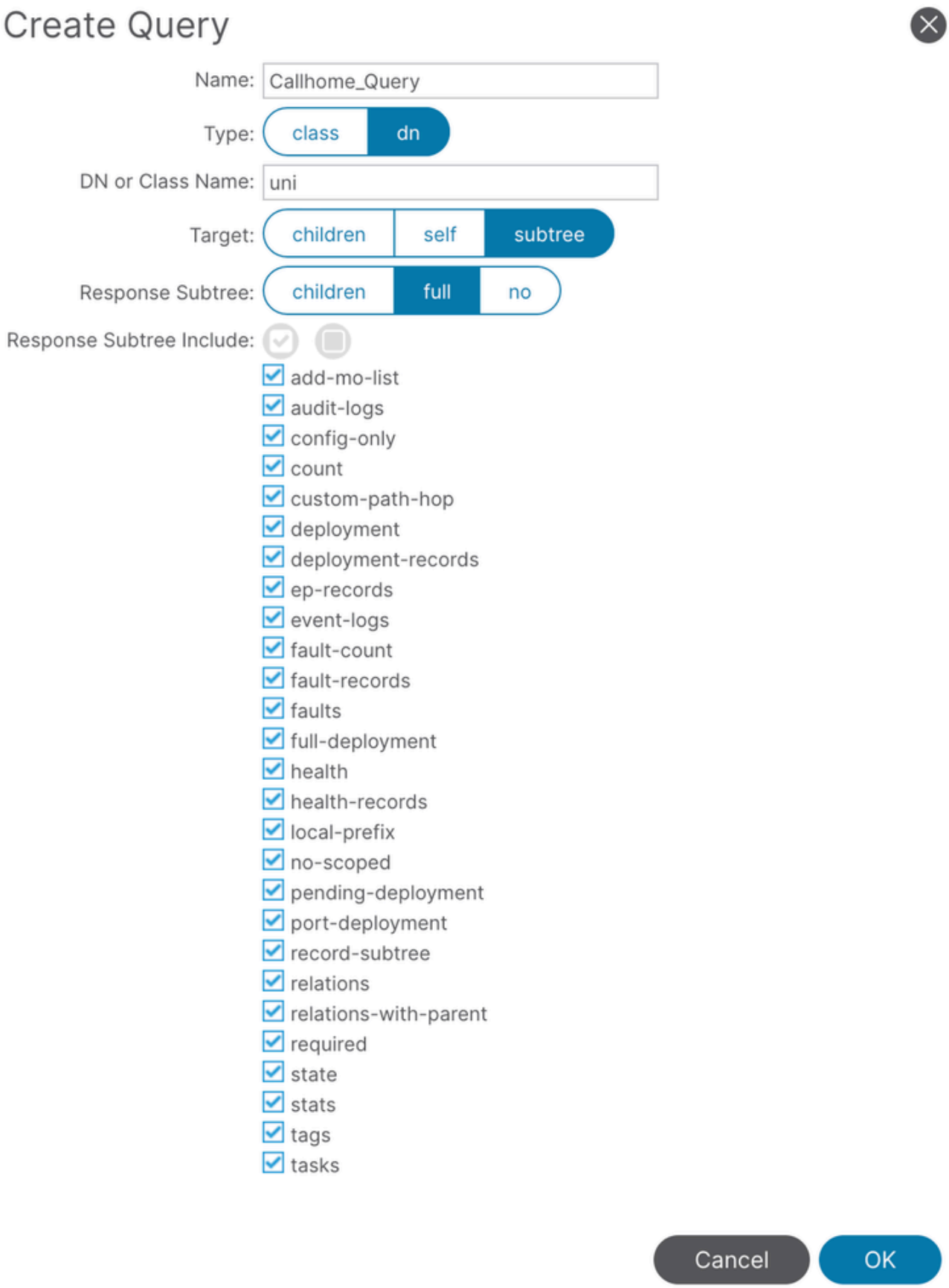


- Klicken Sie mit der rechten Maustaste auf den Ordner CallHome-Abfragegruppen, und

wählen Sie CallHome-Abfragegruppe erstellen aus.



