Configurar o SNMP na ACI

Contents

Introdução

Este documento descreve a configuração do Simple Network Management Protocol (SNMP) e traps SNMP na ACI.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Descoberta de malha concluída
- Conectividade dentro/fora da banda para o Application Policy Infrastructure Controller (APIC) e os switches de malha

- Contratos In-Band/Out-of-Band configurados para permitir tráfego SNMP (portas UDP 161 e 162)
- Endereços de gerenciamento de nó estáticos configurados para seus APICs e switches de malha sob o locatário de gerenciamento padrão (sem isso, a extração de informações SNMP de um APIC falha)
- Entender o fluxo de trabalho do protocolo SNMP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- APIC
- Navegador
- Application Centric Infrastructure (ACI) executando a versão 5.2 (8e)
- Snmpwalk comando

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

A Cisco ACI oferece suporte a SNMPv1, v2c e v3, incluindo bases de informações de gerenciamento (MIBs) e notificações (traps). O padrão SNMP permite que qualquer aplicativo de terceiros que suporte as diferentes MIBs gerencie e monitore os switches leaf e spine e os controladores APIC da ACI.

No entanto, os comandos de gravação SNMP (Set) não são suportados na ACI.

A política SNMP é aplicada e executada de forma independente nos switches leaf e spine e nos controladores APIC. Como cada dispositivo ACI tem sua própria entidade SNMP, ou seja, vários APICs em um cluster APIC devem ser monitorados separadamente, bem como os switches. No entanto, a origem da política SNMP é criada como uma política de monitoramento para toda a estrutura da ACI.

Por padrão, o SNMP usa a porta **UDP 161** para polling e a porta **162** para TRAPs.

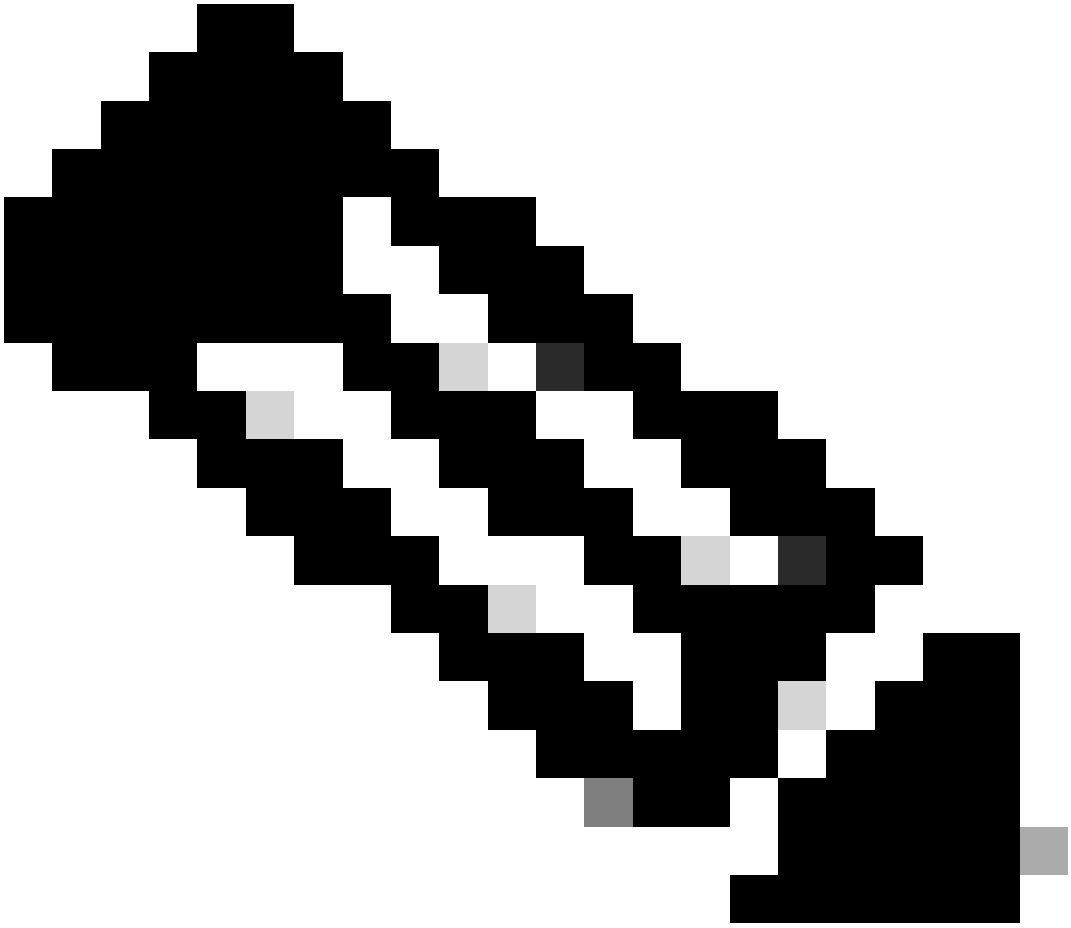
Entendendo os escopos de SNMP

Um conceito básico rápido do SNMP na ACI é que há dois escopos dos quais as informações de SNMP podem ser extraídas:
1. Global
2. Contexto de Roteamento e Encaminhamento Virtual (VRF)

O **Global Scope** é obter MIBs de chassi, como o número de interfaces, índices de interface, nomes de interface, status de interface e assim por diante de um nó leaf/spine.

As MIBs específicas do **VRF Context Scope** obtêm informações específicas de VRF, como endereços IP e informações do protocolo de roteamento.

Há uma lista completa de MIBs globais e de contexto de VRF do APIC e do switch de estrutura compatíveis na lista de suporte da MIB da Cisco ACI.

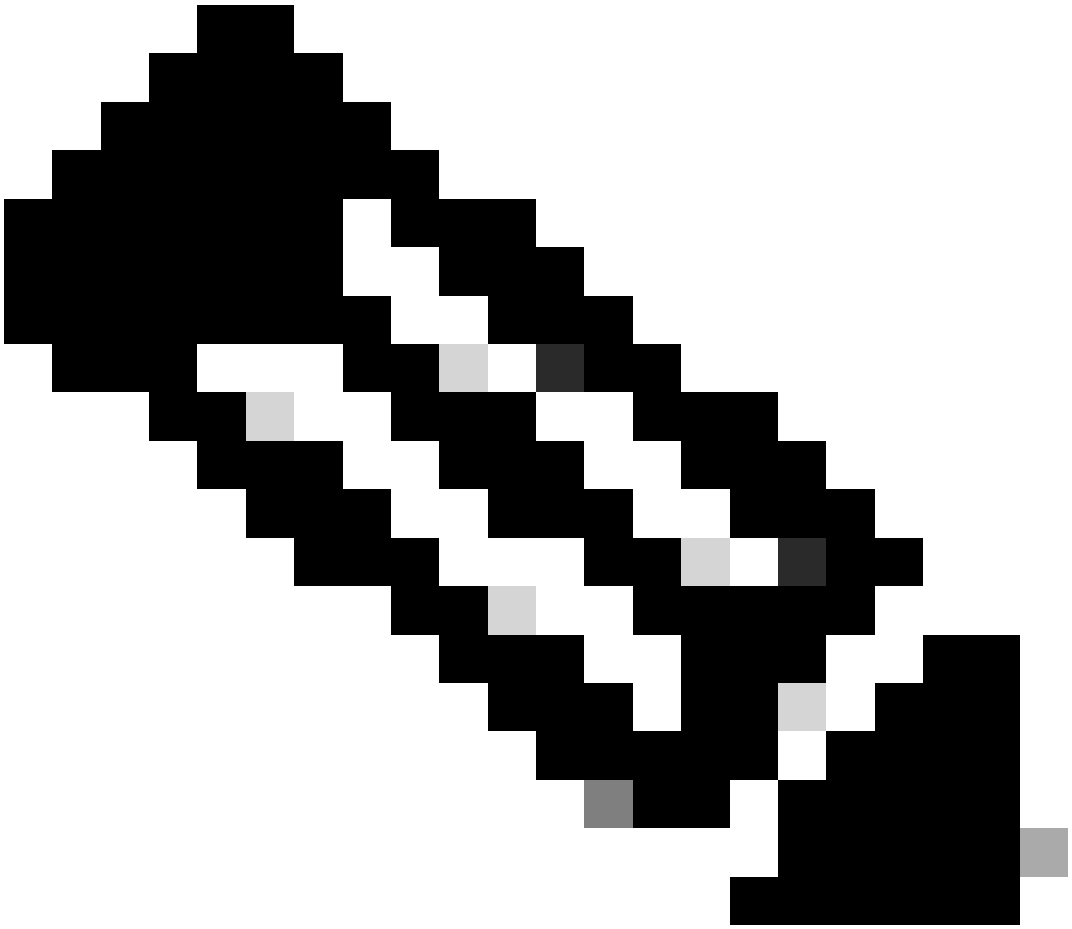


Observação: um MIB com um escopo global tem apenas uma instância no sistema. Os dados em uma MIB global se relacionam ao sistema geral.

Um MIB com escopo específico de VRF pode ter instâncias por VRF no sistema. Os dados em um MIB específico de VRF se relacionam somente a esse VRF.

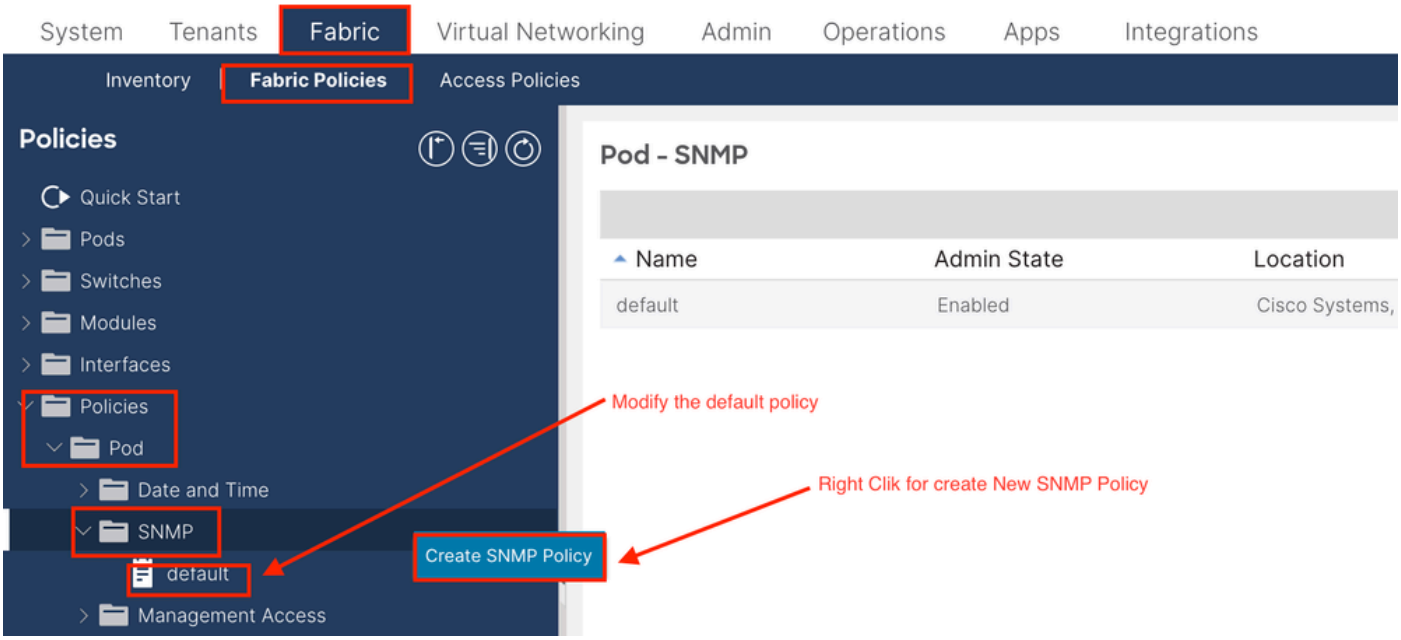
Etapas de configuração (para escopos de contexto global e VRF)

Etapa 1. Configurar a política de estrutura SNMP



Observação: aqui as configurações SNMP são especificadas, como políticas de comunidade SNMP e políticas de grupo de clientes SNMP.

