ACIファブリックでのCallHomeの設定、確認、トラブルシューティング

内容

はじめに

このドキュメントでは、Cisco ACI環境でのCall Homeの設定について説明します。

概念

CallHome機能を使用すると、ファブリック機能に関する重要な通知を電子メールで受信できます。この通知には、診断情報や環境障害またはイベントが含まれます。これらのアラートは、CallHome宛先プロファイルを使用して複数の受信者に配信されます。このプロファイルは、特定のメッセージ形式とコンテンツカテゴリで設定できます。

前提条件

- ファブリックは4.2(1)以降である必要があります。
- すべてのファブリックデバイスは、SMTP/Eメールサーバにネットワーク接続できる必要があります。
- ファブリックデバイスとSMTP/Eメールサーバの間でTCPポート25の通信を許可する必要があります。

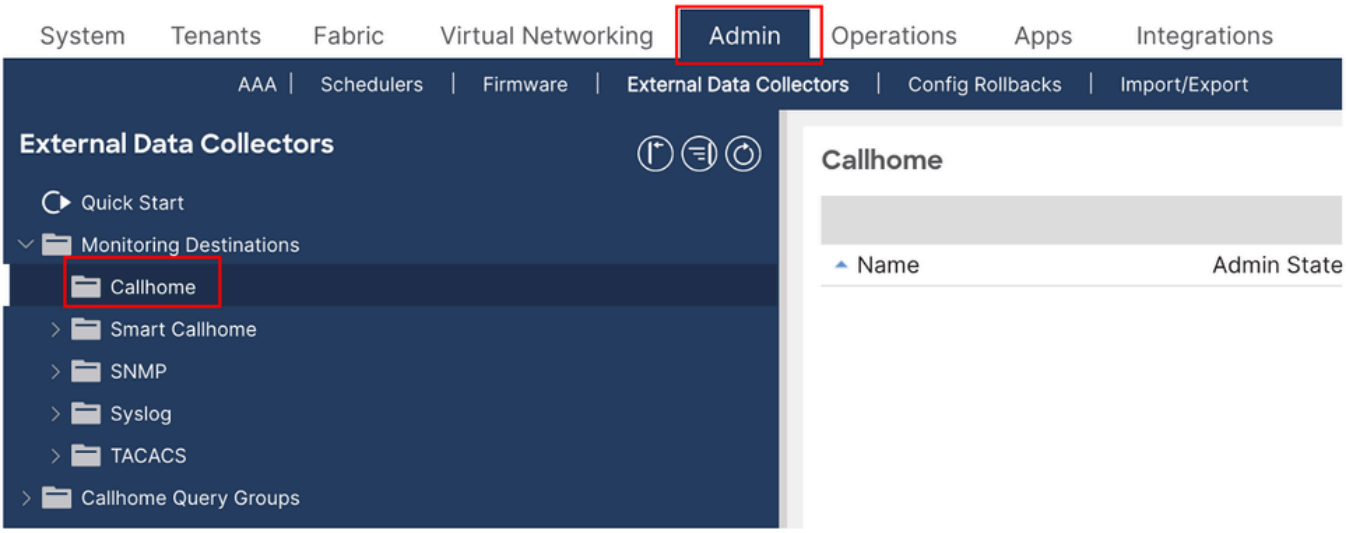
設定手順

ステップ1:APICにログインします。

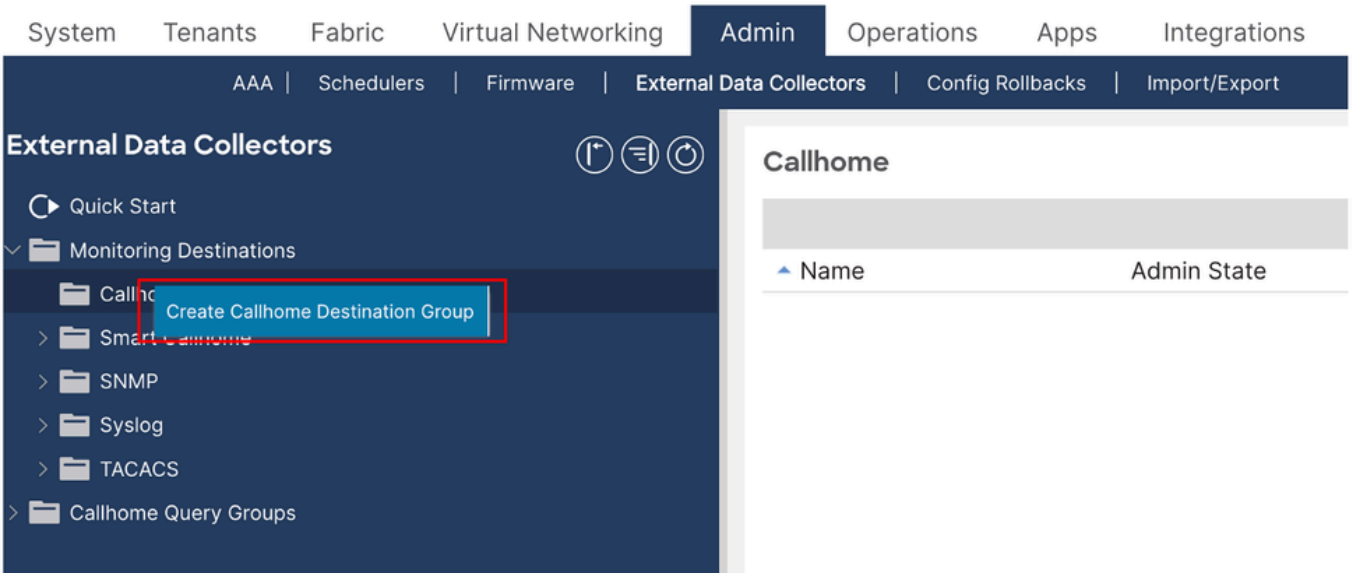
- 管理者クレデンシャルを使用してAPICにアクセスします。

ステップ2:CallHome宛先グループを作成します。

- APIC > Admin > External Data Collectors > Monitoring Destinationの順に移動します。



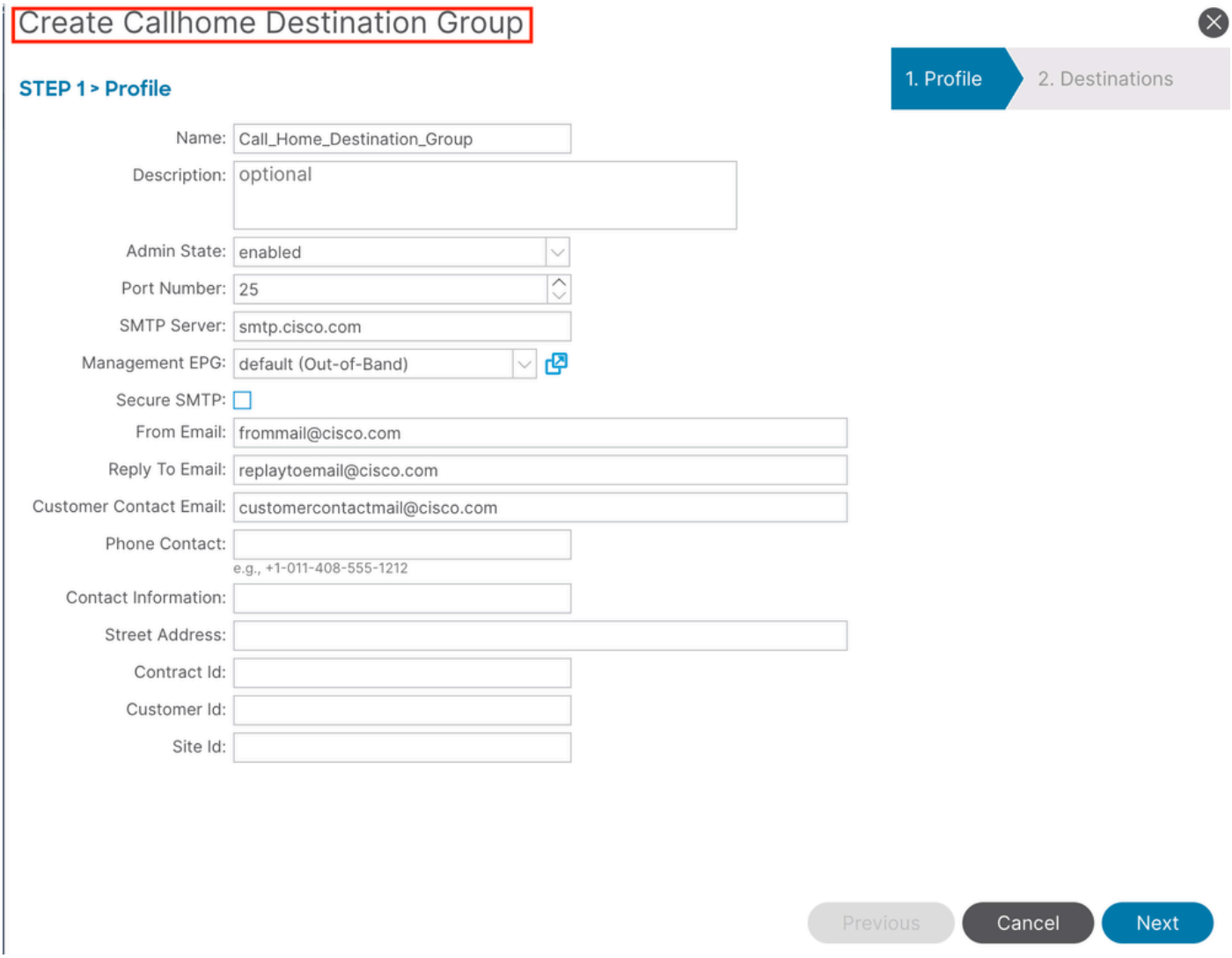
- CallHomefolderを右クリックし、Create CallHome Destination Groupを選択します。



