Configuración de SNMP en ACI

Contenido

Introducción

Este documento describe la configuración del Protocolo simple de administración de red (SNMP) y las trampas SNMP en ACI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Descubrimiento de fabric completado
- Conectividad en banda/fuera de banda con su Application Policy Infrastructure Controller

(APIC) y switches de fabric
- Contratos en banda/fuera de banda configurados para permitir el tráfico SNMP (puertos UDP 161 y 162)
- Direcciones de administración de nodos estáticos configuradas para sus APIC y switches de fabric en el arrendatario de administración predeterminado (sin esto, falla la extracción de información SNMP de un APIC)
- Comprender el flujo de trabajo del protocolo SNMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- APIC
- Navegador
- Infraestructura centrada en aplicaciones (ACI) que ejecuta 5.2 (8e)
- Snmpwalk comando

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Cisco ACI proporciona compatibilidad con SNMPv1, v2c y v3, incluidas las bases de información de gestión (MIB) y las notificaciones (capturas). El estándar SNMP permite que cualquier aplicación de terceros que admita las diferentes MIB administre y supervise los switches de columna y de hoja de ACI y los controladores APIC.

Sin embargo, los comandos de escritura SNMP (Set) no se admiten en ACI.

La política SNMP se aplica y se ejecuta independientemente en los switches de hoja y columna y en los controladores APIC. Dado que cada dispositivo ACI tiene su propia entidad SNMP, es decir, los múltiples APIC de un clúster APIC deben supervisarse por separado, así como los switches. Sin embargo, el origen de la política SNMP se crea como política de supervisión para todo el fabric de ACI.

De forma predeterminada, SNMP utiliza el puerto **UDP 161** para el sondeo y el puerto **162** para las TRAMPAS.

Comprensión de los alcances SNMP

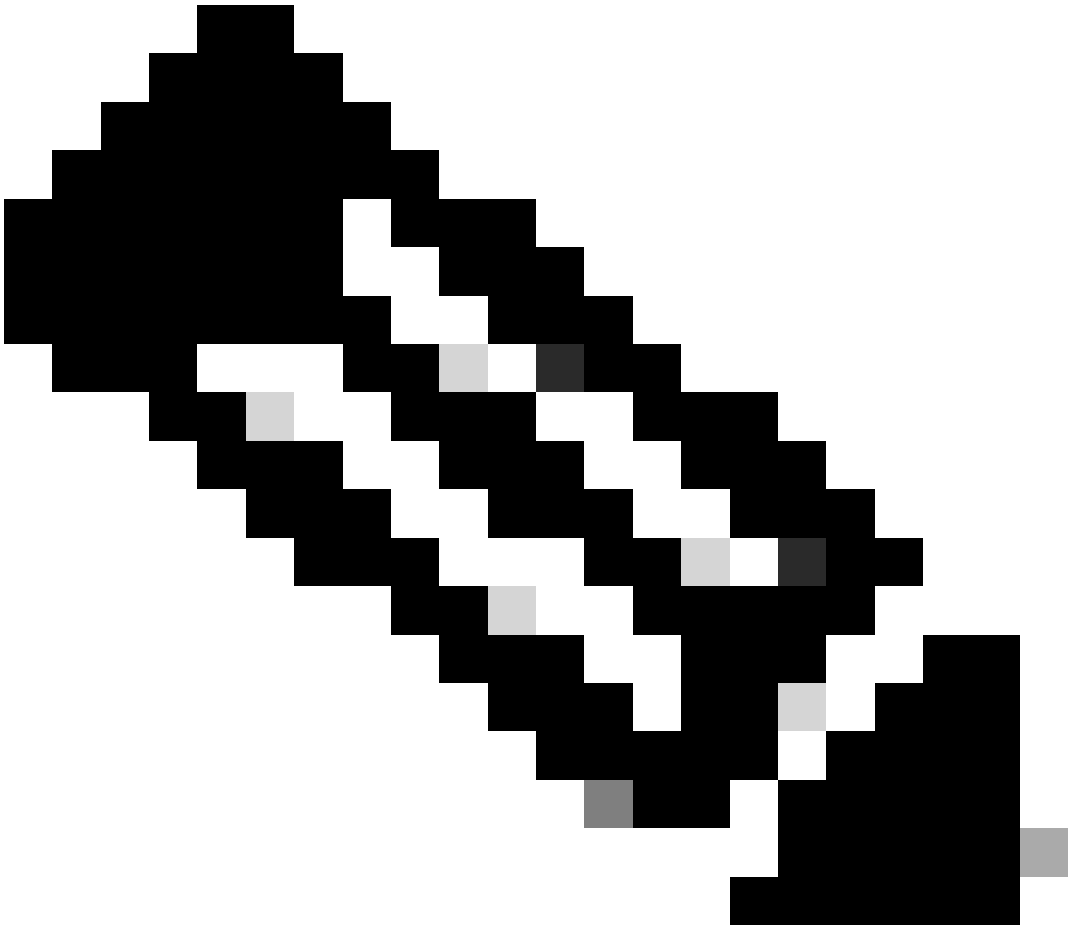
Un concepto fundamental rápido de SNMP en ACI es que hay dos ámbitos de los cuales se puede extraer información SNMP:
1. A escala mundial
2. Contexto de reenvío y routing virtuales (VRF)

El **ámbito global** es extraer MIB de chasis como el número de interfaces, índices de interfaz, nombres de interfaz, estado de interfaz, etc. de un nodo de hoja/columna.

Las MIB específicas de alcance de contexto de VRF obtienen información específica de VRF, como direcciones IP e información de

protocolo de ruteo.

Hay una lista completa de MIB de contexto VRF y globales de switch de fabric y APIC compatibles en la Lista de soporte de MIB de Cisco ACI.