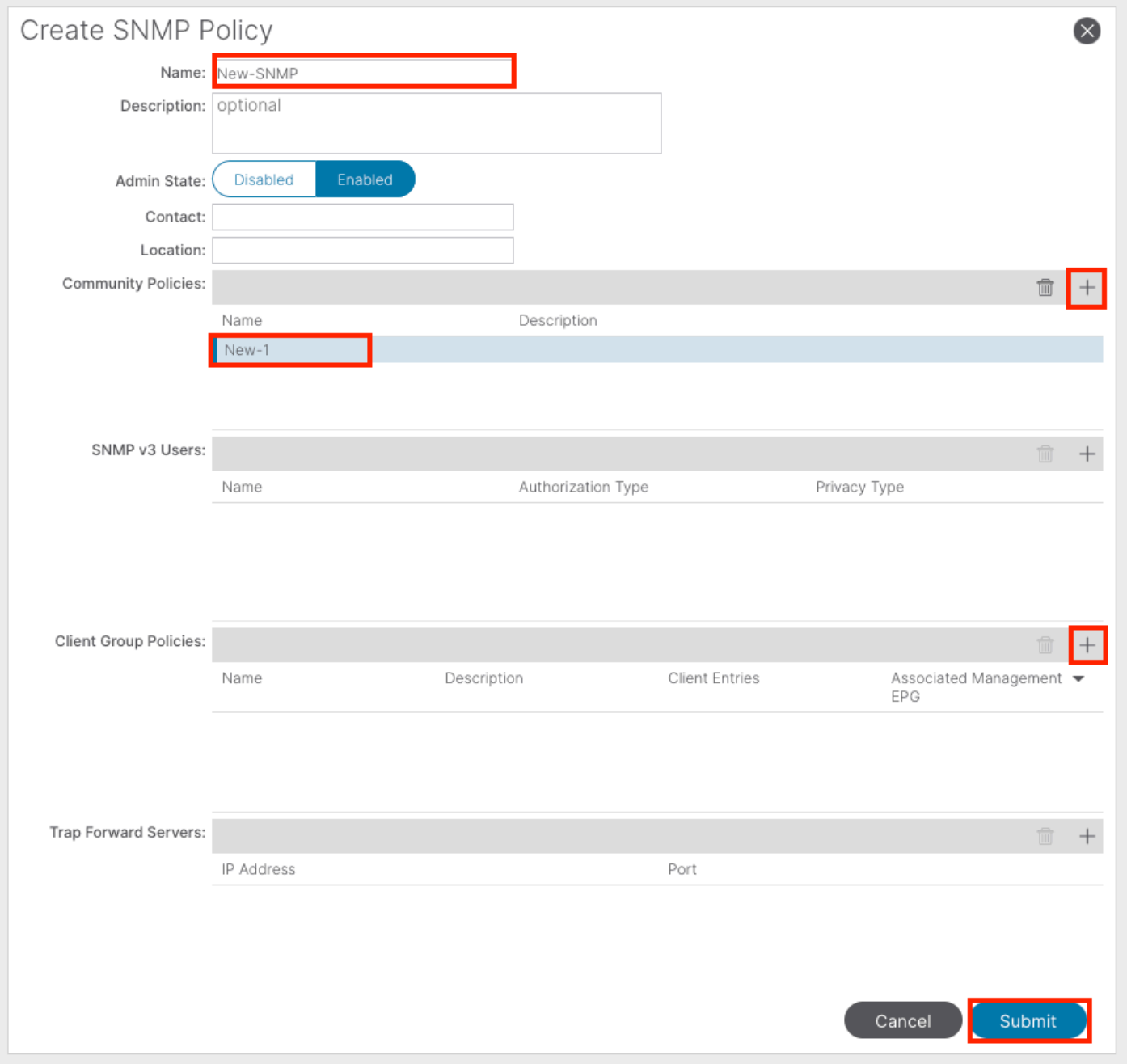
A primeira etapa na configuração do SNMP é criar as Políticas de estrutura SNMP necessárias. Para criar as Políticas de estrutura SNMP, navegue até o caminho da GUI da Web do APIC Fabric > Fabric Policies > Policies > Pod > SNMP.



Você pode criar uma nova Política SNMP ou modificar a política SNMP padrão.

No documento, a política SNMP é chamada **New-SNMP** e usa a versão SNMP v2c, portanto, os únicos campos necessários aqui são Políticas de comunidade e Políticas de grupo de clientes.

O campo Community Policy Name define a sequência de caracteres da comunidade SNMP a ser usada. No nosso caso, **New-1**. Você vê onde essas duas cordas comunitárias chegam mais tarde.



Name - o nome da política SNMP. Esse nome pode ter entre 1 e 64 caracteres alfanuméricos.

Descrição - a descrição da política SNMP. A descrição pode ter de 0 a 128 caracteres alfanuméricos.

Estado do administrador - o estado administrativo da política SNMP. O estado pode ser ativado ou desativado. Os estados são:

- enabled (habilitado) - o estado admin está habilitado
- desabilitado - o estado do administrador está desabilitado

O padrão é **desabilitado**.

Contato - as informações de contato para a política SNMP.

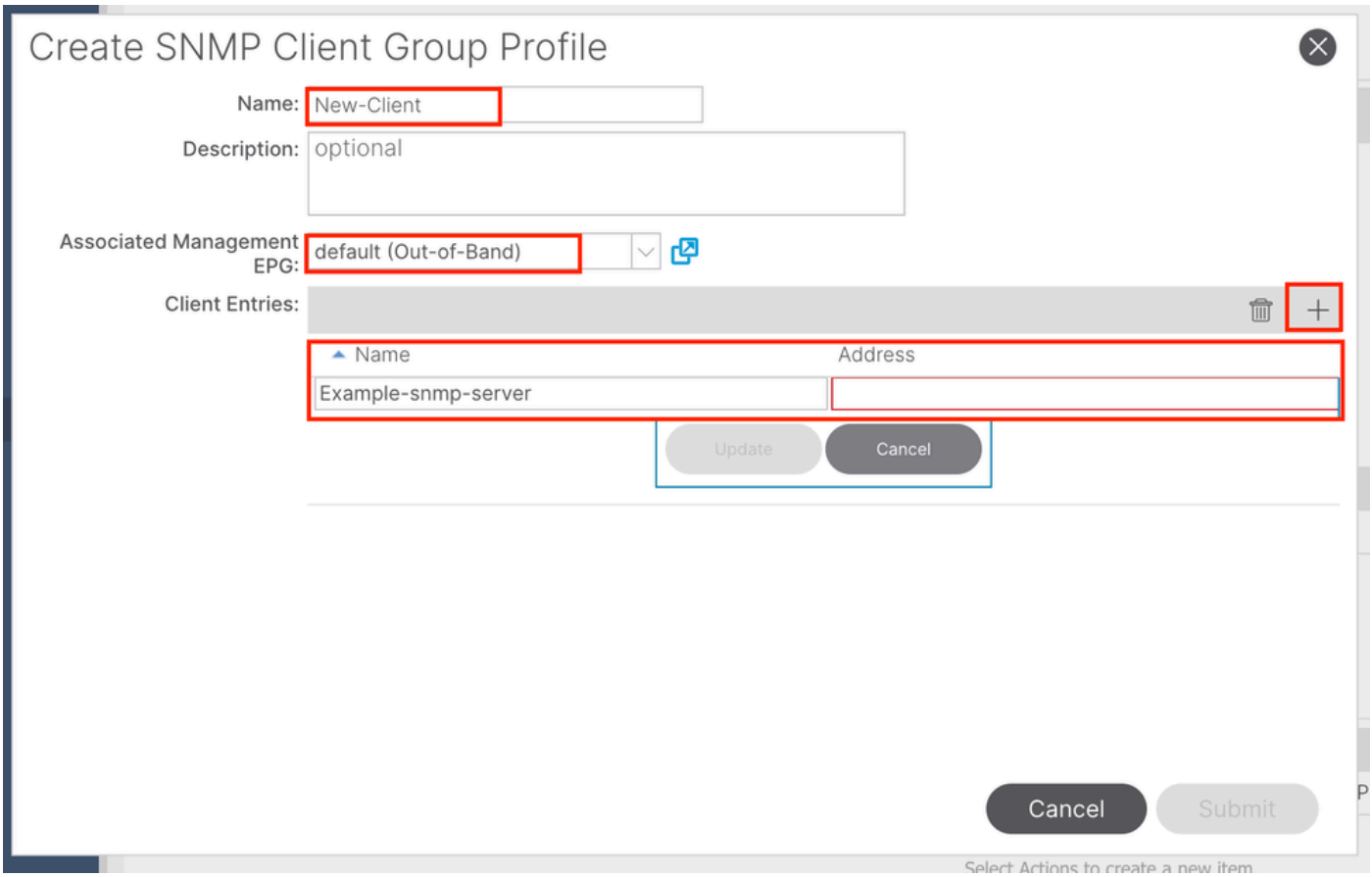
Local - o local da política SNMP.

Usuários SNMP v3 - o perfil de usuário SNMP é usado para associar usuários com políticas SNMP para dispositivos de monitoramento em uma rede.

Políticas de comunidade - o perfil de comunidade SNMP permite o acesso às estatísticas do roteador ou switch para monitoramento.