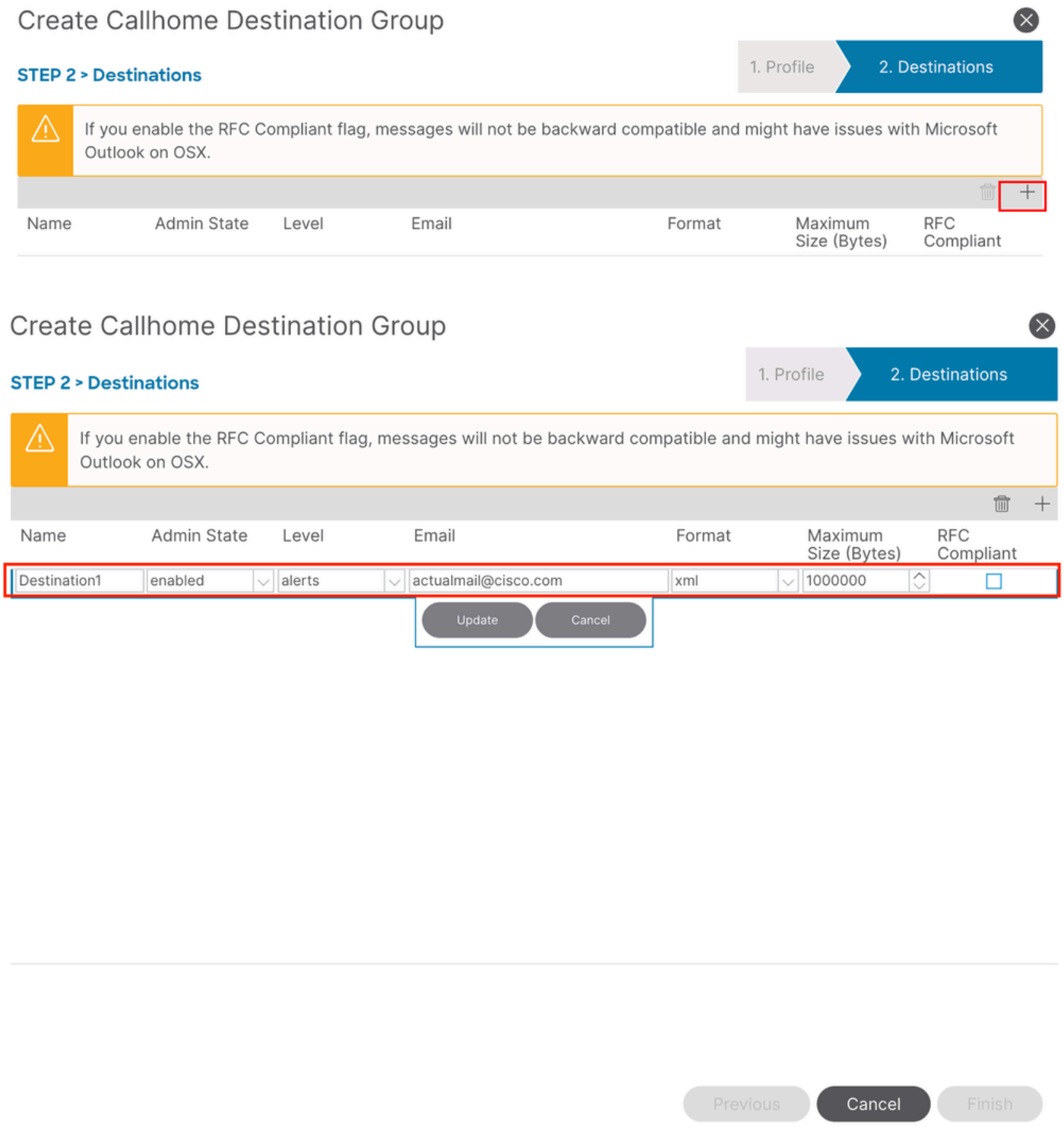
ステップ3：必要な詳細情報を入力します。

必要な詳細は次のとおりです

- Name:CallHome宛先グループの名前
- Admin：このオプションを有効にします。
- ポート：25、SMTPが通信するポート番号。
- SMTP Server:SMTPサーバのDNS名またはIPアドレス
- From Email:ファブリックがメッセージを送信する送信元の電子メールアドレス
- 管理EPG:SMTPサーバへの到達可能性があるoobまたはinb EPG
- Contact Email（担当者の電子メール）：メッセージの受信先の電子メールアドレス



- 次のページでは、正確な宛先（つまり、CallHomeメッセージの受信者）を作成できます。
- +記号をクリックして、フィールドに入力します。
    - Name – 宛先の名前
    - 管理状態 – 無効にすると、宛先はメッセージを受信しません
    - Level：宛先に送信されるメッセージの重大度レベル。このセットをerror以上にすることをお勧めします。重大度レベルの表は次のとおりです。
    - 電子メール：メッセージの送信先となる実際の電子メールアドレス
    - フォーマット：着信メッセージを自動的に解析する予定がない場合は、short-txtに設定します。両者の違いを見るために実験してみることができます。
    - Maximum Size (Bytes)：単一の電子メールメッセージの最大サイズ。フォーマットをamlまたはxmlに設定した場合、メッセージはかなり大きくなる可能性があるので、100-200KBの数で問題ありません。必要なサイズを決定するためにこの数を試すことができます。ショートテキスト形式の場合は、10KBに設定するのに十分な値でなければなりません。
    - RFC準拠：これを有効にしない方が適切です。



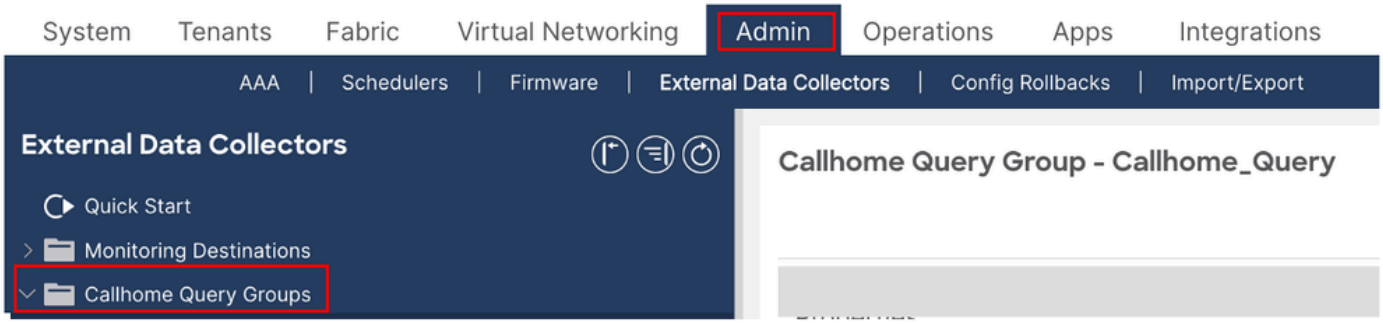
- 宛先は必要な数だけ作成できます。また、CallHome宛先グループを右クリックして、Create CallHome Destinationを選択すると、さらに多くの宛先を作成できます。