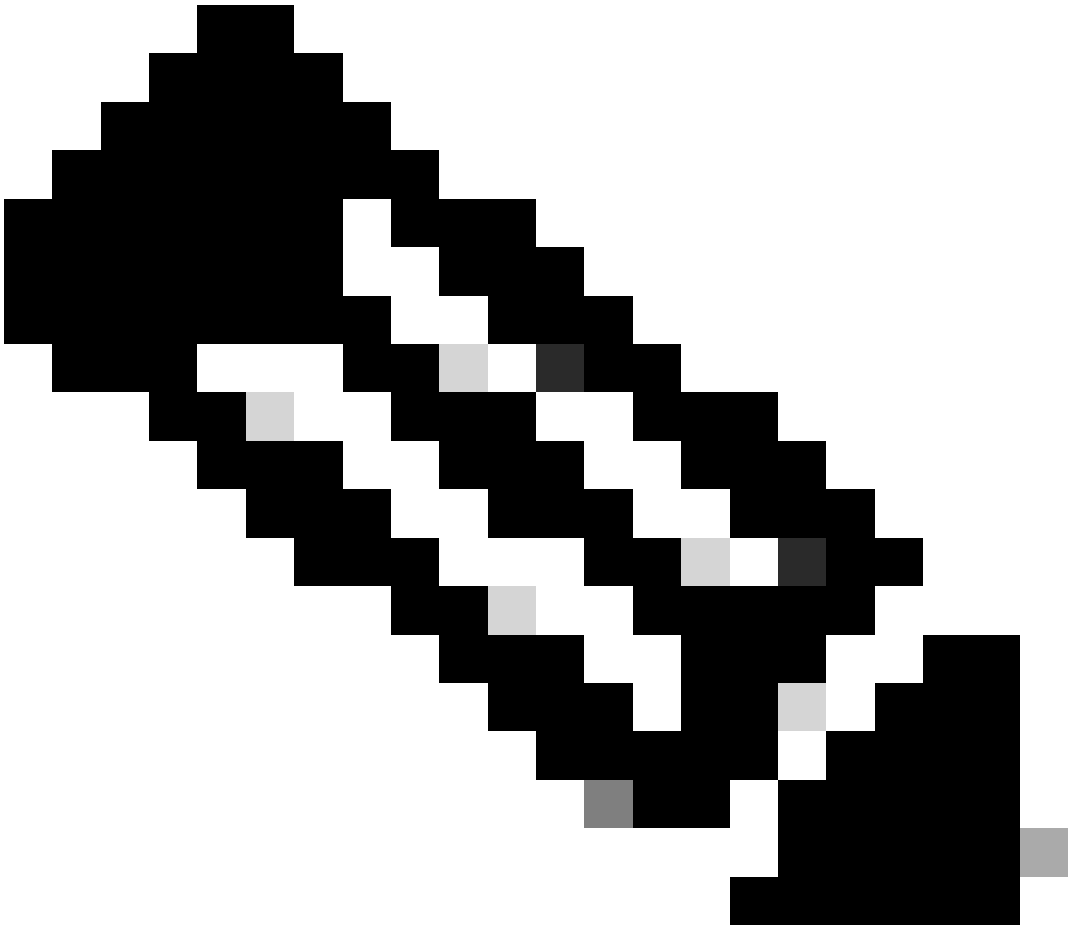


Nota: Una MIB con un ámbito Global sólo tiene una instancia en el sistema. Los datos de una MIB global se relacionan con el sistema general.

Una MIB con alcance específico de VRF puede tener instancias por VRF en el sistema. Los datos en una MIB específica de VRF se relacionan solamente con ese VRF.

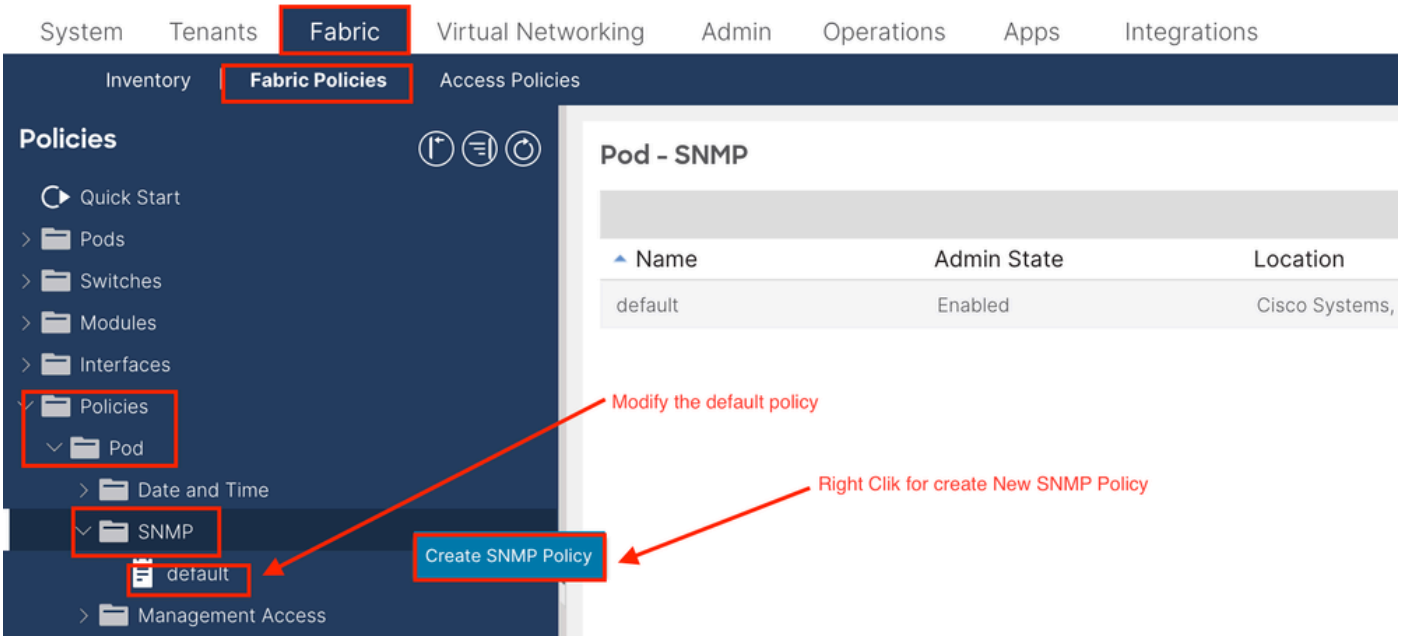
Pasos de Configuración (Para Ámbitos de Contexto Global y VRF)

Paso 1. Configurar la política de fabric SNMP



Nota: Aquí se especifican las configuraciones SNMP, como las políticas de comunidad SNMP y las políticas de grupo de clientes SNMP.