Diretivas de Grupo de Clientes:

A próxima etapa é adicionar o perfil/política de grupo do cliente. A finalidade da Política de grupo/Perfil do cliente é definir quais IPs/sub-redes podem receber dados SNMP de APICs e switches de estrutura:



Nome - o nome do perfil do grupo de clientes. Esse nome pode ter entre 1 e 64 caracteres alfanuméricos.

Descrição - a descrição do perfil do grupo de clientes. A descrição pode ter de 0 a 128 caracteres alfanuméricos.

Grupo de endpoint de gerenciamento associado (EPG) - o nome distinto de um grupo de endpoint através do qual o VRF é acessível. O comprimento máximo de sequência de caracteres suportado é 255 caracteres ASCII. O padrão é o EPG de acesso de gerenciamento fora da banda do locatário de gerenciamento.

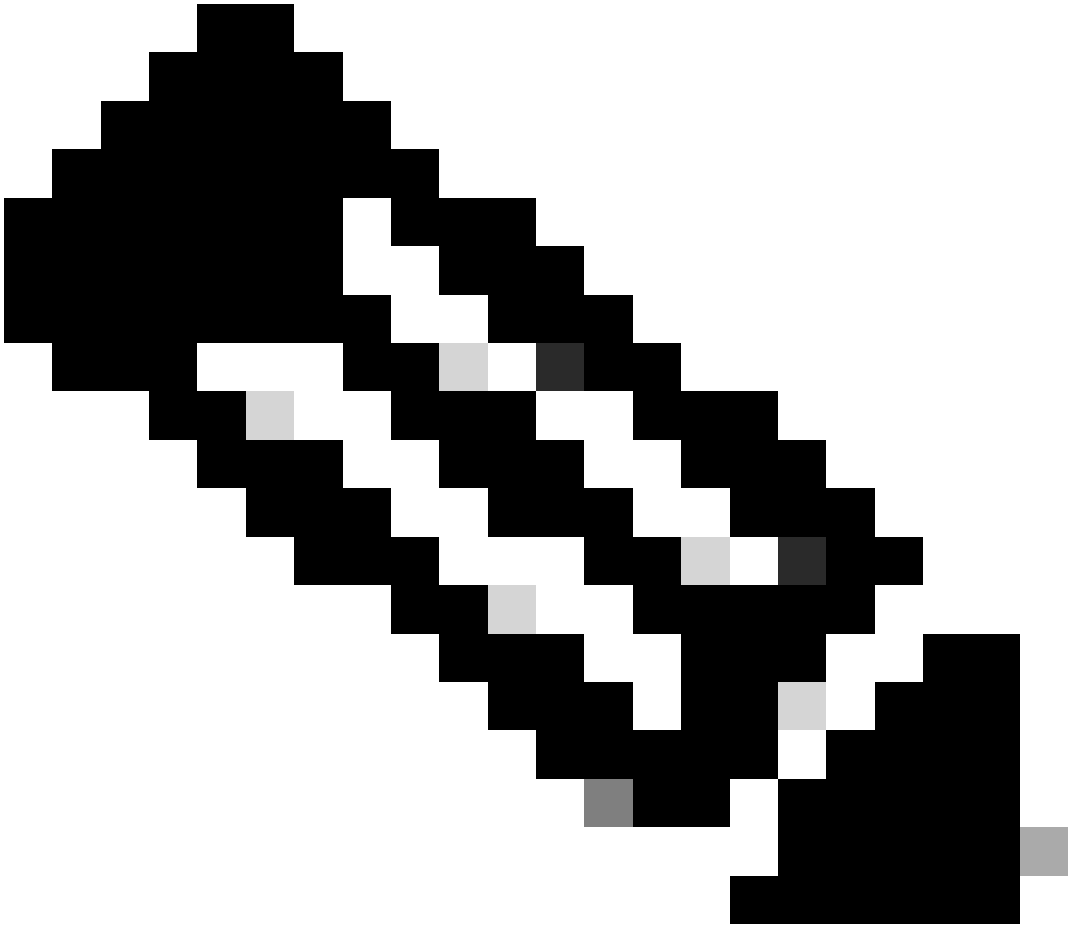
Entradas do cliente - o endereço IP do perfil do cliente SNMP.

No documento, a Política de grupo/perfil do cliente é chamada de **Novo cliente**.

Na Política de grupo/perfil do cliente, você deve associar o EPG de gerenciamento preferencial. Você deve garantir que o EPG de gerenciamento escolhido tenha os contratos necessários para permitir o tráfego SNMP (portas UDP 161 e 162). O EPG de gerenciamento fora de banda padrão é usado no documento para fins de demonstração.

A última etapa é definir as **Entradas do Cliente** para permitir que IPs específicos ou sub-redes inteiras acessem os dados SNMP da ACI. Há uma sintaxe para definir um IP específico ou uma sub-rede inteira:

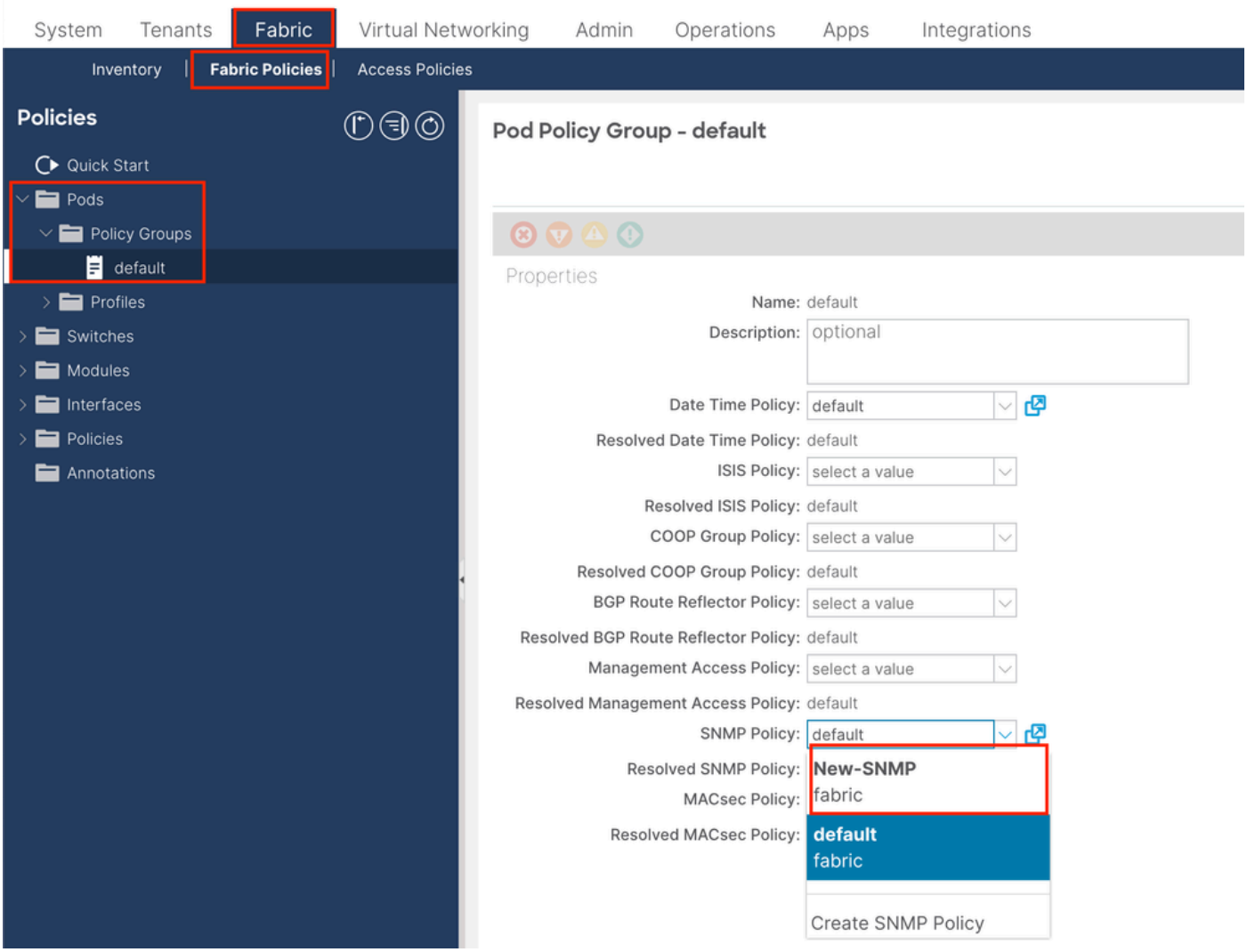
- IP específico do host: 192.168.1.5
- Sub-rede inteira: 192.168.1.0/24



Observação: você não pode usar 0.0.0.0 na entrada do cliente para permitir todas as sub-redes (se quiser permitir que todas as sub-redes acessem SNMP MIB, apenas deixe as entradas do cliente vazias).

Etapa 2. Aplicar política SNMP ao grupo de política do Pod (grupo de política de malha)

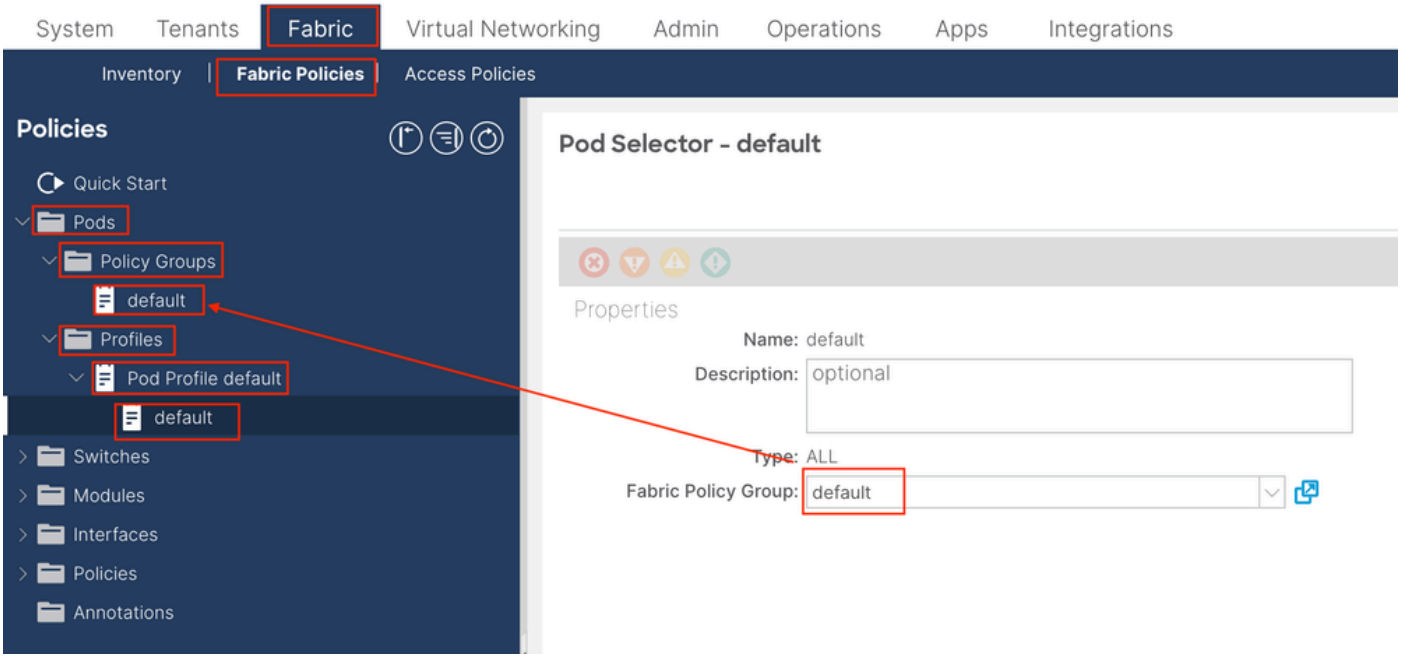
Para aplicar essa configuração, navegue até o caminho da GUI da Web do APIC; Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP (padrão no documento).