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

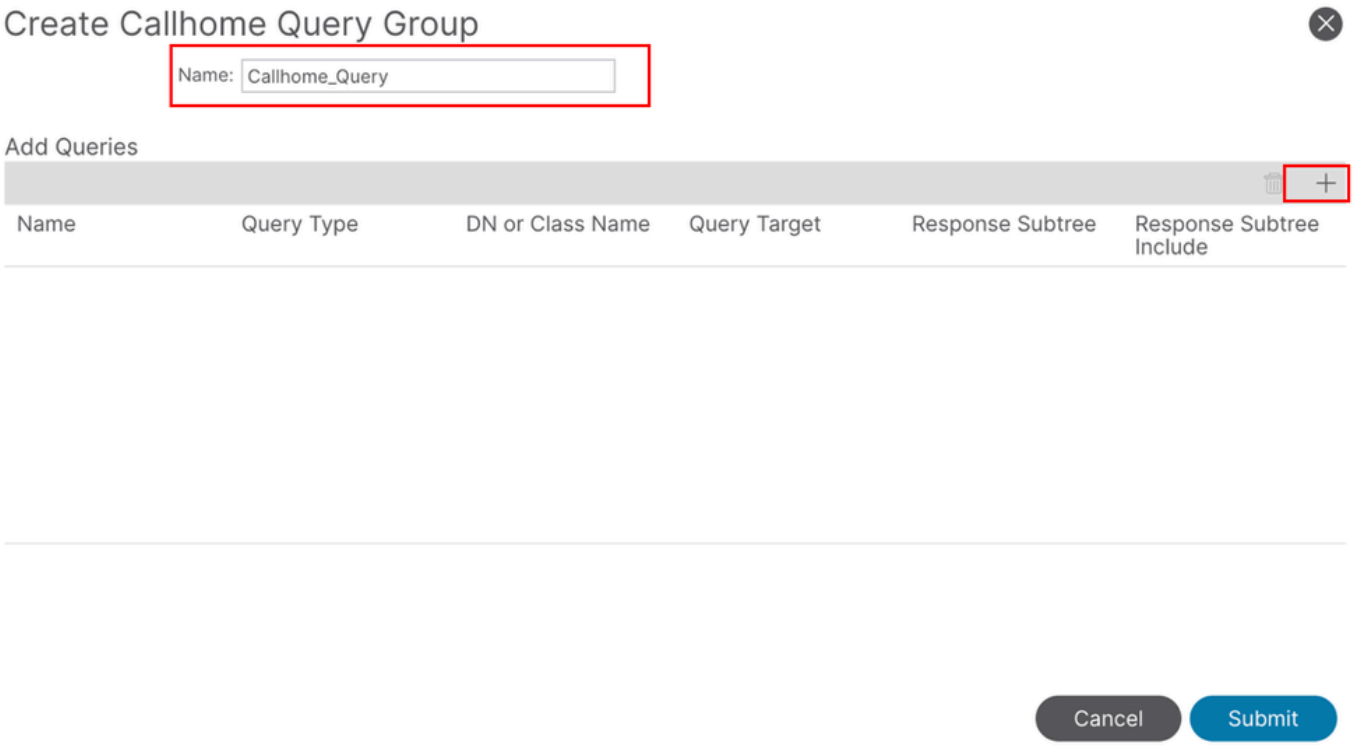
ステップ4:Callhomeクエリグループの作成

- APIC > Admin > External Data Collectors > CallHome Query Groupsの順に移動します。

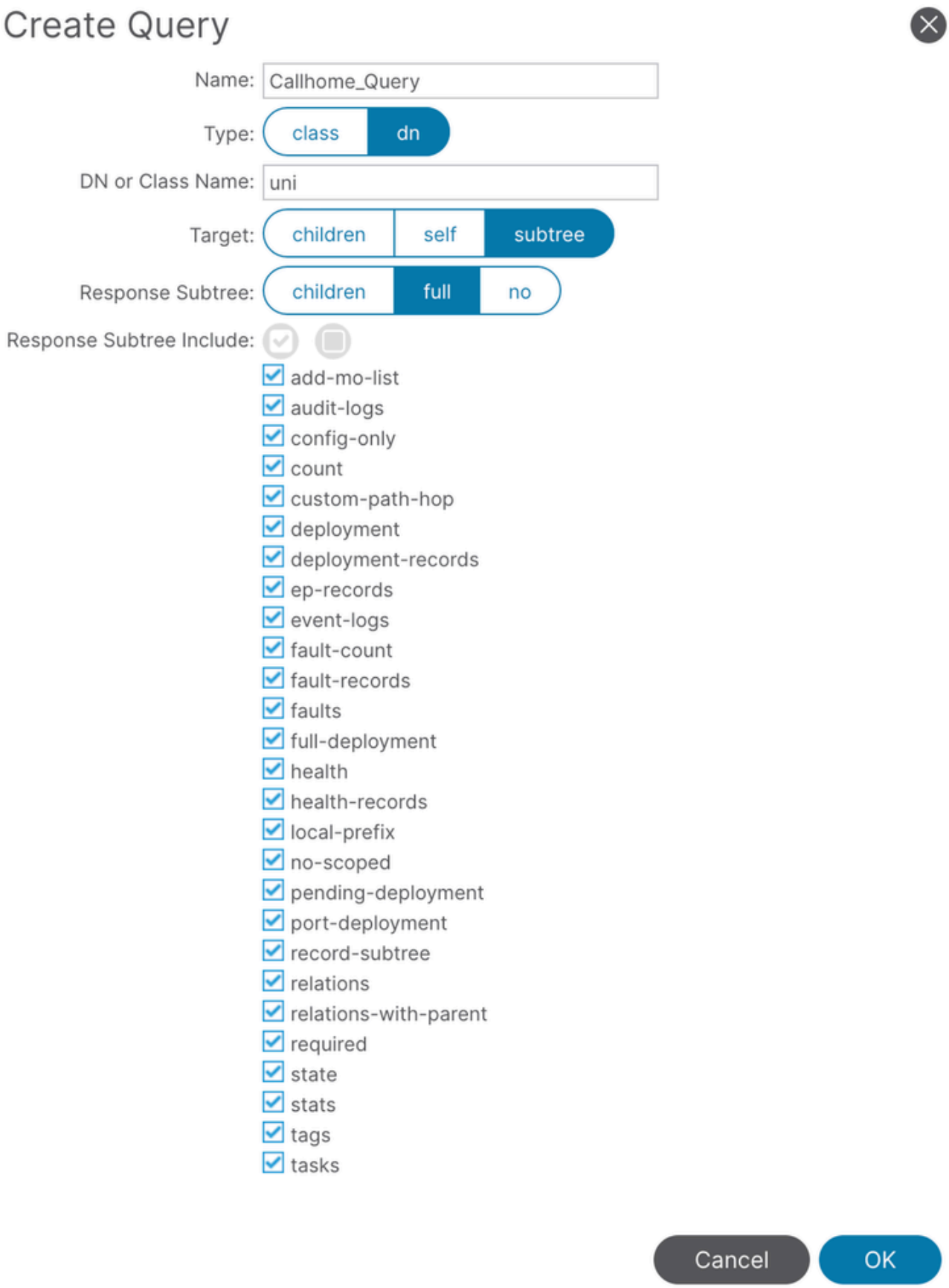


- CallHome Query Groupsフォルダを右クリックし、Create CallHome Query Groupを選択し

ます。



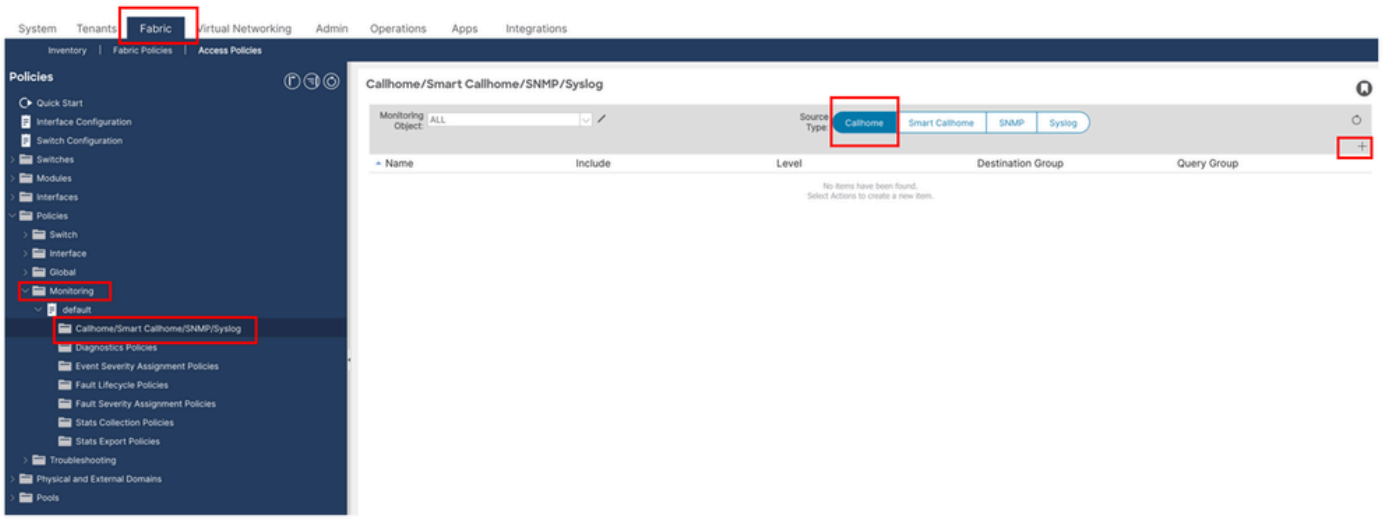
- クエリグループの名前を定義し、+記号をクリックしてクエリ定義を作成します。
  - Name – クエリ名
  - 変更を監視するオブジェクトタイプのタイプセレクタ。私は「識別名」を意味するheredn selectedを持っています。