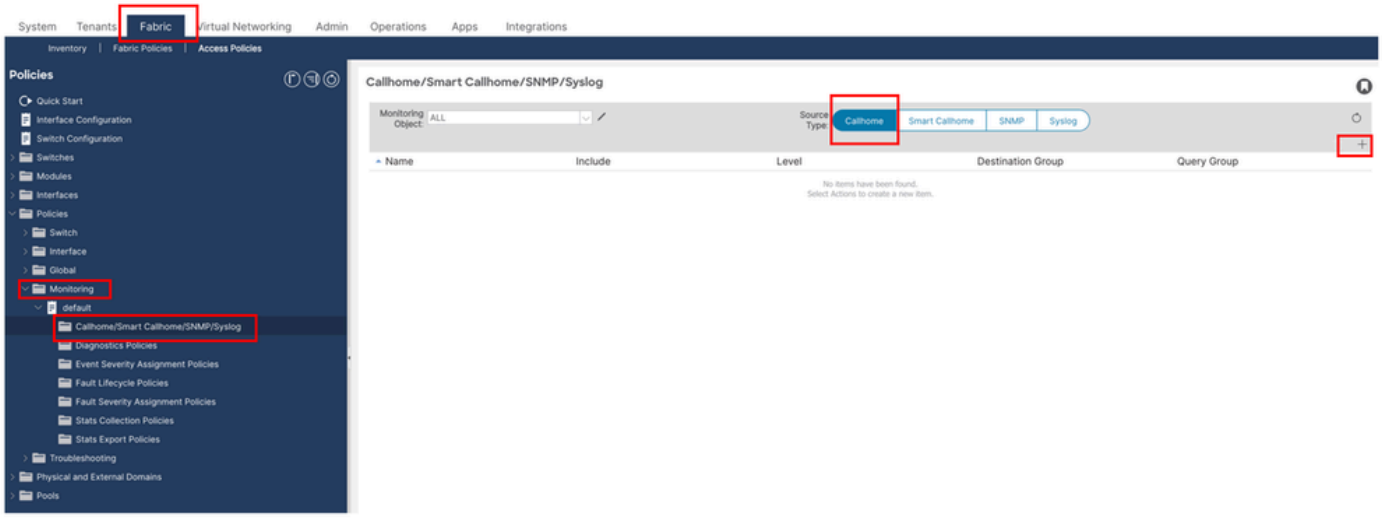
- Definieren Sie den Namen der Abfragegruppe, und klicken Sie auf +Zeichen, um eine Abfragedefinition zu erstellen.
  - Name - Abfragename
  - Typ- Auswahl des Objekttyps, der auf Änderungen überwacht wird. Ich habe hier ausgewählt, was "Distinguished Name" bedeutet.
  - DN oder Klassenname - Name des überwachten Objekts. Und hier kommt der Zauber zum Tragen! Wir werden keine Beschreibung finden, welche Art von Objektnamen oder was auch immer in dieses Feld eingefügt werden muss. In der vorherigen APIC Version 4 war dieses Feld nicht erforderlich. Ab Version 4 ist es obligatorisch. Wenn wir dnforType ausgewählt haben, dann können wir hierunidas wörtlich "Ganzes Universum" oder mit anderen Worten - "Alle Gewebeobjekte" bedeutet hierin setzen.
  - Target: Diese Option wählt aus, ob Subtree-Informationen für das von der Abfrage zurückgegebene Objekt eingeschlossen werden müssen. Ich habe hier einen Unterordner ausgewählt.
  - Unterbaum: Wählt Unterbaumobjekte aus, die von der Abfrage zurückgegeben werden müssen. Ich habe hier eine vollständige Auswahl getroffen.
  - Include - Typ der Objekte, die von der Abfrage zurückgegeben werden. Ich habe alle ausgewählt.