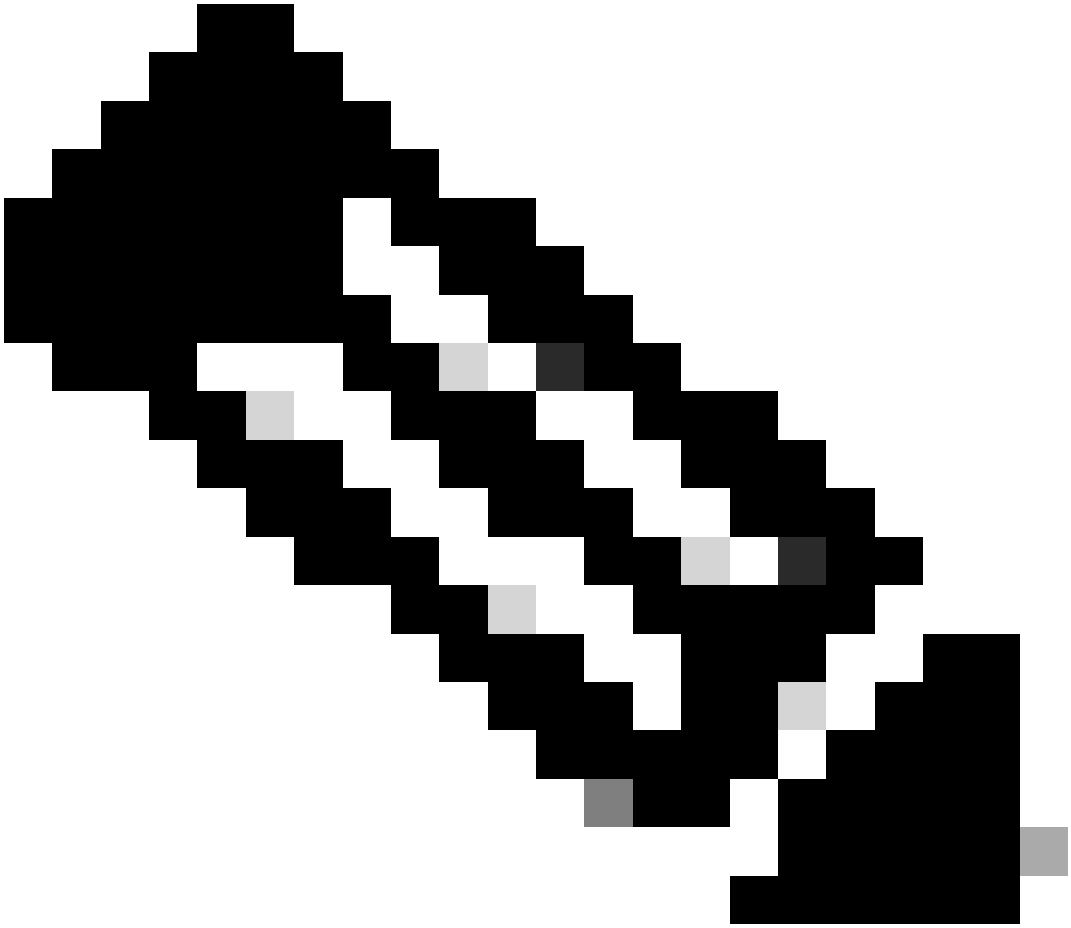
No painel à direita, você vê um campo para SNMP Policy. No menu suspenso, escolha sua política SNMP recém-criada e envie suas alterações.

Etapa 3. Associar o Grupo de Políticas do Pod ao Perfil do Pod

No documento, use o perfil de pod padrão para simplificar. Para fazer isso, navegue até o caminho da GUI da Web do APIC; Fabric > Fabric Policies > Pods > Profiles > POD_PROFILE (padrão no documento).



Nesta etapa, configure o SNMP básico para MIBs globais.