  - DNまたはクラス名 – 監視対象オブジェクトの名前。そこで魔法を使いましょう！このフィールドに挿入する必要があるオブジェクト名の種類や内容に関する説明は見つかりません。APICのバージョン4より前のバージョンでは、このフィールドは不要でした。バージョン4からは必須です。selecteddnforTypeを設定した場合は、ここに「Whole universe（宇宙全体）」または言い換えれば「All fabric objects（すべてのファブリックオブジェクト）」を文字通り意味します。
  - Target：クエリによって返されるオブジェクトにサブツリー情報を含める必要があるかどうかを選択します。I have ubesubtreehere selected.これは、USBが選択されています。
  - サブツリー：クエリーから返す必要があるサブツリーオブジェクトを選択します。ここを選択しました。
  - Include – クエリーによって返されるオブジェクトのタイプ。すべて選択しました。



ステップ5:ファブリックモニタリングポリシーを適用し、CallHomeソースを作成します。

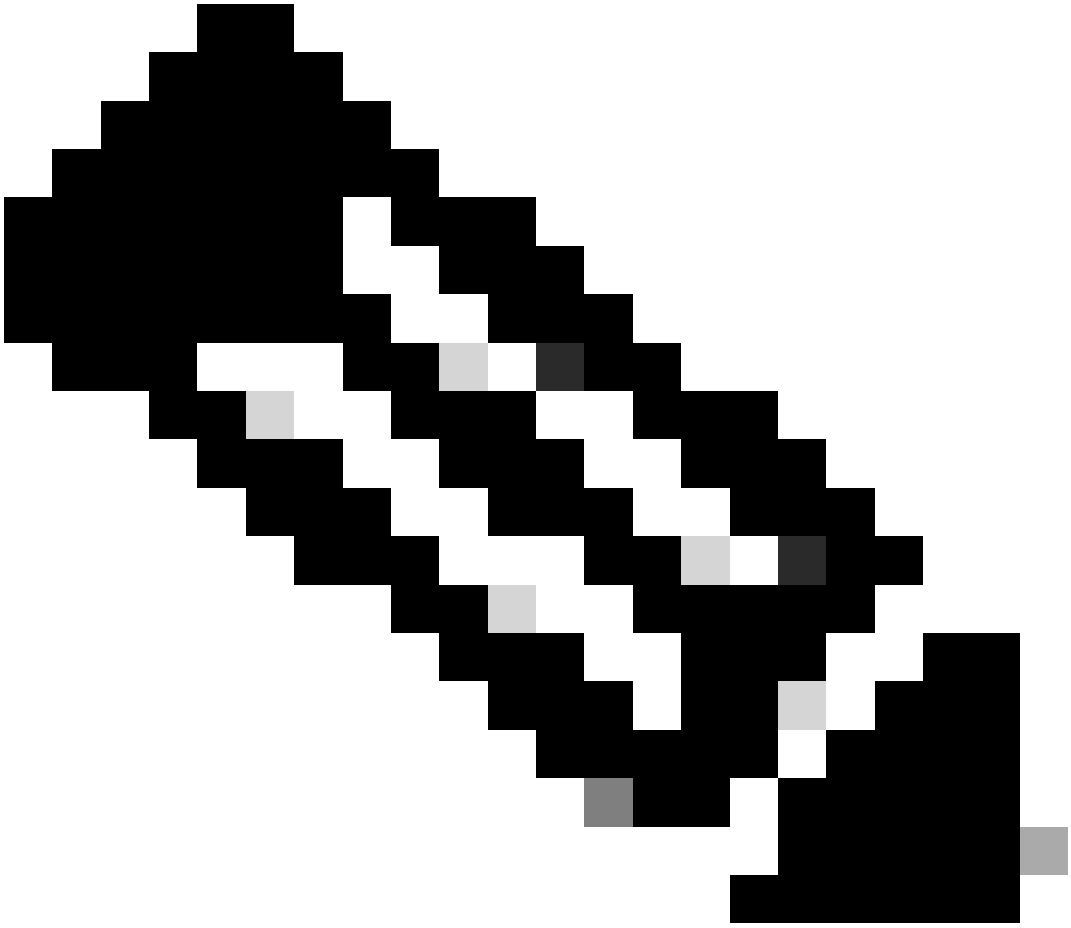
CallHomeの宛先とクエリが設定されたので、次はモニタリングポリシーの編集に進みます。