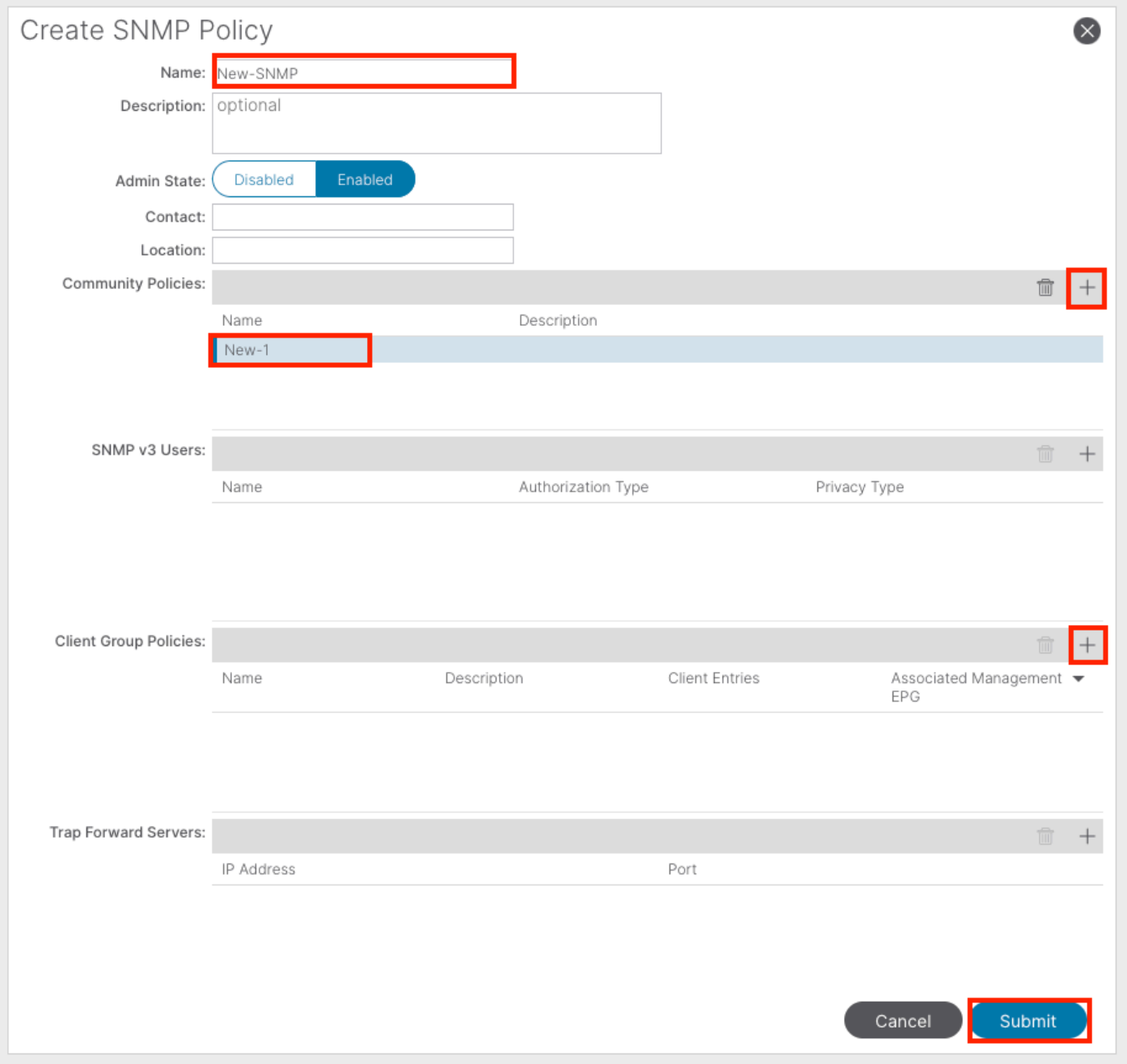
El primer paso en la configuración de SNMP es crear las políticas de fabric SNMP necesarias. Para crear las políticas de entramado SNMP, navegue hasta la ruta GUI web APIC; Fabric > Fabric Policies > Policies > Pod > SNMP.



Puede crear una nueva política SNMP o modificar la política SNMP predeterminada.

En el documento, la política SNMP se llama **New-SNMP** y utiliza la versión v2c de SNMP, por lo que los únicos campos necesarios aquí son políticas de comunidad y políticas de grupo de clientes.

El campo Community Policy Name define la cadena de comunidad SNMP que se utilizará. En nuestro caso, **New-1**. Verá dónde entran estas dos cadenas de comunidad más adelante.



Nombre: el nombre de la política SNMP. Este nombre puede tener entre 1 y 64 caracteres alfanuméricos.

Description (Descripción): la descripción de la política SNMP. La descripción puede tener entre 0 y 128 caracteres alfanuméricos.

Admin State - el estado administrativo de la política SNMP. El estado puede estar activado o desactivado. Los estados son:

- enabled (habilitado): el estado de administración está habilitado
- inhabilitado: el estado del administrador es inhabilitado

El valor predeterminado es **disabled**.

Contacto: la información de contacto de la política SNMP.

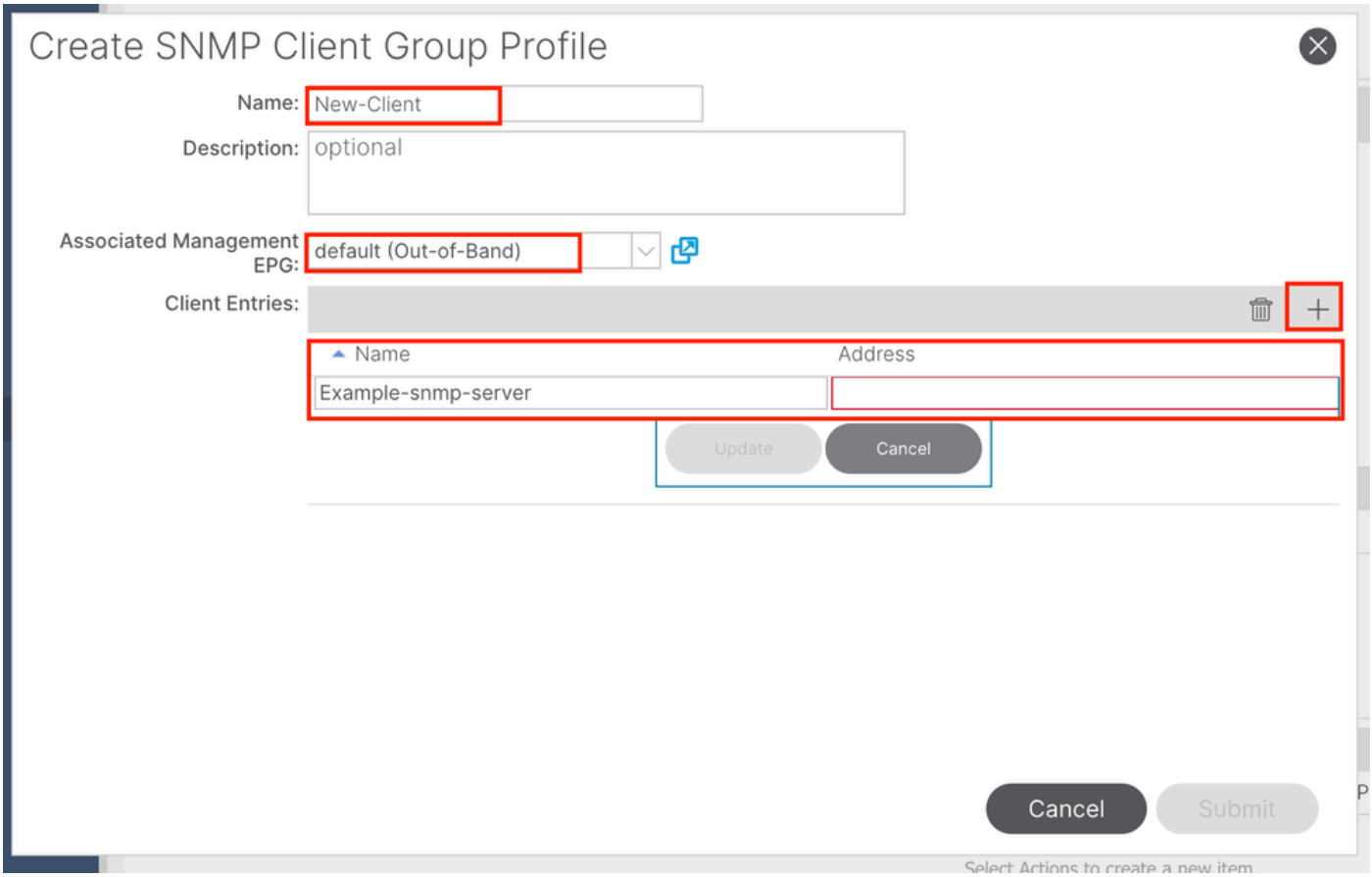
Location (Ubicación): la ubicación de la política SNMP.