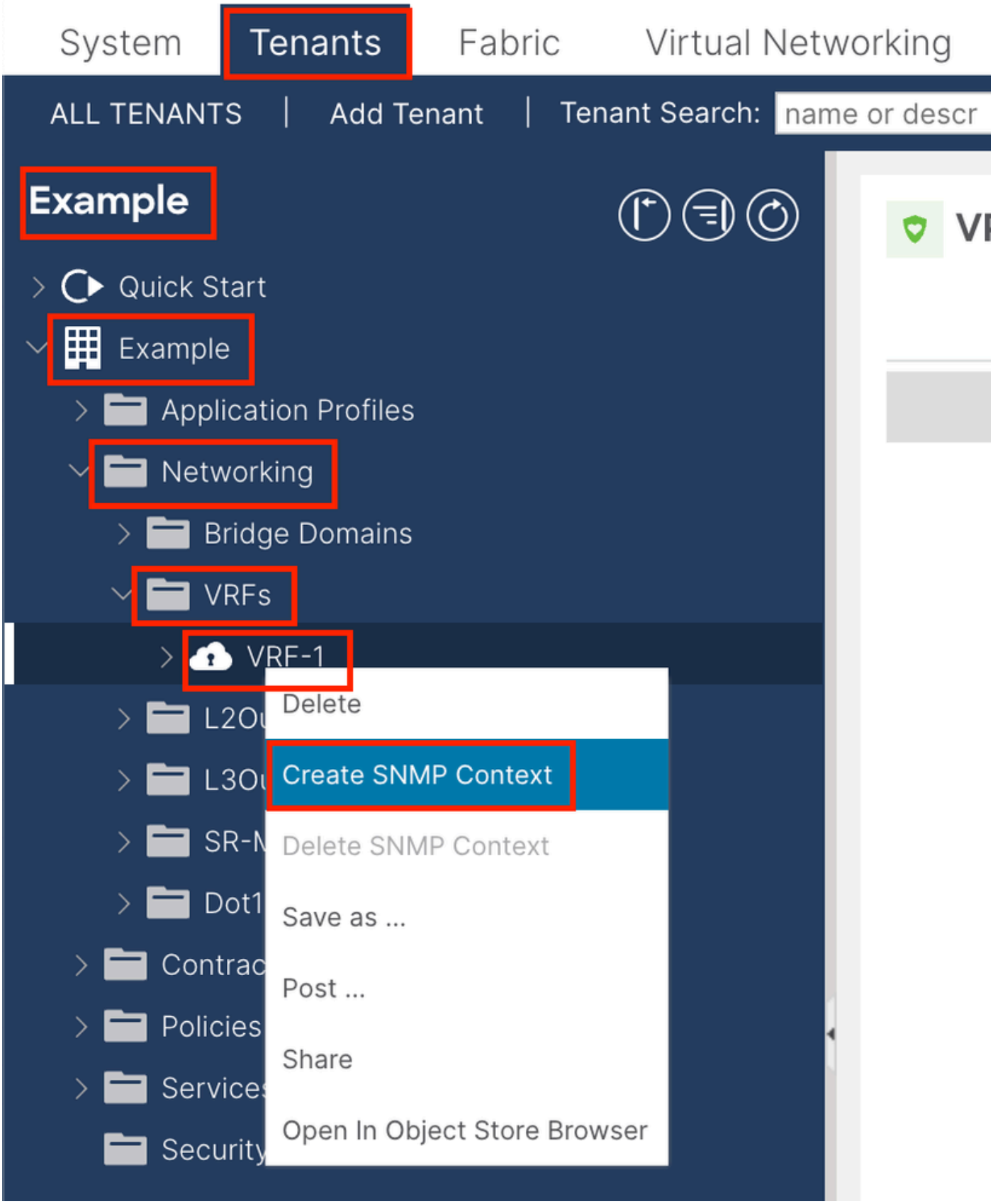


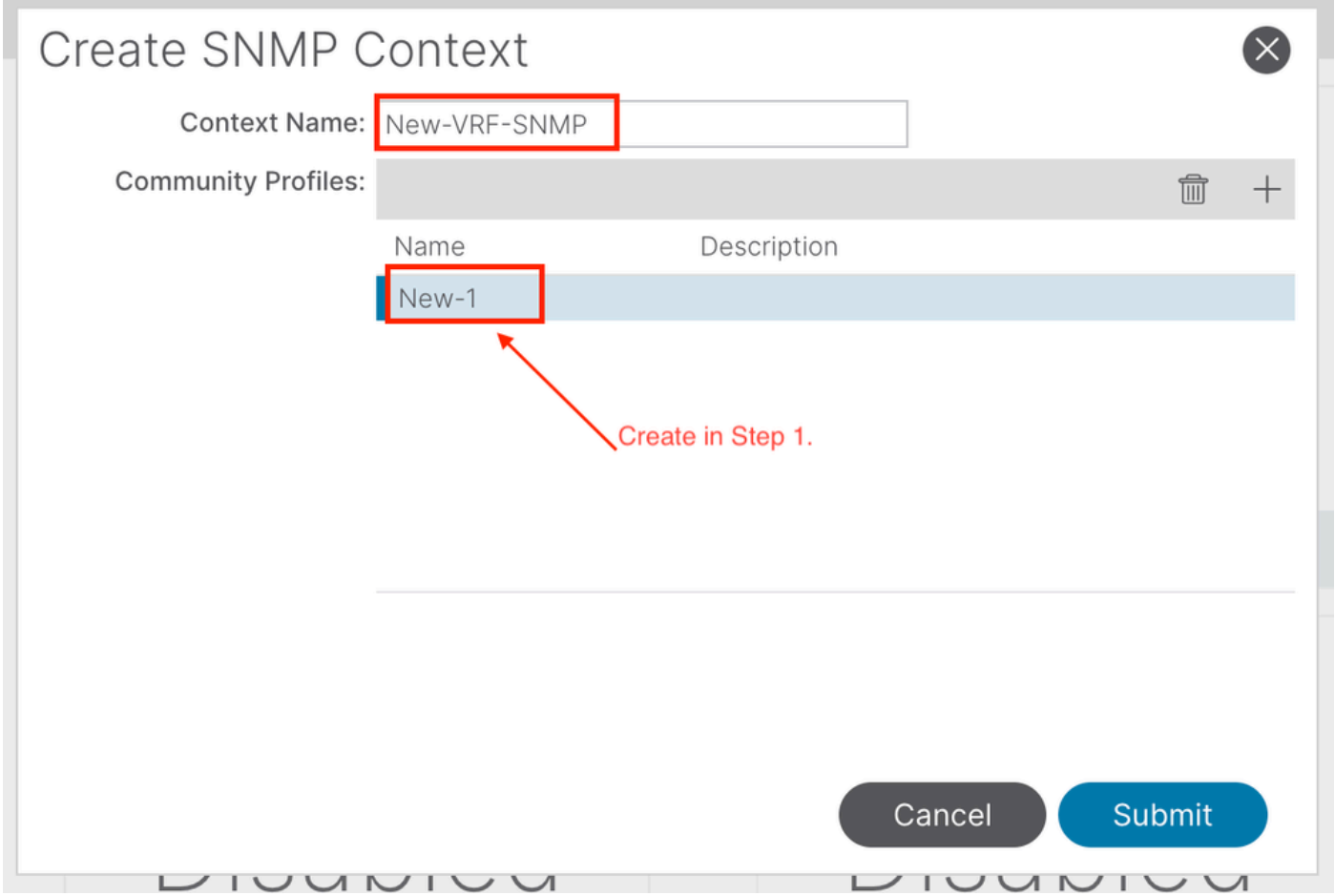
Observação: neste ponto, todas as etapas necessárias (Etapas 1-3) para a configuração do SNMP foram concluídas e o escopo global da MIB foi implicitamente usado. Isso permite que seja realizada uma caminhada SNMP para qualquer nó da ACI ou APIC.

Etapa 4. Configurar Escopos de Contexto VRF

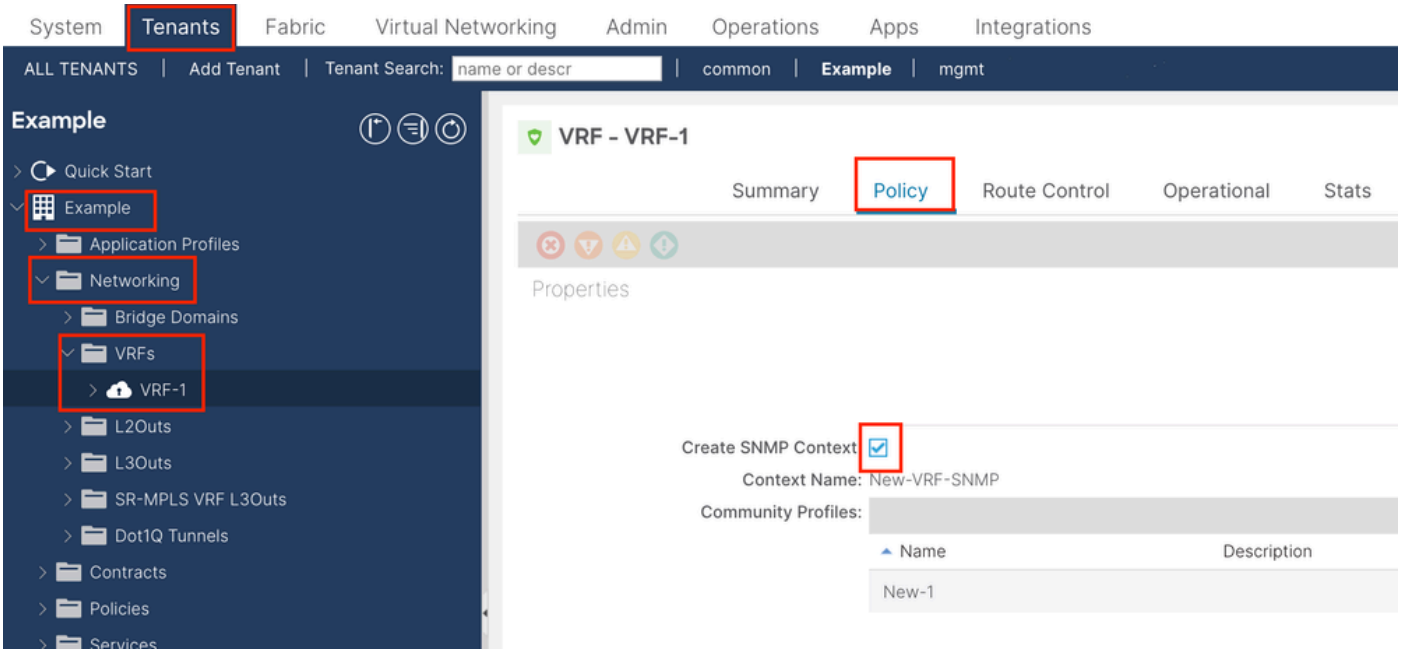
Depois de associar uma sequência de caracteres de comunidade a um Contexto VRF, essa sequência de caracteres de comunidade específica não pode ser usada para receber dados SNMP de escopo global. Portanto, é necessário criar duas séries de comunidade SNMP se você estiver procurando receber dados de SNMP de contexto global e de contexto VRF.

Nesse caso, as strings de comunidade criadas anteriormente (na Etapa 1.), ou seja, (**New-1**), use **New-1** para o escopo de contexto do VRF e **VRF-1** para o locatário personalizado de **Example** . Para fazer isso, navegue até o caminho da GUI da Web do APIC;
Tenants > Example > Networking > VRFs > VRF-1 (right click) > Create SNMP Context .


System
Tenants
Fabric
Virtual Networking
ALL TENANTS
Add Tenant
Tenant Search:
name or descr
Example
Quick Start
Example
Application Profiles
Networking
Bridge Domains
VRFs
VRF-1
Delete
Create SNMP Context
Delete SNMP Context
Save as ...
Post ...
Share
Open In Object Store Browser



Após enviar a configuração, você pode verificar a configuração do contexto SNMP aplicada clicando com o botão esquerdo do mouse em seu VRF, navegando até a guia Policy (Política) no VRF e rolando para baixo em direção à parte inferior do painel:

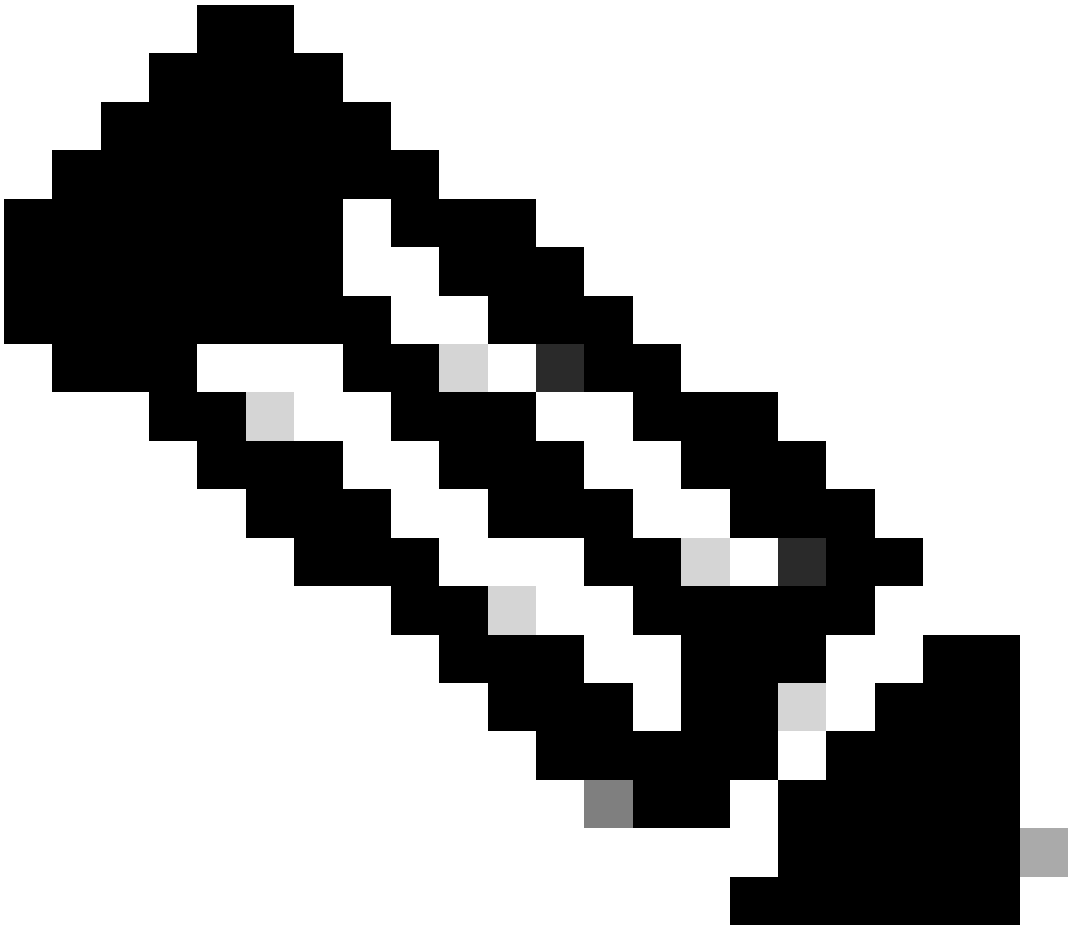


Para desabilitar um contexto SNMP em um VRF, você pode desmarcar a caixa de seleção **Criar contexto SNMP** (exibida na captura de tela) ou clicar com o botão direito do mouse no VRF e escolher **Excluir contexto SNMP**.

Configuração de SNMP TRAPs usando GUI

As TRAPs SNMP são enviadas ao servidor SNMP (SNMP Destination/Network Management Systems (NMS)) sem interrogação e o nó/APIC da ACI envia a TRAP SNMP assim que ocorre a falha/evento (condição definida).

As interceptações SNMP são habilitadas com base no escopo de política nas políticas de monitoramento Access/Fabric/Tenant. A ACI comporta no máximo 10 receptores Trap.