- APIC > Fabric > Fabric Policies > Policies > Monitoringの順に移動します。
- 「Monitoring Object」ドロップダウンで値「ALL」が選択され、「Source Type」が「CallHome」に設定されていることを確認します。



- 右側のペインの右端で+サインインをクリックします。
  - Name- CallHomeソース名(Callhome_Source)
  - Include：受信する通知の種類を選択します。
  - Level：アクションをトリガーするイベントの重大度（選択したレベル以上）
  - 宛先グループ：ここで、以前に作成されたCallHome宛先グループを選択します。
  - Query Group：ここで、以前に作成したCallHomeクエリグループを選択します。

- Submitをクリックします。



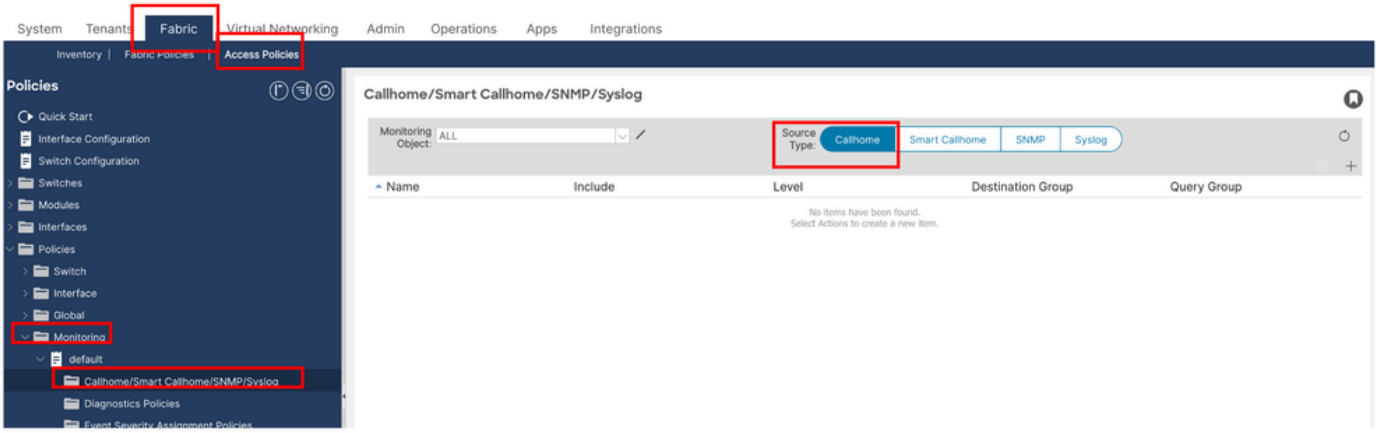
注：セットアップが完了したら、異なるモニタリングオブジェクトに対して個別のCallHomeソースを作成し、複数のCallHome宛先グループとクエリを使用することで、モニタリングポリシーを微調整できます

ステップ6:CallHomeソースへのポリシーのアクセス

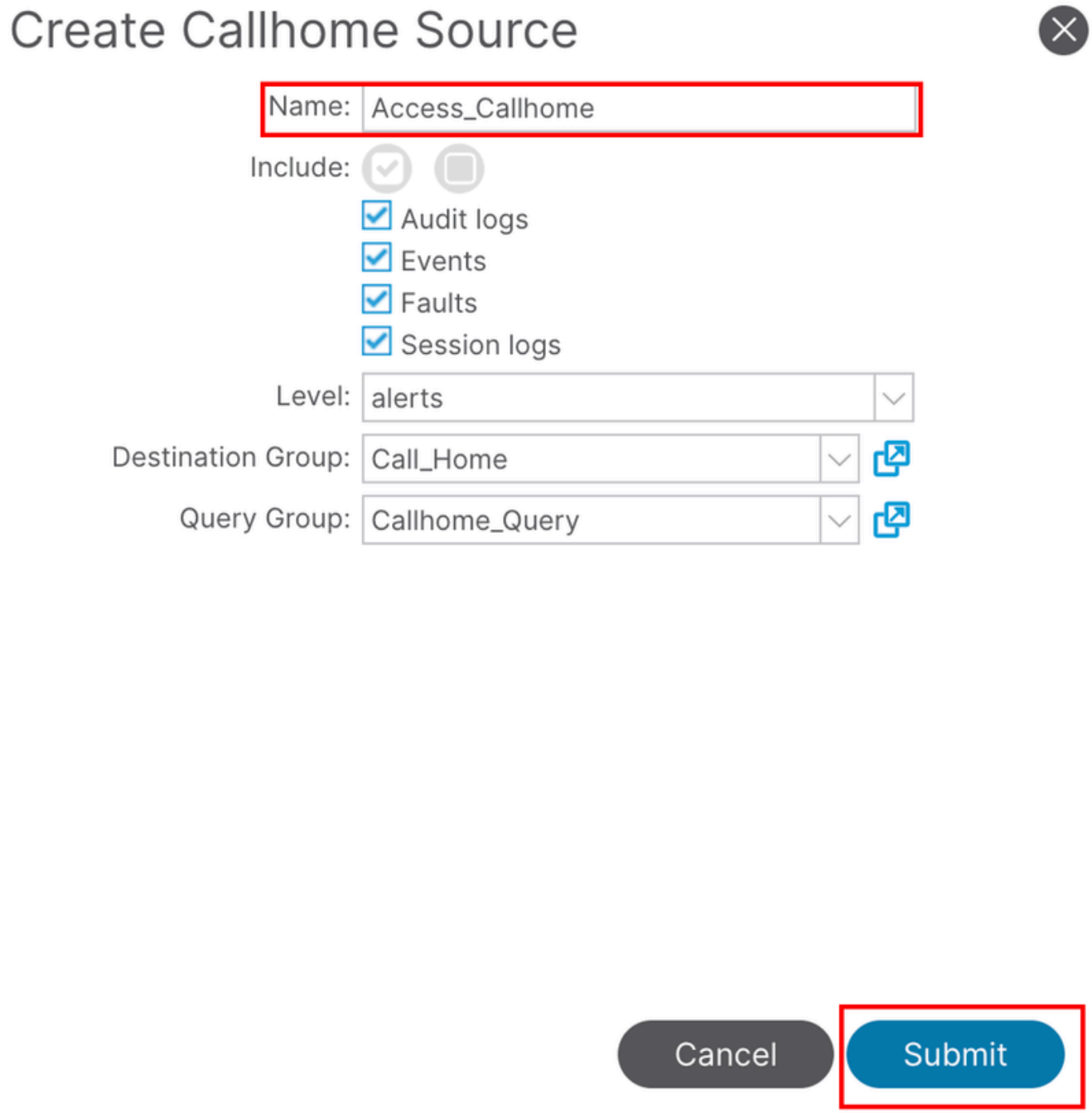
このセクションでは、CallHomeソースを作成するためのファブリックアクセスポリシーを設定します。