Usuarios SNMP v3: el perfil de usuario SNMP se utiliza para asociar usuarios con políticas SNMP para monitorear dispositivos en una red.

Políticas de comunidad: el perfil de comunidad SNMP habilita el acceso al router o a las estadísticas del switch para monitoreo.

Políticas de grupos de clientes:

El siguiente paso es agregar el perfil/directiva de grupo de clientes. El propósito del perfil/política de grupo de clientes es definir qué IP/subredes pueden extraer datos SNMP de APIC y switches de fabric:



Nombre: el nombre del perfil del grupo de clientes. Este nombre puede tener entre 1 y 64 caracteres alfanuméricos.

Descripción: la descripción del perfil del grupo de clientes. La descripción puede tener entre 0 y 128 caracteres alfanuméricos.

Associated Management End Point Group (EPG): nombre distinguido de un grupo de terminales a través del cual se puede acceder al VRF. La longitud máxima de cadena admitida es de 255 caracteres ASCII. El valor predeterminado es el EPG de acceso a la administración fuera de banda del arrendatario de administración.

Entradas de cliente: la dirección IP del perfil de cliente SNMP.

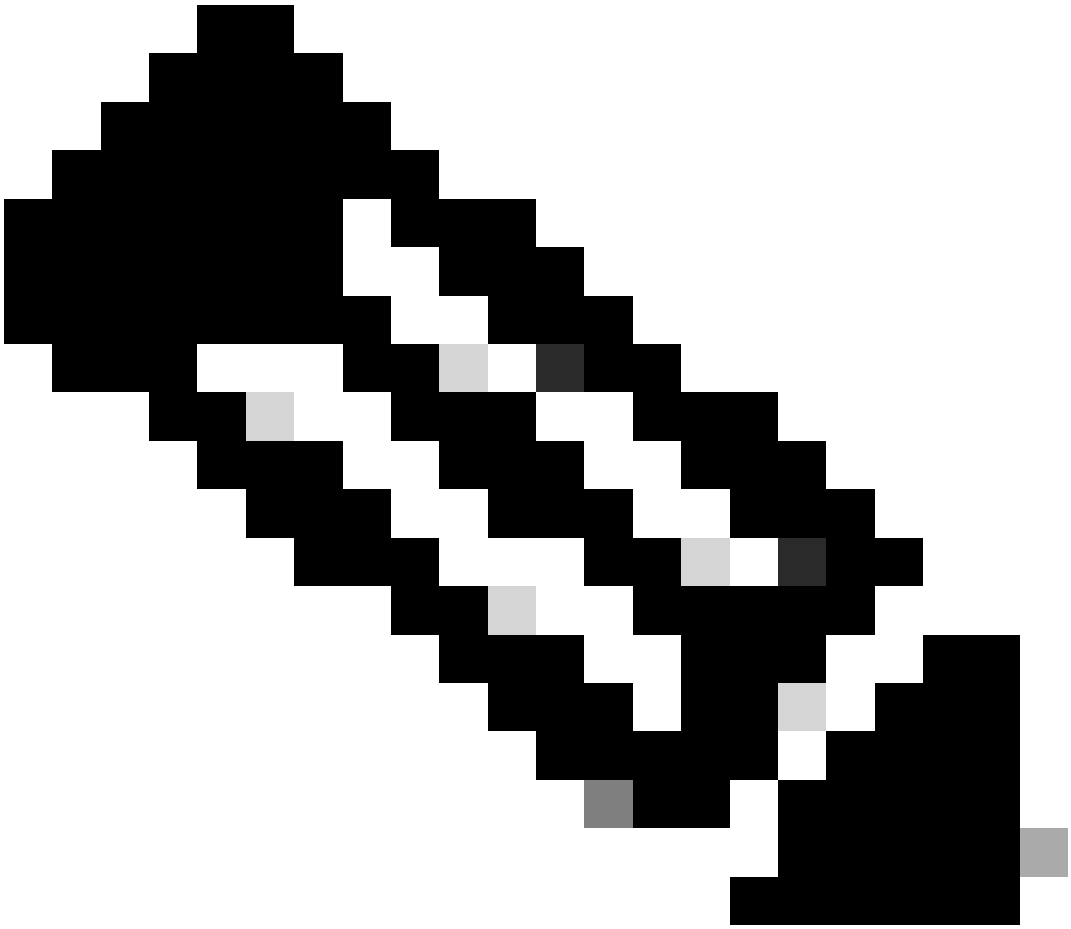
En el documento, el perfil/directiva de grupo de clientes se denomina **New-Client**.

En el perfil/política de grupo de clientes debe asociar el EPG de administración preferido. Debe asegurarse de que el EPG de administración que

elija tenga los contratos necesarios para permitir el tráfico SNMP (puertos UDP 161 y 162). El EPG de administración fuera de banda predeterminado se utiliza en el documento para fines de demostración.

El último paso es definir sus **entradas de cliente** para permitir el acceso de IPs específicas o subredes enteras para extraer datos SNMP de ACI. Hay una sintaxis para definir una IP específica o una subred completa:

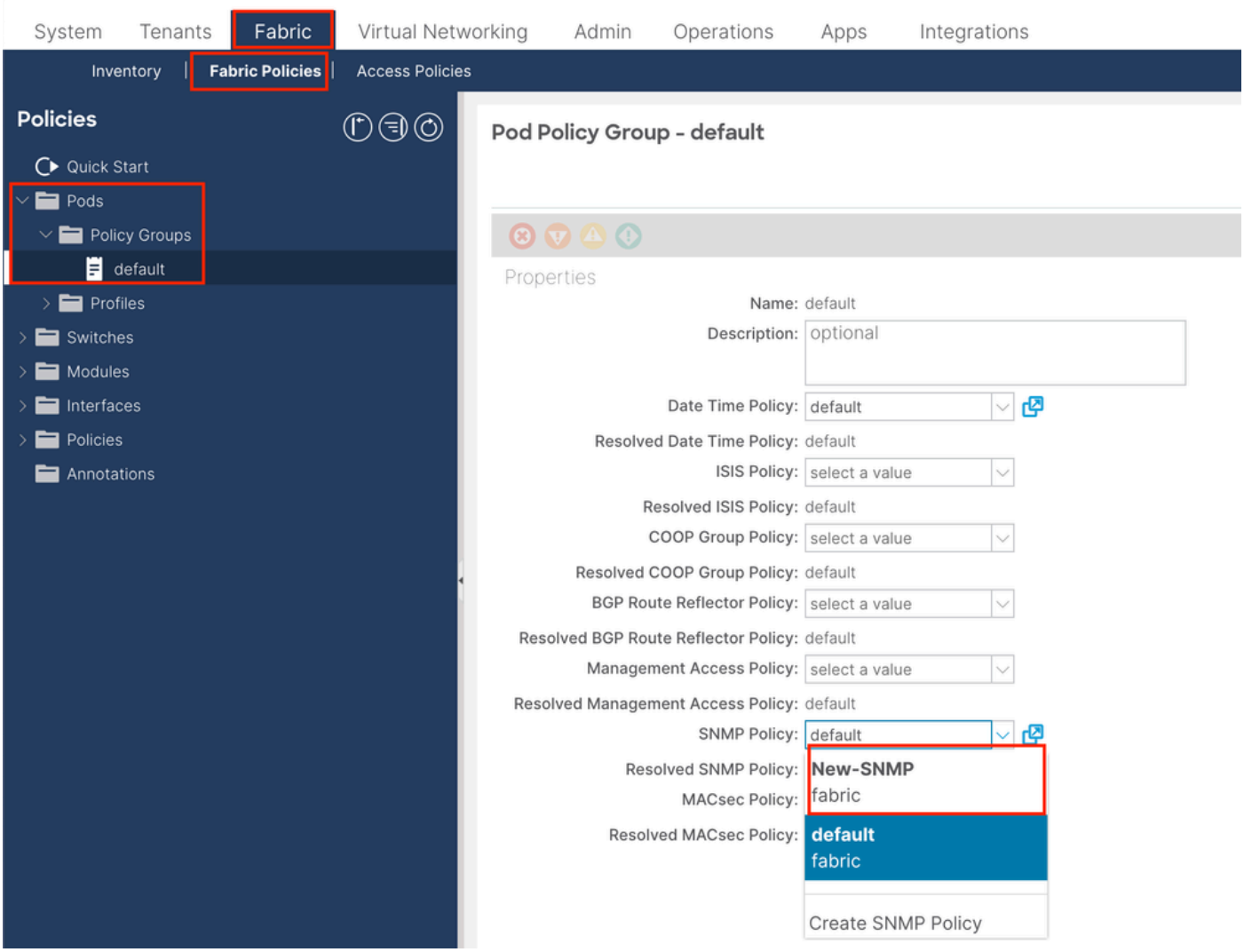
- IP de host específica: 192.168.1.5
- Subred completa: 192.168.1.0/24



Nota: No puede utilizar 0.0.0.0 en la entrada de cliente para permitir todas las subredes (si desea permitir que todas las subredes accedan a SNMP MIB, deje las entradas de cliente vacías).

Paso 2. Aplicación de la política SNMP al grupo de políticas de grupo de dispositivos (grupo de políticas de fabric)

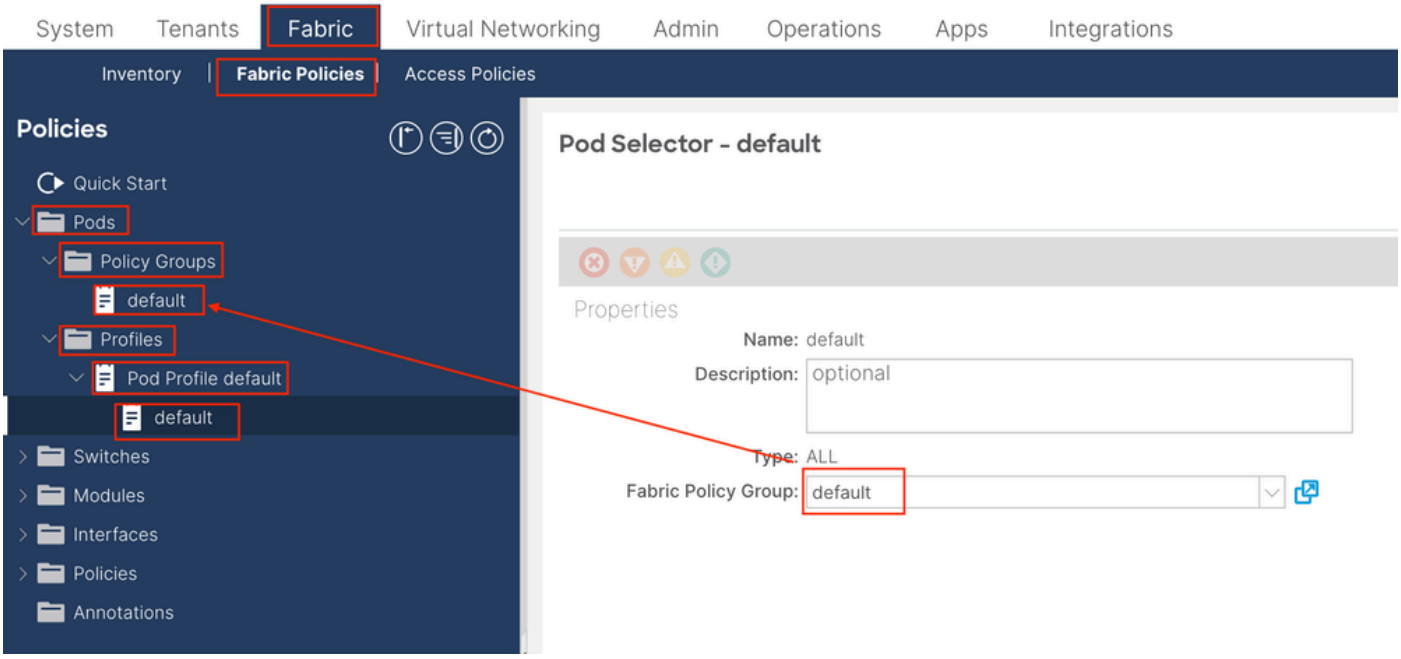
Para aplicar esta configuración, navegue hasta la ruta GUI web de APIC; Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP (valor predeterminado en el documento).