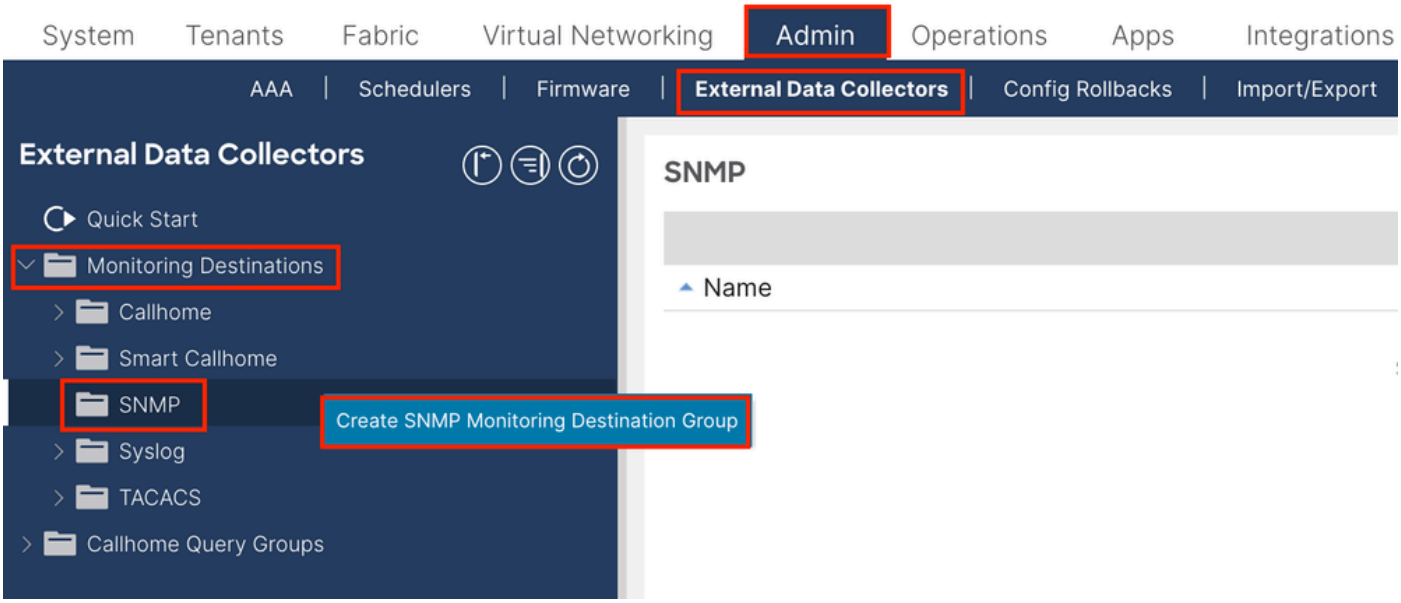


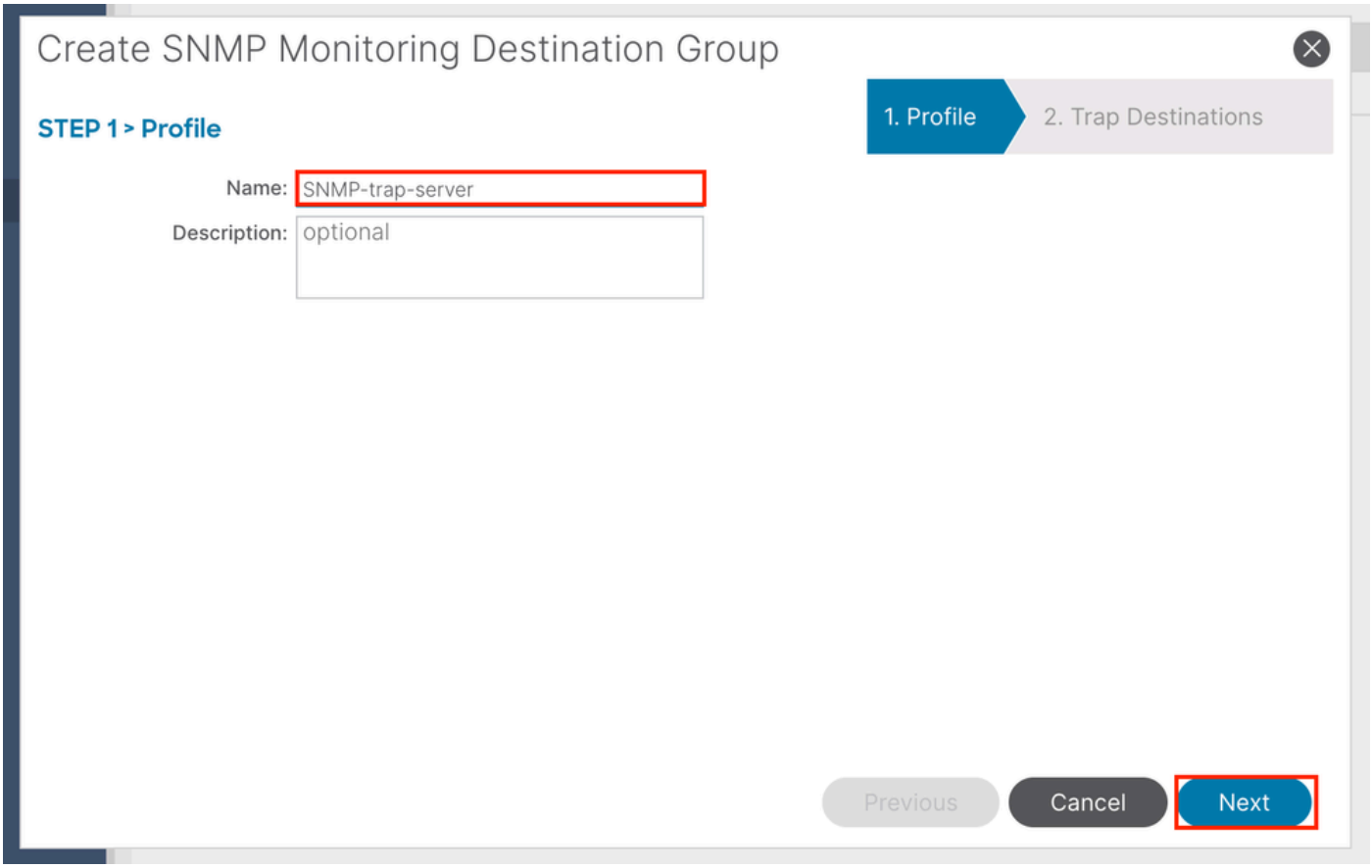
Observação: sem as etapas de 1 a 3 da seção anterior, a configuração de SNMP TRAPs não é suficiente. Etapa 2. na configuração do SNMP TRAP está relacionada às Políticas de monitoramento para (Acesso/Malha/Locatário).

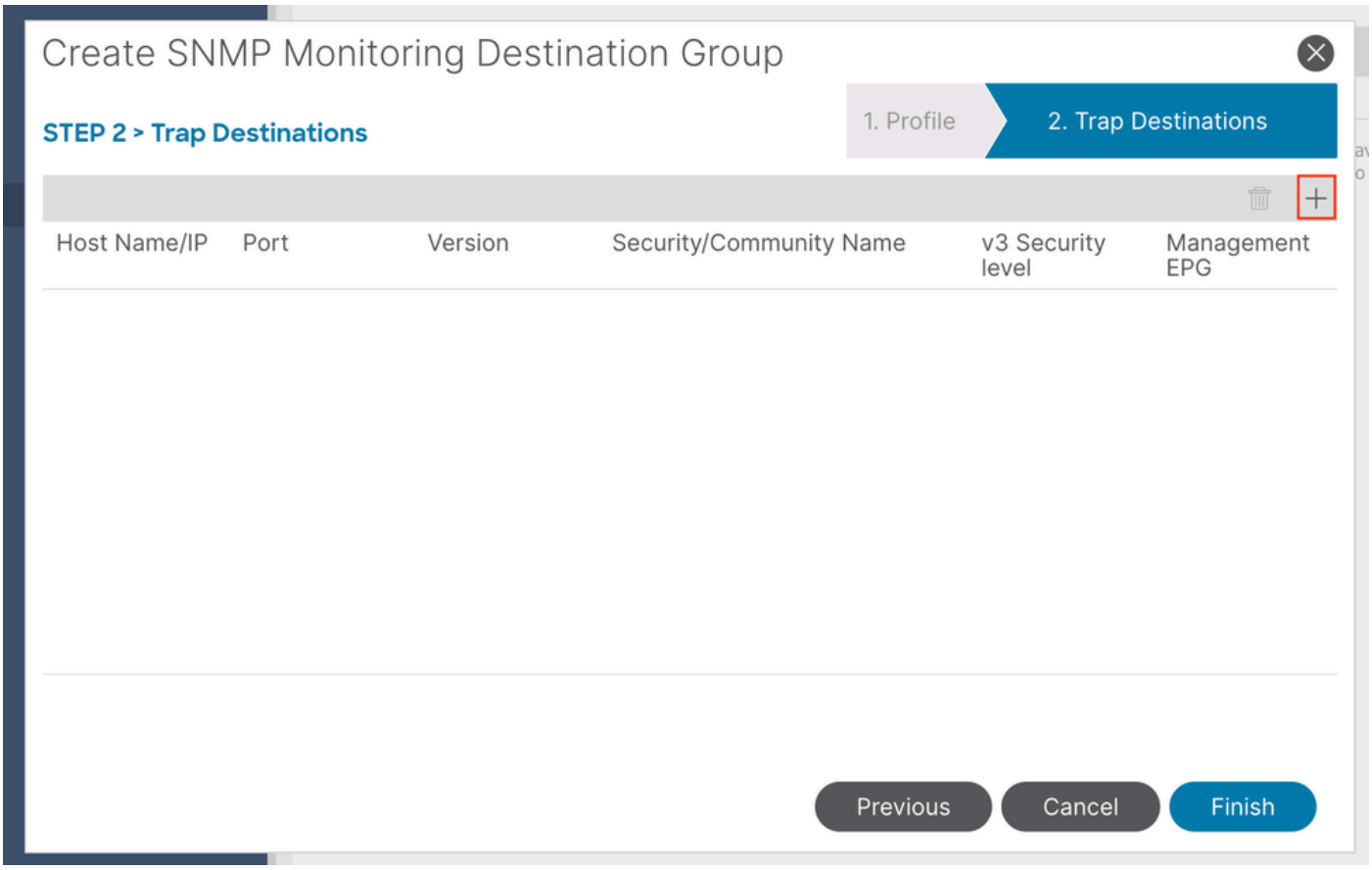
Para configurar TRAPs SNMP na ACI, você precisa das duas etapas além das etapas 1, 2 e 3 na seção anterior.