APIC > Fabric > Access Policies > Policies > Monitoringの順に移動します。

- Monitoringフォルダには、デフォルトのモニタリングポリシーがあります。デフォルトポリシーを開き、CallHome/Smart CallHome/SNMP/Syslog/TACACSフォルダをクリックします。
- Monitoring ObjectドロップダウンでALLが選択されており、Source TypeがCallHomeに設定されていることを確認します。



- 右側のペインの右端で+sign inをクリックします。
  - Name（名前）:CallHomeソース名(`Access_CallHome`)を入力します。
  - 含める：受信する通知の種類を選択します。
  - Level：アクションをトリガーするイベントの重大度（選択したレベル以上）
  - 宛先グループ：ここでは、以前に作成したCallHome宛先グループを選択します
  - Query Group：ここでは、以前に作成したCallHomeクエリグループを選択します。



ステップ7:これらの変更を行った後、設定済みのメールIDに関する電子メールアラートを受信する必要があります。

トラブルシューティングと確認

1. SMTPサーバ接続の確認

APICデバイスとリーフデバイスの両方がTCPポート25を介してSMTPサーバに到達できることを確認するには、pingとtelnetのテストを実行します。

1.1 Pingテスト

次のコマンドを使用して、SMTPホストへの基本的なネットワーク到達可能性を確認します。

APIC上：

<#root>

APIC # ping x.x.x.x

リーフスイッチ：

<#root>

Leaf# iping x.x.x.x

1.2 Telnetテスト（ポート25）

次のコマンドを実行して、SMTPポート25が開いていて到達可能であることを確認します。

APIC上：

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

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

リーフスイッチ：

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

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

2. CallHome設定の検証

CallHomeがAPICとリーフスイッチの両方で正しく設定されていることを確認します。

2.1 CallHomeプロファイルの検証

プロファイルに正しいポートとパラメータが設定されていることを確認します。

APIC上：

<#root>

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

リーフスイッチ：

```
<#root>
Leaf# moquery -c callhomeProf
```

2.2 CallHome接続先の検証

宛先SMTPサーバとポートが正しく設定されていることを確認します。

APIC上：

```
<#root>
Apic# moquery -c callhomeDest
```

リーフスイッチ：

```
<#root>
Leaf# moquery -c callhomeDest
```

3. CallHome電子メール送信の確認

一般的なACIファブリックでは、CallHomeメッセージは3ノードクラスタのAPIC2から開始されます。APIC2が使用できない場合、これらのメッセージはリーフスイッチから発信できます。CallHomeメッセージの送信元と送信を確認するには、関連するインターフェイスで`tcpdump`を使用します。

3.1 APICから（ルートアクセスが必要）

インバンド管理が設定されている場合は、`bond0.330`をインバンド管理に使用されるVLANに置き換えます。

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

リーフスイッチから

発信SMTPトラフィックを監視するには、kpm_inbインターフェイスを使用します。

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

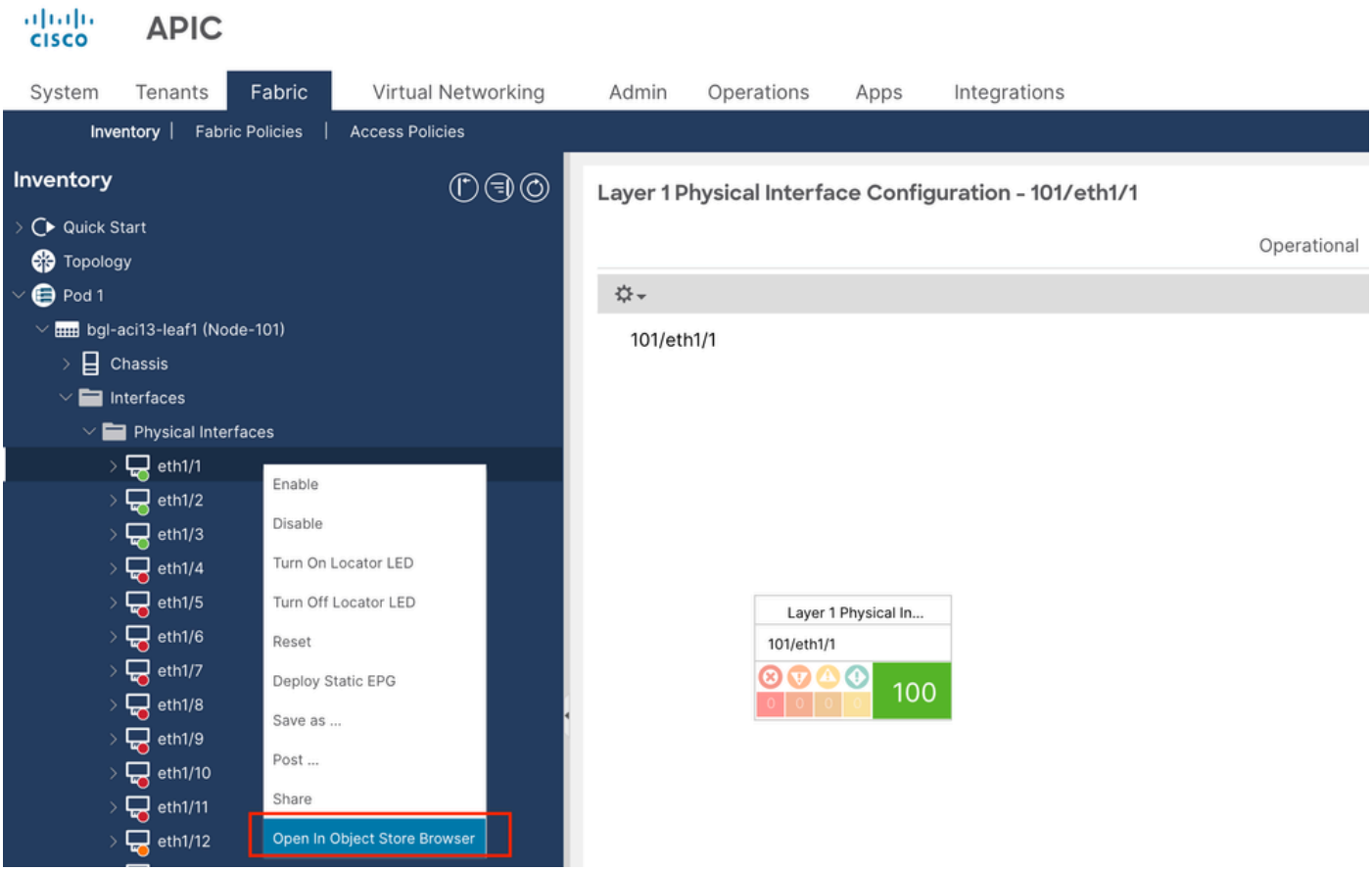
4. 場合によっては、CallHome、SMTP接続、監視ポリシーの設定と検証が正常に完了した後でも、インターフェイスの障害アラートを電子メールで受信できないことがあります。