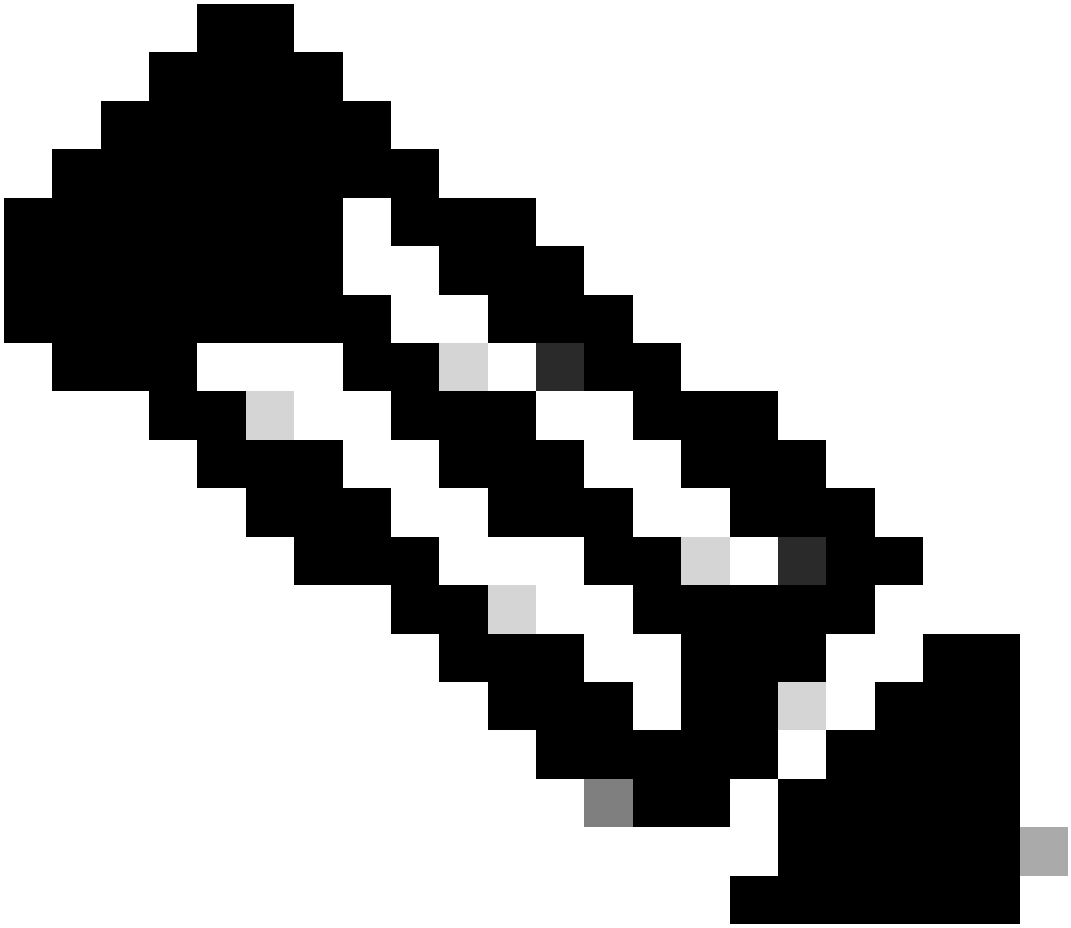
En el panel derecho, verá un campo para Política SNMP. En el menú desplegable, seleccione la política SNMP recién creada y envíe los cambios.

Paso 3. Asociación del grupo de políticas de grupo de dispositivos con el perfil de grupo de dispositivos

En el documento, utilice el perfil de grupo predeterminado para simplificar. Para hacerlo, navegue hasta la ruta GUI web de APIC; Fabric > Fabric Policies > Pods > Profiles > POD_PROFILE (valor predeterminado en el documento).



En esta etapa, configure el SNMP básico para los MIB globales.