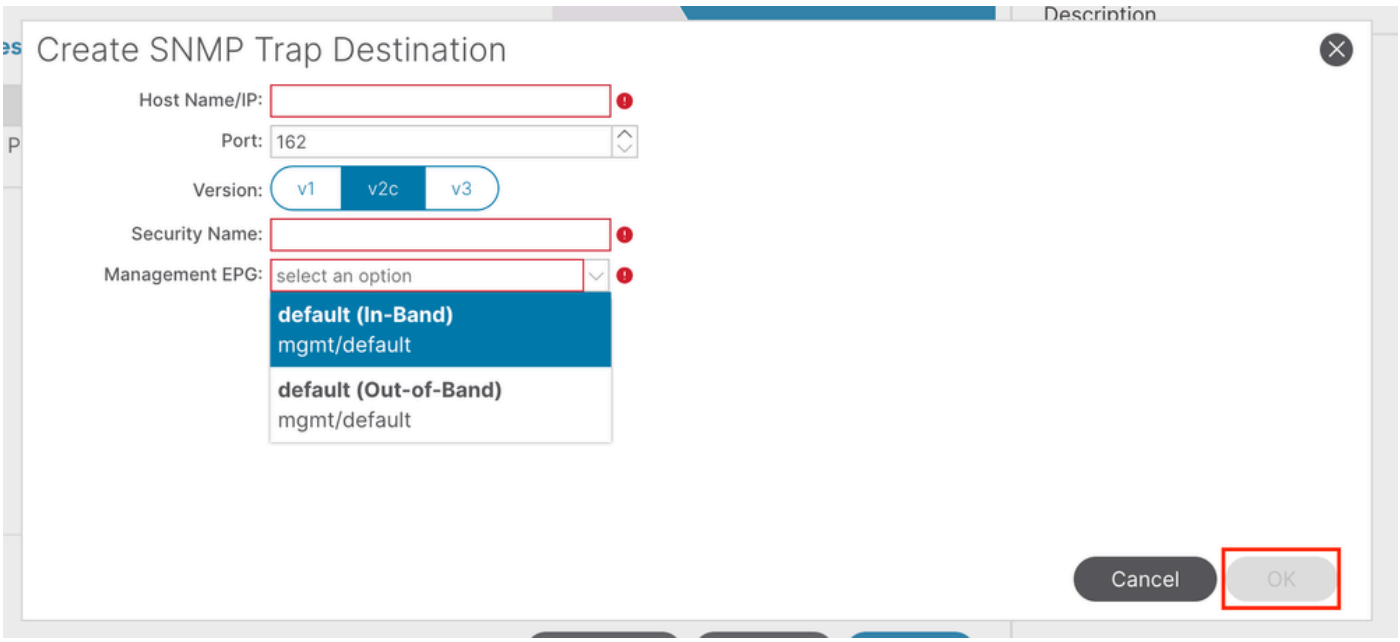
Etapa 1. Configurar servidor SNMP TRAP

Para fazer isso, navegue até o caminho da GUI da Web do APIC; Admin > Eternal Data Collectors > Monitoring Destinations > SNMP.









Host Name/IP - o host para o destino de interceptação SNMP.

Porta - a porta de serviço do destino de interceptação SNMP. O intervalo é de 0 (não especificado) a 65535; o padrão é 162.

Versão - a versão CDP suportada para o destino de interceptação SNMP. A versão pode ser:

- v1 - usa uma correspondência de community string para autenticação de usuário.

- v2c - usa uma correspondência de community string para autenticação de usuário.

- v3 - um protocolo interoperável baseado em padrões para gerenciamento de rede que fornece acesso seguro a dispositivos por uma combinação de quadros de autenticação e criptografia na rede.

O padrão é **v2c**.

Nome de segurança - o nome de segurança do destino de interceptação SNMP (nome da comunidade). Ele não pode conter o símbolo **@**.

Nível de segurança v.3 - o nível de segurança SNMPv3 para o caminho de destino SNMP. O nível pode ser:

- auth

- noauth

- priv

O padrão é **noauth**.

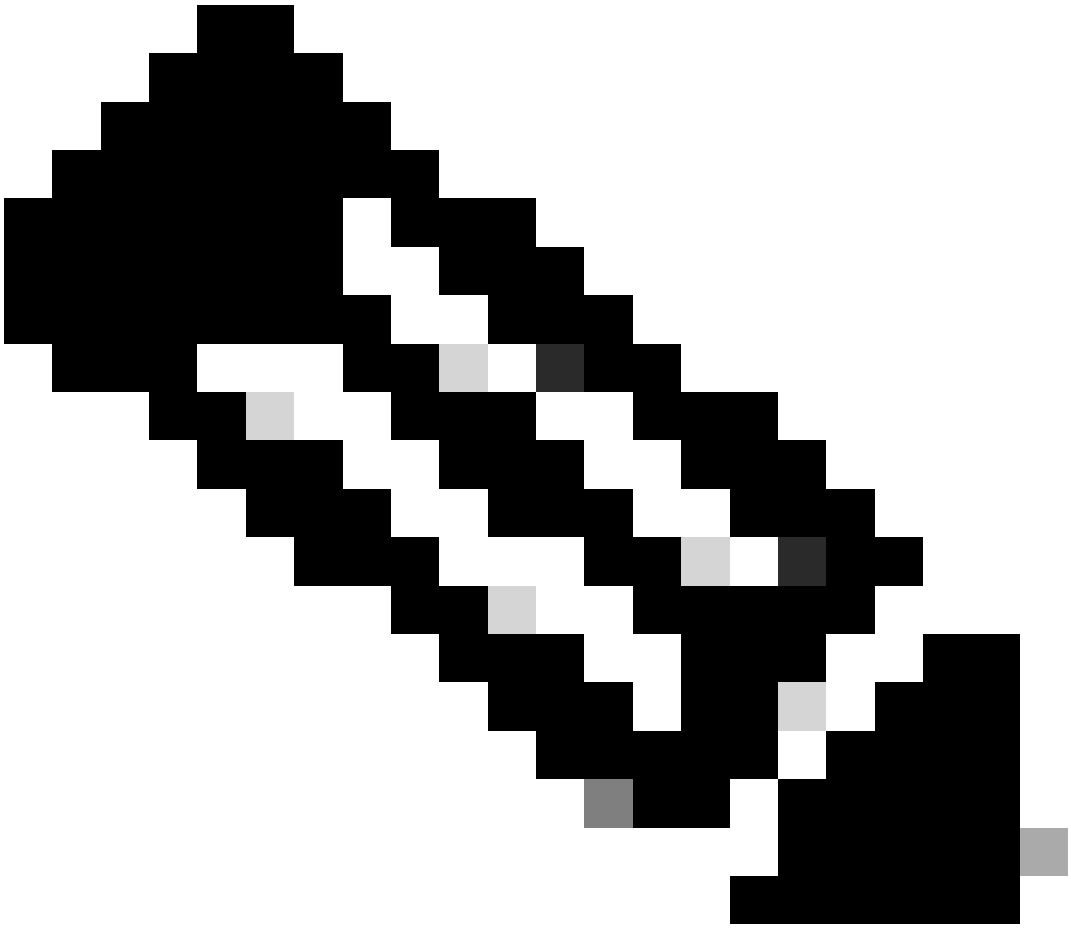
EPG de gerenciamento - o nome do grupo de endpoints de gerenciamento para o destino SNMP através do qual o host remoto pode ser alcançado.

Etapa 2. Configurar a origem de SNMP TRAP na política de monitoramento (acesso/malha/usuário)

Você pode criar políticas de monitoramento com os três escopos:

- Acesso - portas de acesso, FEX, controladores de VM
- Estrutura - portas, placas, chassi e ventiladores de estrutura

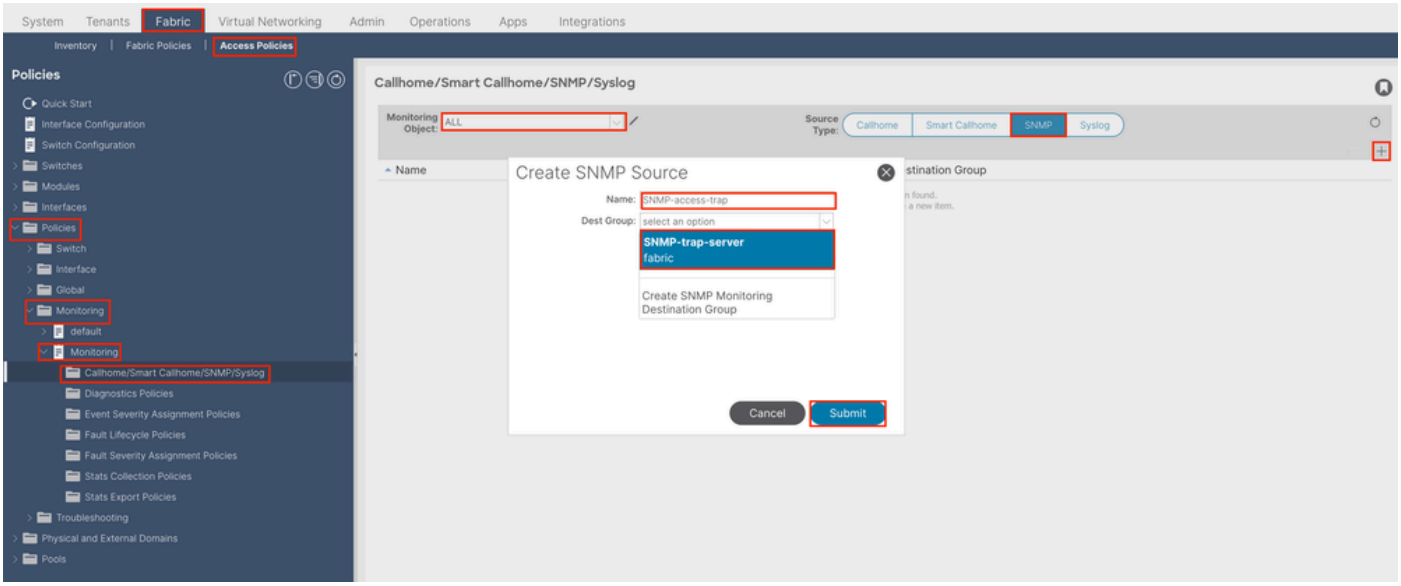
- Locatário - EPGs, perfis de aplicativo, serviços