トラブルシューティングを行うには、次の手順に従います。

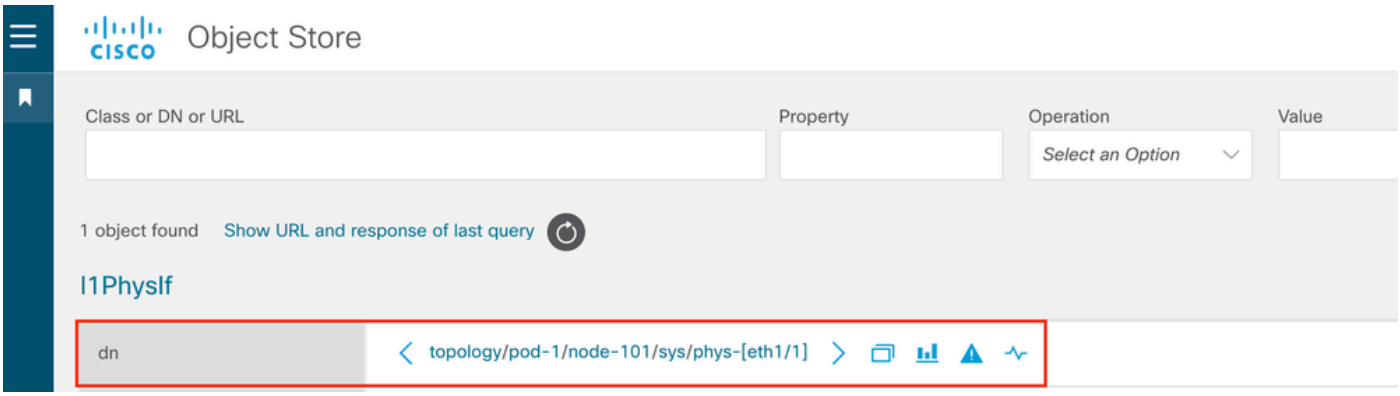
オブジェクトストアブラウザを使用して障害を調査します。

4.1 Cisco ACI GUIで、影響を受けるインターフェイスに移動します。

4.2インターフェイスを右クリックし、「オブジェクトストアブラウザで開く」を選択します（以下のスクリーンショットを参照してください）。



4.3オブジェクトストアブラウザで、障害オブジェクトに関連付けられている識別名(DN)を探します。



4.4 DNを特定した後、APIC CLIにアクセスし、次のコマンドを実行してオブジェクトの詳細を照会します。

例：-

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

4.5.前のコマンドの出力で、monPolDnフィールドを見つけます。

例：

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

このフィールドは、インターフェイスオブジェクトに適用されるモニタリングポリシー識別名(DN)を示します。

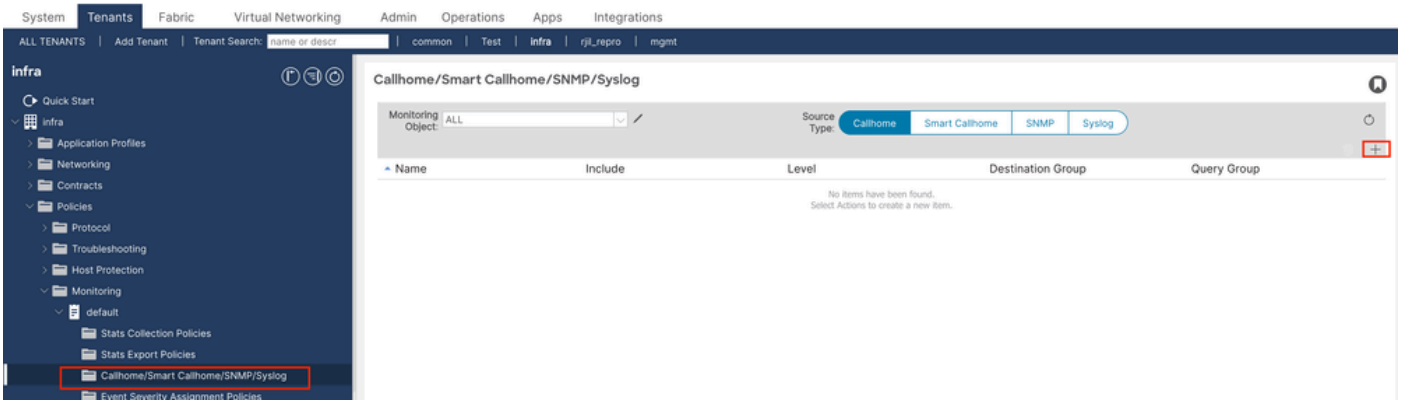
4.6この例では、モニタリングポリシーはuni/infra/moninfra-defaultです。

これは、Infraテナントの下のデフォルトのモニタリングポリシーがインターフェイスに適用されていることを示します。

4.7 CallHomeでインターフェイスエラーのアラートを生成および送信するには、次の手順を実行します。

InfraテナントにCallHome設定が存在することを確認します。

モニタリングポリシー(この場合は`moninfra-default`)が適切に設定されたCallHomeプロファイルにリンクされていることを確認します。


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.

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。