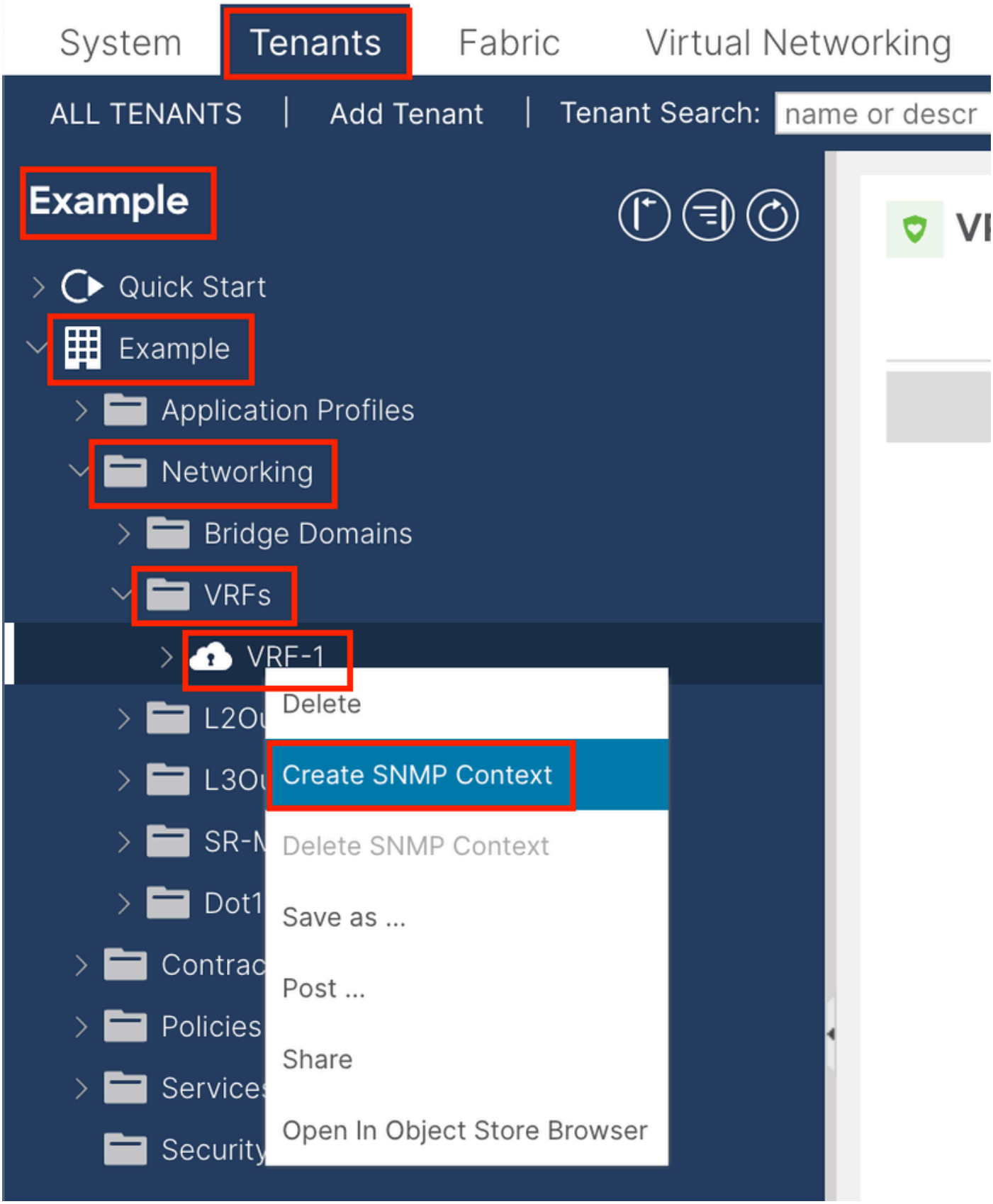


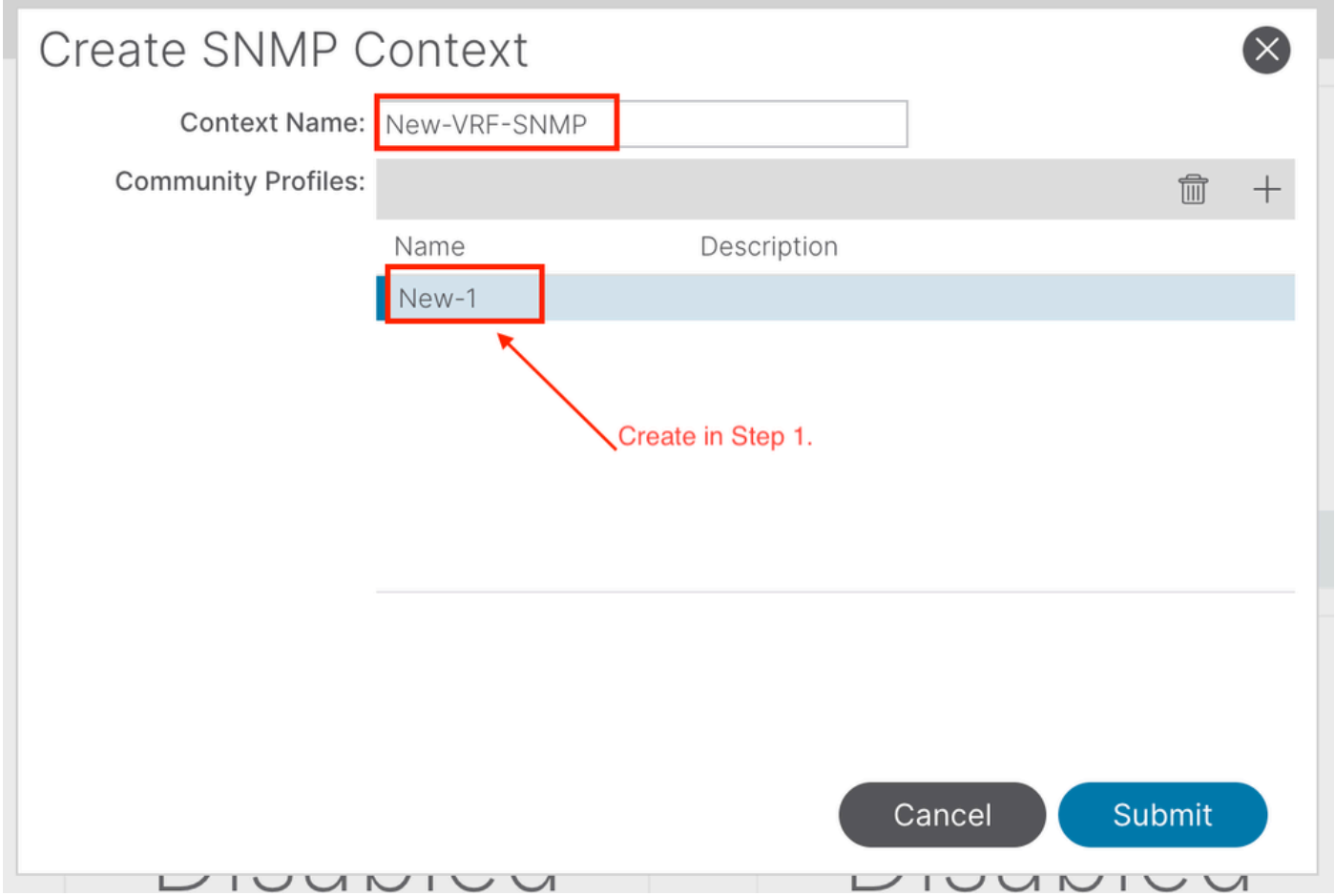
Nota: En este momento, se han completado todos los pasos necesarios (pasos 1-3) para la configuración de SNMP y se ha utilizado implícitamente el alcance global de MIB. Esto permite realizar un recorrido SNMP para cualquier nodo ACI o APIC.

Paso 4. Configuración de Ámbitos de Contexto VRF

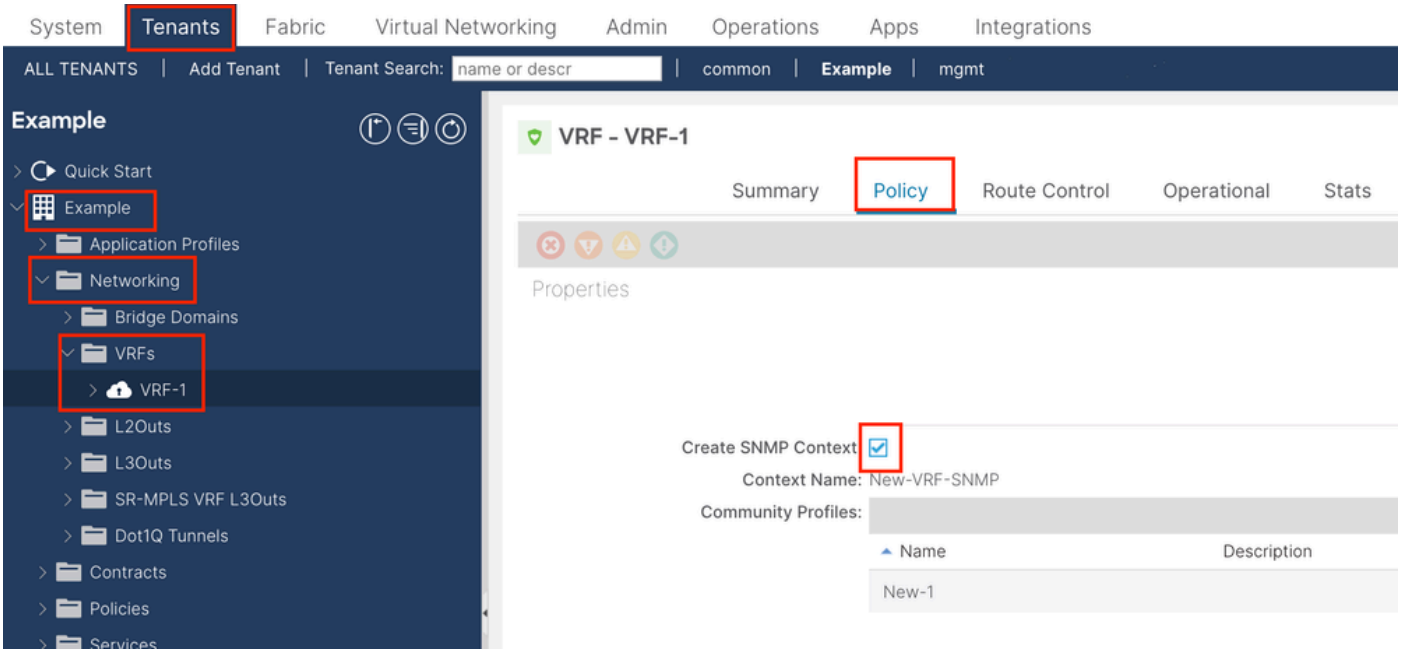
Una vez asociada una cadena de comunidad a un contexto VRF, esa cadena de comunidad específica no se puede utilizar para extraer datos SNMP de ámbito global. Por lo tanto, es necesario crear dos cadenas de comunidad SNMP si se desea extraer datos SNMP de ámbito global y de contexto VRF.