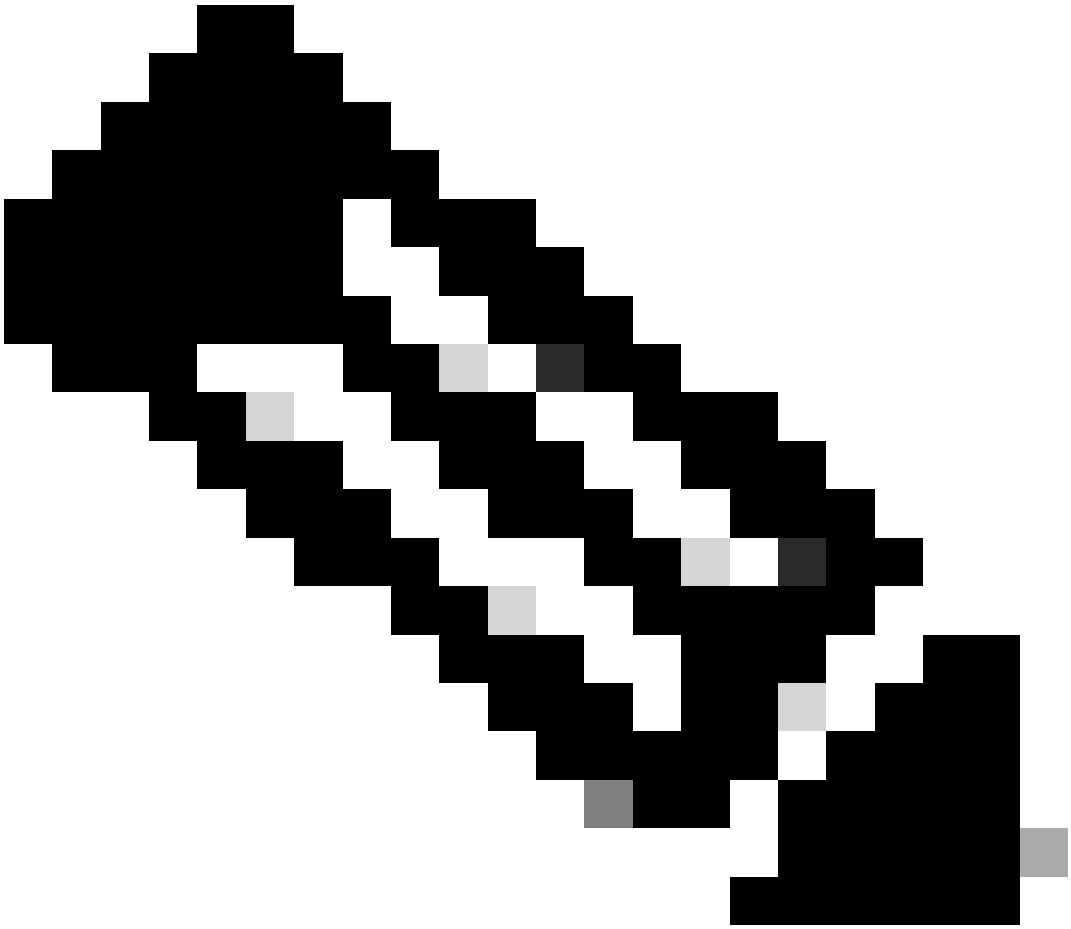


Observação: você pode escolher qualquer um ou qualquer combinação deles para configurar de acordo com suas necessidades.

Opção 1. Definir origem SNMP em Políticas de acesso

Para fazer isso, navegue até o caminho da GUI da Web do APIC; Fabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

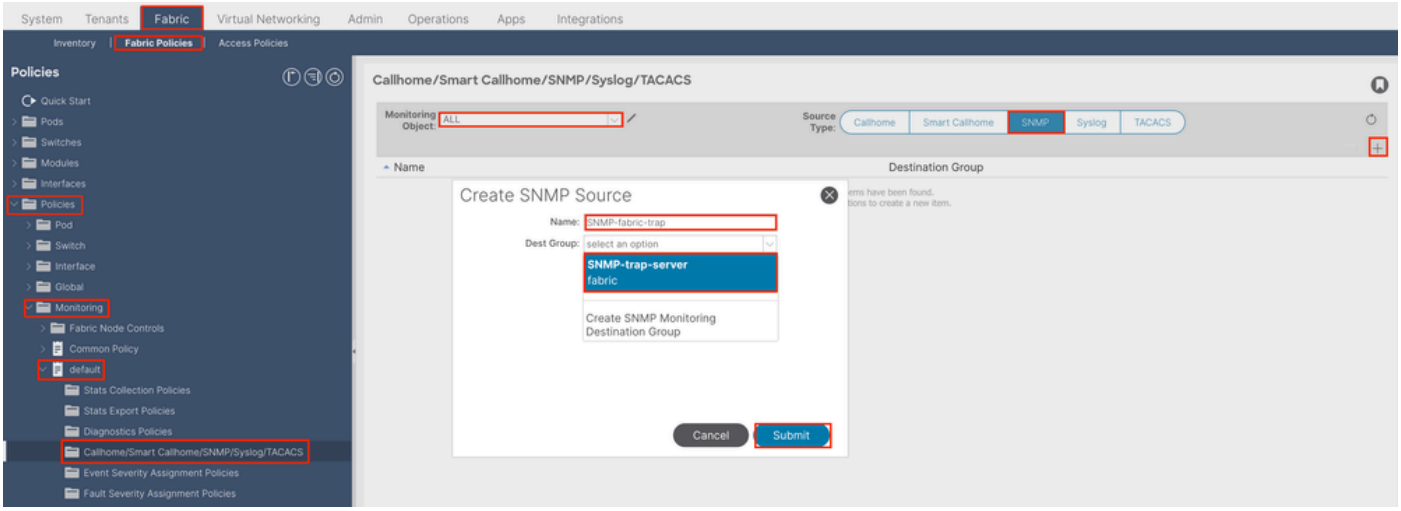

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog
Diagnostics Policies
Event Severity Assignment Policies
Fault Lifecycle Policies
Fault Severity Assignment Policies
Stats Collection Policies
Stats Export Policies
Troubleshooting
Physical and External Domains
Pools
Callhome/Smart Callhome/SNMP/Syslog
Monitoring Object:
ALL
Source Type:
Callhome
Smart Callhome
SNMP
Syslog
Name
Create SNMP Source
Name:
SNMP-access-trap
Dest Group:
select an option
SNMP-trap-server
fabric
Create SNMP Monitoring Destination Group
Cancel
Submit



Observação: você pode usar uma política de monitoramento definida pelo cliente (se configurada) em vez da padrão, use a padrão aqui. Você pode especificar qual objeto de monitoramento deve ser monitorado; todos foram usados aqui.

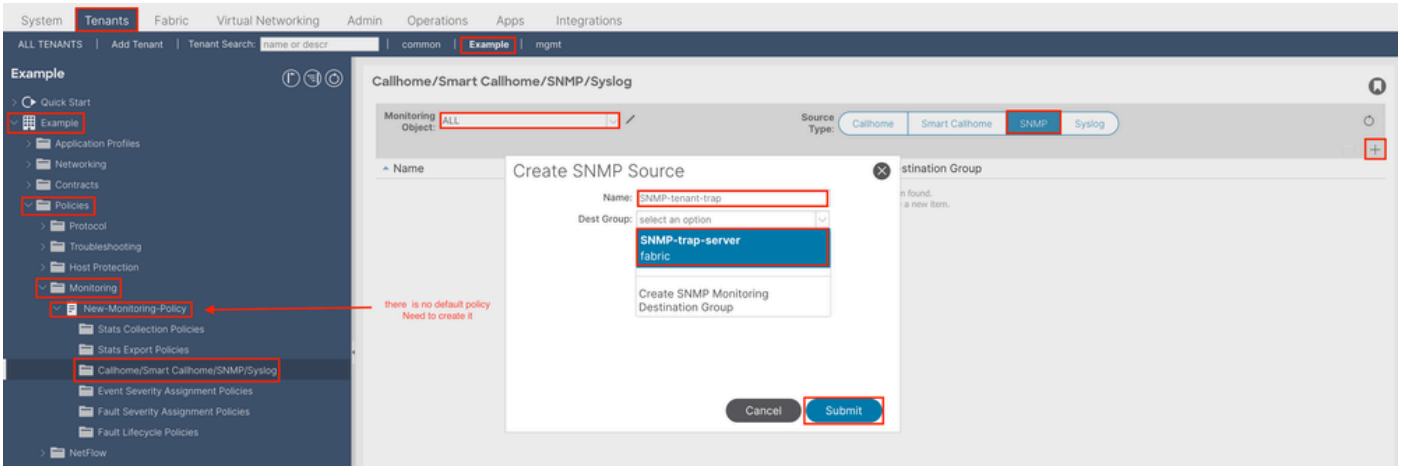
Opção 2. Definir origem SNMP em políticas de estrutura

Para fazer isso, navegue até o caminho da GUI da Web do APIC; Fabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Opção 3. Definir a origem SNMP nas políticas do usuário

Para fazer isso, navegue até o caminho da GUI da Web do APIC; Tenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Verificar

Use o comando snmpwalk para verificar

Primeiro, examine o recebimento de dados SNMP do escopo global de um switch leaf. Usar o comando snmpwalk pode fazer exatamente isso;

snmpwalk -v 2c -c New-1 x.x.x.x.

Esse comando desdobrado representa:

snmpwalk = O executável snmpwalk instalado no MacOS/Linux/Windows

-v = Especifica a versão do SNMP que deseja usar

2c= Especifica que estão usando o SNMP versão 2c

-c= Especifica que uma sequência de caracteres de comunidade específica

New-1= A string de comunidade é usada para receber dados SNMP de escopo global

x.x.x.x= O endereço IP de gerenciamento fora de banda do meu switch leaf

Resultado do comando:

```
$ snmpwalk -v 2c -c New-1 x.x.x.x SNMPv2-MIB::sysDescr.0 = STRING: Cisco NX-OS(tm) aci, Software (aci-n
```

Na saída do comando snipped, você pode ver que o snmpwalk é bem-sucedido e as informações específicas de hardware foram recebidas. Se você permitir que o snmpwalk continue, verá os nomes da interface de hardware, as descrições e assim por diante.

Agora, continue para recuperar os dados de SNMP do contexto de VRF, contextos de SNMP criados anteriormente, **New-VRF-SNMP** para VRFs utilizando a sequência de comunidade de SNMP, **New-1**.

Como a mesma string de comunidade é usada, **New-1**, em dois Contextos SNMP diferentes, você deve especificar de qual Contexto SNMP deseja que os dados SNMP sejam extraídos. Existe a sintaxe snmpwalk que você precisa usar para especificar um Contexto SNMP específico; snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.

Você pode ver que para extrair de um Contexto SNMP específico, você usa o formato: COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

Usando comandos show da CLI

No APIC:

```
show snmp show snmp policy <SNMP_policy_name> show snmp summary show snmp clientgroups show snmp commun
```

No Switch:

```
show snmp show snmp | grep "SNMP packets" show snmp summary show snmp community show snmp host show snm
```

Usando comandos Moquery da CLI

No APIC/Switch:

```
moquery -c snmpGroup #The SNMP destination group, which contains information needed to send traps or in
```

Utilizando comandos cat da CLI

No APIC:

```
cat /aci/tenants/mgmt/security-policies/out-of-band-contracts/summary cat /aci/tenants/mgmt/security-po
```

Troubleshooting

Verifique o processo snmpd

No Switch:

```
ps aux | grep snmp pidof snmpd
```

No APIC:

```
ps aux | grep snmp
```

Se o processo for normal, entre em contato com o TAC da Cisco para obter mais assistência.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.