Schritt 5: Fabric-Überwachungsrichtlinien und Erstellen von CallHome-Quellen

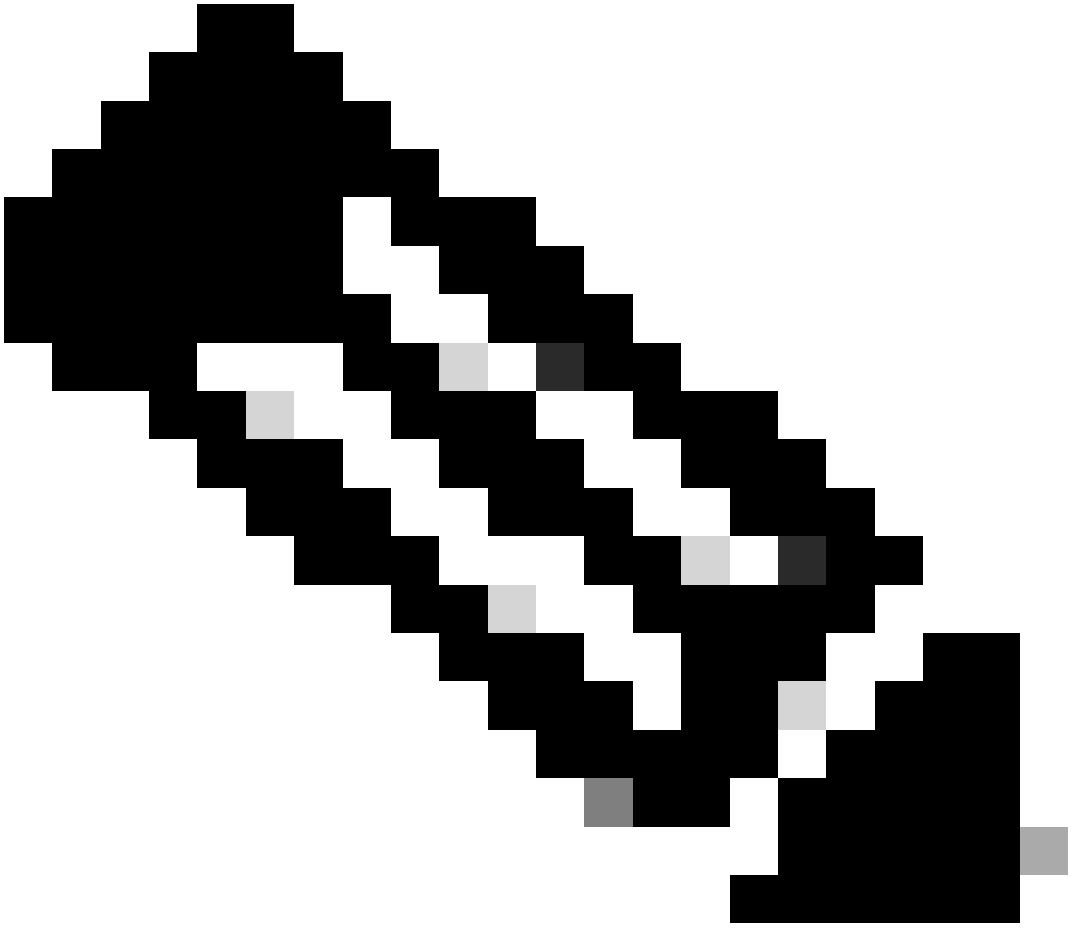
Nachdem CallHome-Ziele und -Abfragen konfiguriert wurden, können wir nun die Überwachungsrichtlinie bearbeiten.

- Navigieren Sie zu APIC > Fabric > Fabric Policies > Policies > Monitoring.
- Stellen Sie sicher, dass der Wert "ALL" in der Dropdown-Liste "Monitoring Object" (Überwachungsobjekt) ausgewählt und "Source Type" (Quelltyp) auf "CallHome" (CallHome) festgelegt ist.



- Klicken Sie auf+Anmelden im rechten Bereich.
  - Name - Name der CallHome-Quelle (Callhome_Source)
  - Einschließen: Wählen Sie aus, welche Arten von Benachrichtigungen empfangen werden sollen.
  - Ebene: Ereignisschweregrad, der eine Aktion auslöst (ausgewählte Ebene oder höher)
  - Zielgruppe - Wählen Sie hier CallHome-Zielgruppe aus, die zuvor erstellt wurde.
  - Abfragegruppe - Wählen Sie hier die zuvor erstellte CallHome-Abfragegruppe aus.

- Klicken Sie auf Senden.



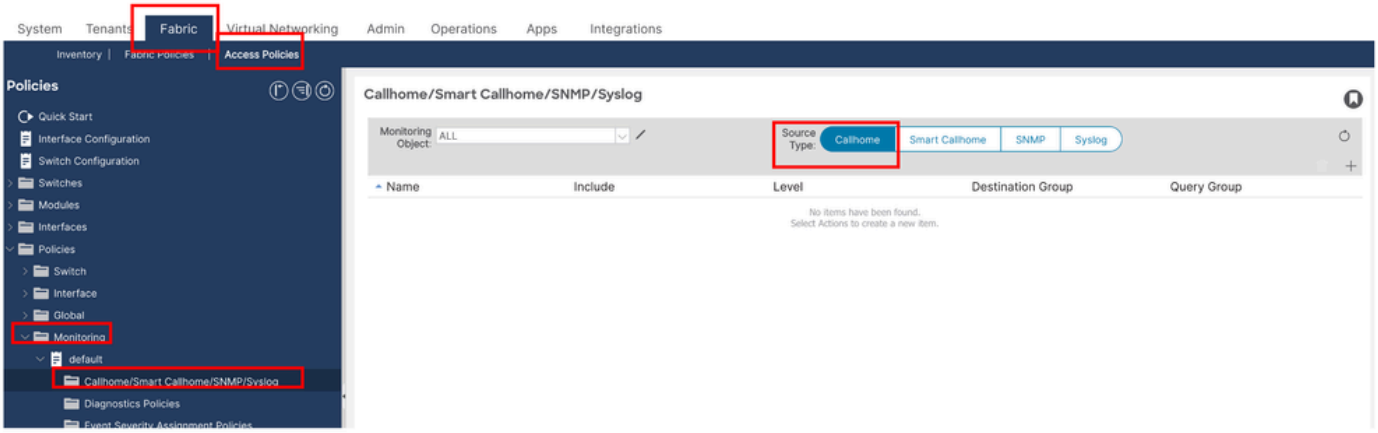
Anmerkung: Nach Abschluss der Einrichtung können wir unsere Überwachungsrichtlinie weiter anpassen, indem wir separate CallHome-Quellen für verschiedene Überwachungsobjekte erstellen und mehrere CallHome-Zielgruppen und -Abfragen verwenden.

Schritt 6: Zugriffsrichtlinien CallHome-Quellen

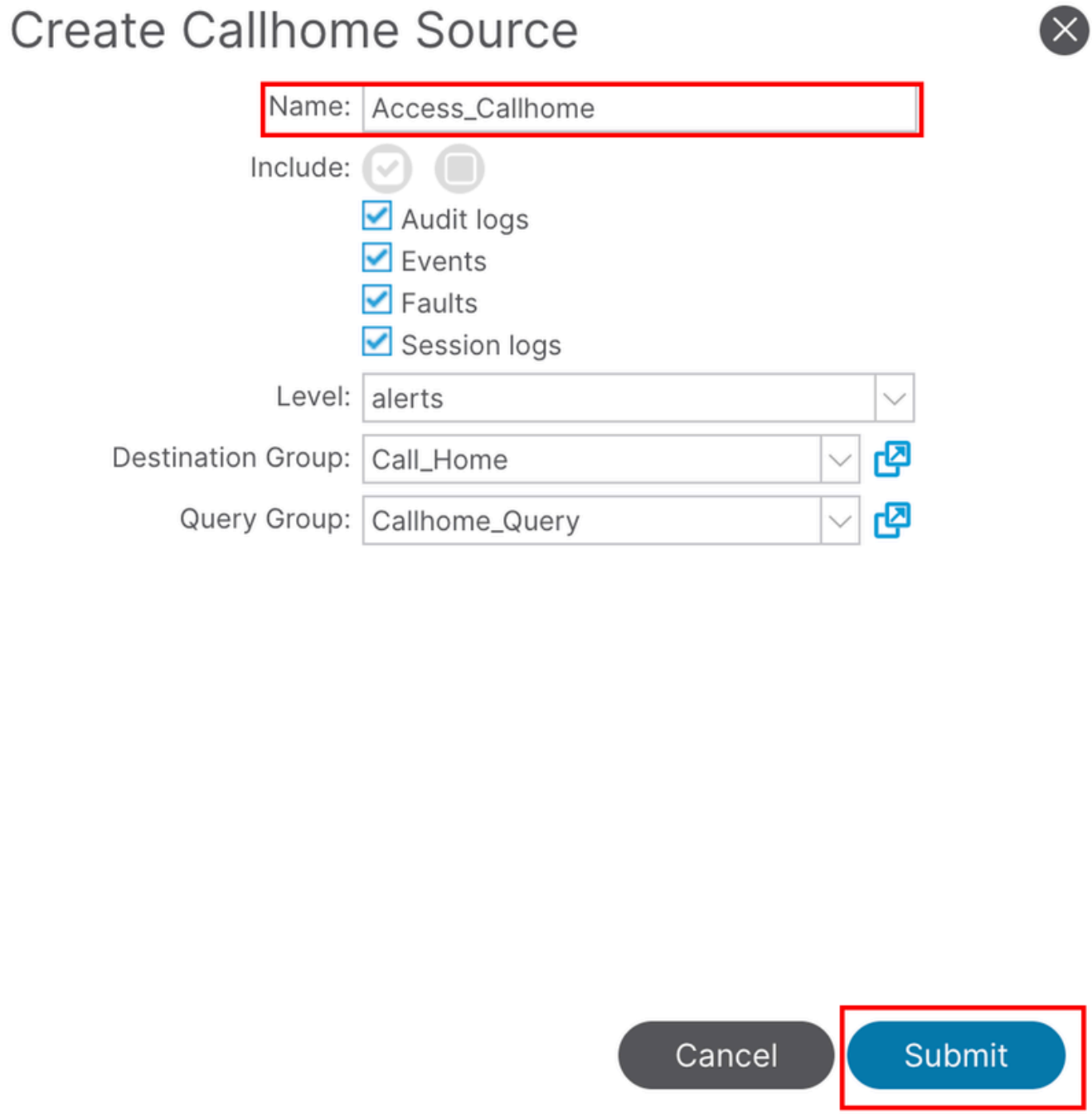
In diesem Abschnitt konfigurieren wir Fabric-Zugriffsrichtlinien, um CallHome-Quellen zu erstellen.

Navigieren Sie zu APIC > Fabric > Access Policies > Policies > Monitoring

- Im Ordner Monitoring finden Sie die Standard-Überwachungsrichtlinie. Öffnen Sie die Standardrichtlinie, und klicken Sie auf den Ordner CallHome/Smart CallHome/SNMP/Syslog/TACACS.
- Stellen Sie sicher, dass im Dropdown-Menü Überwachungsobjekt die Option ALL (Alle) ausgewählt ist und dass Quelltyp auf CallHome festgelegt ist.



- Klicken Sie auf+Anmelden im rechten Bereich:
  - Name: Geben Sie den CallHome-Quellnamen ein (`Access_CallHome`)
  - Einschließen: Wählen Sie, welche Arten von Benachrichtigungen empfangen werden sollen.
  - Ebene - Ereignisschweregrad, der eine Aktion auslöst (ausgewählte Ebene oder höher)
  - Zielgruppe: Wählen Sie hier die zuvor erstellte CallHome-Zielgruppe aus.
  - Abfragegruppe: Wählen Sie hier die zuvor erstellte CallHome-Abfragegruppe aus.



Schritt 7: Nachdem diese Änderungen vorgenommen wurden, müssen wir E-Mail-Warnmeldungen zur konfigurierten E-Mail-ID erhalten.

Fehlerbehebung und Verifizierung

1. Überprüfung der SMTP-Serververbindung

Um zu bestätigen, dass sowohl APIC- als auch Leaf-Geräte den SMTP-Server über TCP-Port 25 erreichen können, führen Sie Ping- und Telnet-Tests durch.

1.1 Ping-Test

Verwenden Sie die folgenden Befehle, um die grundlegende Netzwerkerreichbarkeit für den

SMTP-Host zu überprüfen:

Im APIC:

<#root>

APIC # ping x.x.x.x

Switch auf Leaf:

<#root>

Leaf# iping x.x.x.x

1.2 Telnet-Test (Port 25)

Führen Sie die folgenden Befehle aus, um sicherzustellen, dass der SMTP-Port 25 offen und erreichbar ist:

Im APIC:

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

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

Switch auf Leaf:

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

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

2. Validierung der CallHome-Konfiguration

Vergewissern Sie sich, dass CallHome sowohl auf dem APIC als auch auf den Leaf-Switches richtig konfiguriert ist.

2.1 CallHome-Profilvalidierung

Stellen Sie sicher, dass das Profil mit dem richtigen Port und den richtigen Parametern konfiguriert ist:

Im APIC:

<#root>

Apic# moquery -c callhomeProf

Switch auf Leaf:

<#root>

Leaf# moquery -c callhomeProf

2.2 Validierung der CallHome-Ziele

Stellen Sie sicher, dass der Ziel-SMTP-Server und der Zielport korrekt eingestellt sind:

Im APIC:

<#root>

Apic# moquery -c callhomeDest

Switch auf Leaf:

<#root>

Leaf# moquery -c callhomeDest

3. Überprüfen der CallHome-E-Mail-Übertragung

In einer typischen ACI-Fabric werden CallHome-Nachrichten vom APIC2 in einem Cluster mit drei Knoten initiiert. Wenn APIC2 nicht verfügbar ist, können diese Nachrichten von einem Leaf-Switch stammen. Um die Quelle und Übertragung von CallHome-Nachrichten zu bestätigen, verwenden Sie `tcpdump` an den entsprechenden Schnittstellen.

3.1 vom APIC (Root-Zugriff erforderlich)

Wenn das In-Band-Management konfiguriert ist, ersetzen Sie `bond0.330` durch das für das In-Band-Management verwendete VLAN:

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

Von Leaf-Switch:

Verwenden Sie die Schnittstelle `kpm_inb`, um ausgehenden SMTP-Datenverkehr zu überwachen:

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

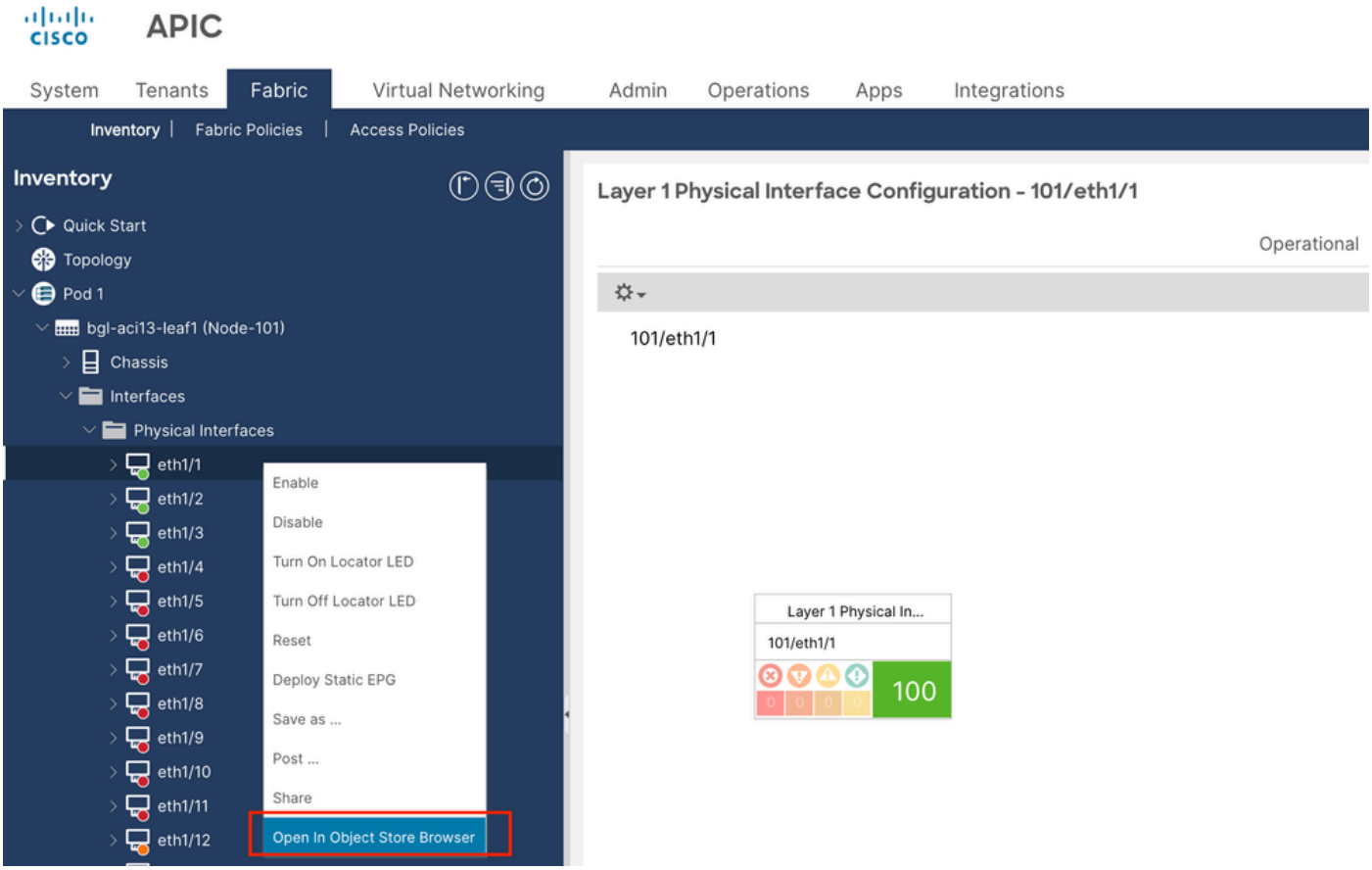
4. In bestimmten Fällen können wir selbst nach erfolgreicher Konfiguration und Verifizierung von CallHome, SMTP-Verbindungen und Überwachungsrichtlinien keine Schnittstellenfehlerbenachrichtigungen per E-Mail erhalten.

Führen Sie zur Fehlerbehebung die folgenden Schritte aus:

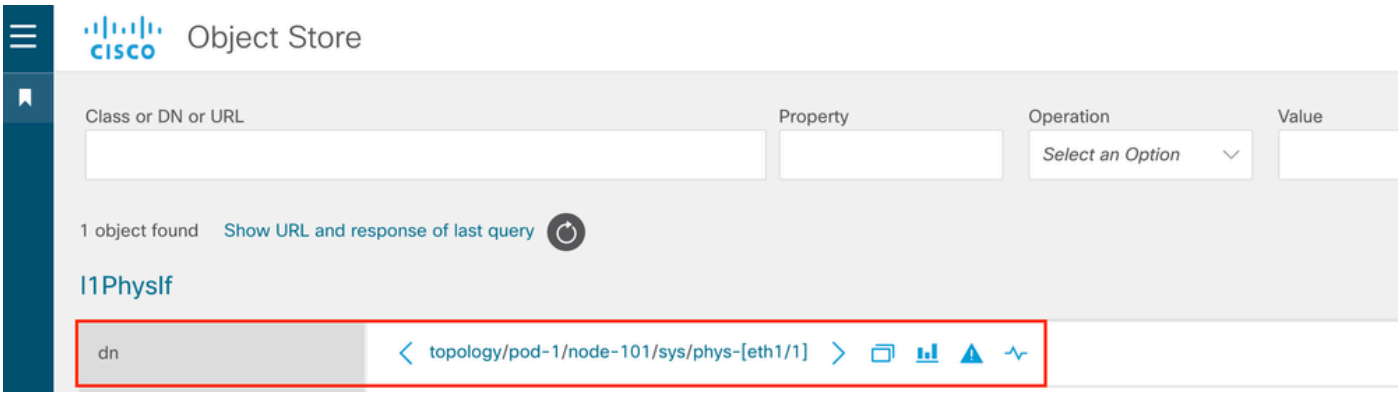
Verwenden Sie den Objektspeicherbrowser, um den Fehler zu überprüfen.

4.1 Navigieren Sie in der Cisco ACI-GUI zu der betroffenen Schnittstelle.

4.2 Klicken Sie mit der rechten Maustaste auf die Oberfläche und wählen Sie "Open in Object Store Browser" (siehe Screenshot unten für visuelle Anleitung).



4.3 Suchen Sie im Objektspeicherbrowser den Distinguished Name (DN), der dem Fehlerobjekt zugeordnet ist.



4.4 Greifen Sie nach der Identifizierung der DN auf die APIC-CLI zu, und führen Sie den folgenden Befehl aus, um die Details für das Objekt abzufragen:

Beispiel:

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

4.5. Suchen Sie in der Ausgabe des vorherigen Befehls das Feld `monPolDn`.

Beispiele:

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

Dieses Feld gibt den DN (Distinguished Name) der Überwachungsrichtlinie an, der auf das Schnittstellenobjekt angewendet wird.

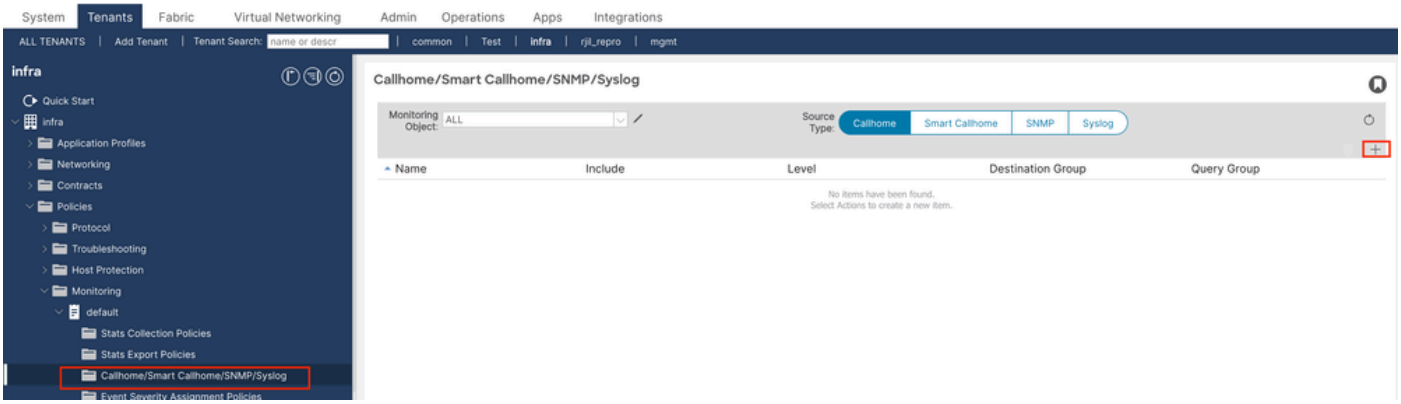
4.6 In diesem Beispiel lautet die Überwachungsrichtlinie: uni/infra/moninfra-default

Dies zeigt, dass die Standardüberwachungsrichtlinie unter dem Infra-Tenant auf die Schnittstelle angewendet wird.

4.7 So stellen Sie sicher, dass CallHome bei Schnittstellenfehlern Warnungen generiert und sendet:

Bestätigen Sie, dass die CallHome-Konfiguration unter dem Infra-Tenant vorhanden ist.

Stellen Sie sicher, dass die Überwachungsrichtlinie (in diesem Fall **`Standard-Moninfra`**) mit einem ordnungsgemäß konfigurierten CallHome-Profil verknüpft ist.


System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | Test | infra | rjil_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 Assignment 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.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.