En este caso, las cadenas de comunidad creadas anteriormente (en el paso 1), a saber, (**New-1**), utilizan **New-1** para el ámbito de contexto VRF y **VRF-1** VRF personalizado en el **ejemplo** de arrendatario personalizado. Para hacerlo, navegue a la ruta de la GUI web de 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



Después de enviar la configuración, puede verificar la configuración de Contexto SNMP que aplicó haciendo clic con el botón izquierdo del ratón en su VRF, navegando a la pestaña Política en el VRF y desplazándose hacia abajo hacia la parte inferior del panel:

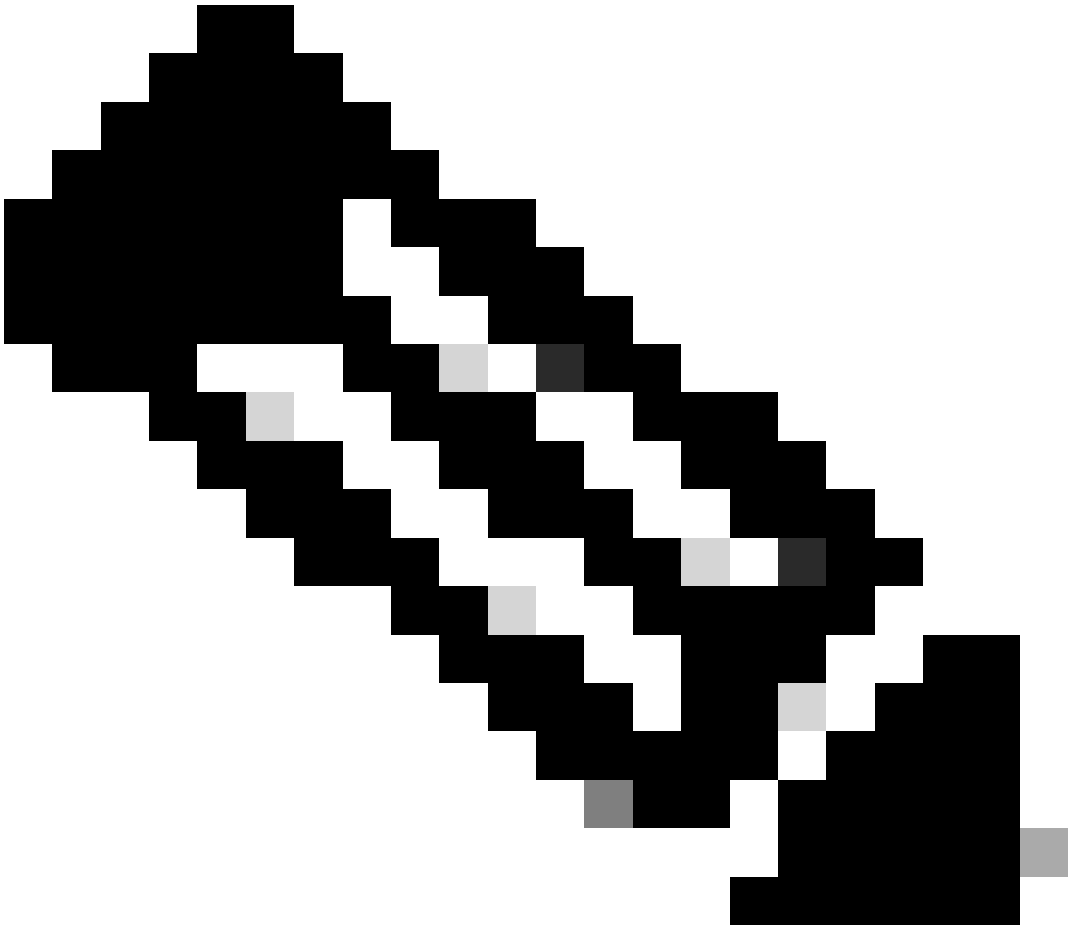


Para inhabilitar un Contexto SNMP en un VRF, puede deseleccionar la casilla de verificación **Create SNMP Context** (que se ve en la captura de pantalla), o hacer clic con el botón derecho en el VRF y elegir **Delete SNMP Context**.

Configuración de SNMP TRAPs mediante GUI

Las SNMP TRAP se envían al servidor SNMP (SNMP Destination/Network Management Systems (NMS)) sin sondear, y el nodo ACI/APIC envía la SNMP TRAP una vez que se produce el fallo/evento (condición definida).

Las trampas SNMP se habilitan según el alcance de la política bajo las políticas de monitoreo de acceso/estructura/arrendatario. ACI admite un máximo de 10 receptores de trampas.

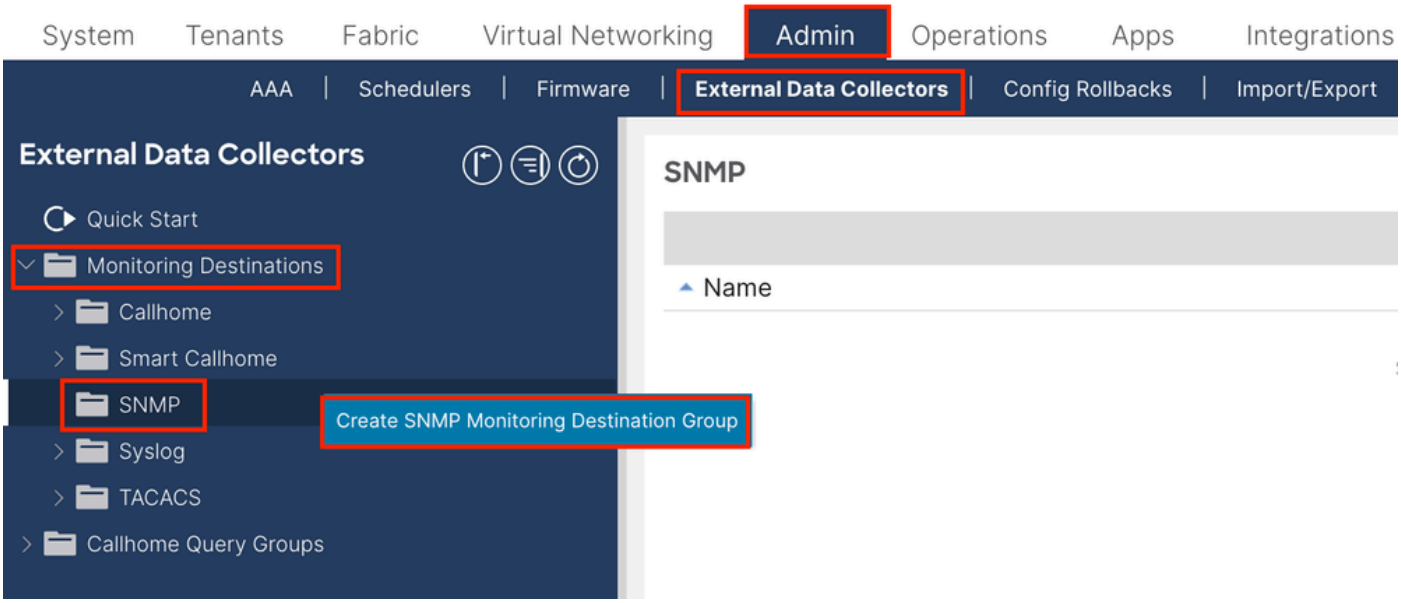


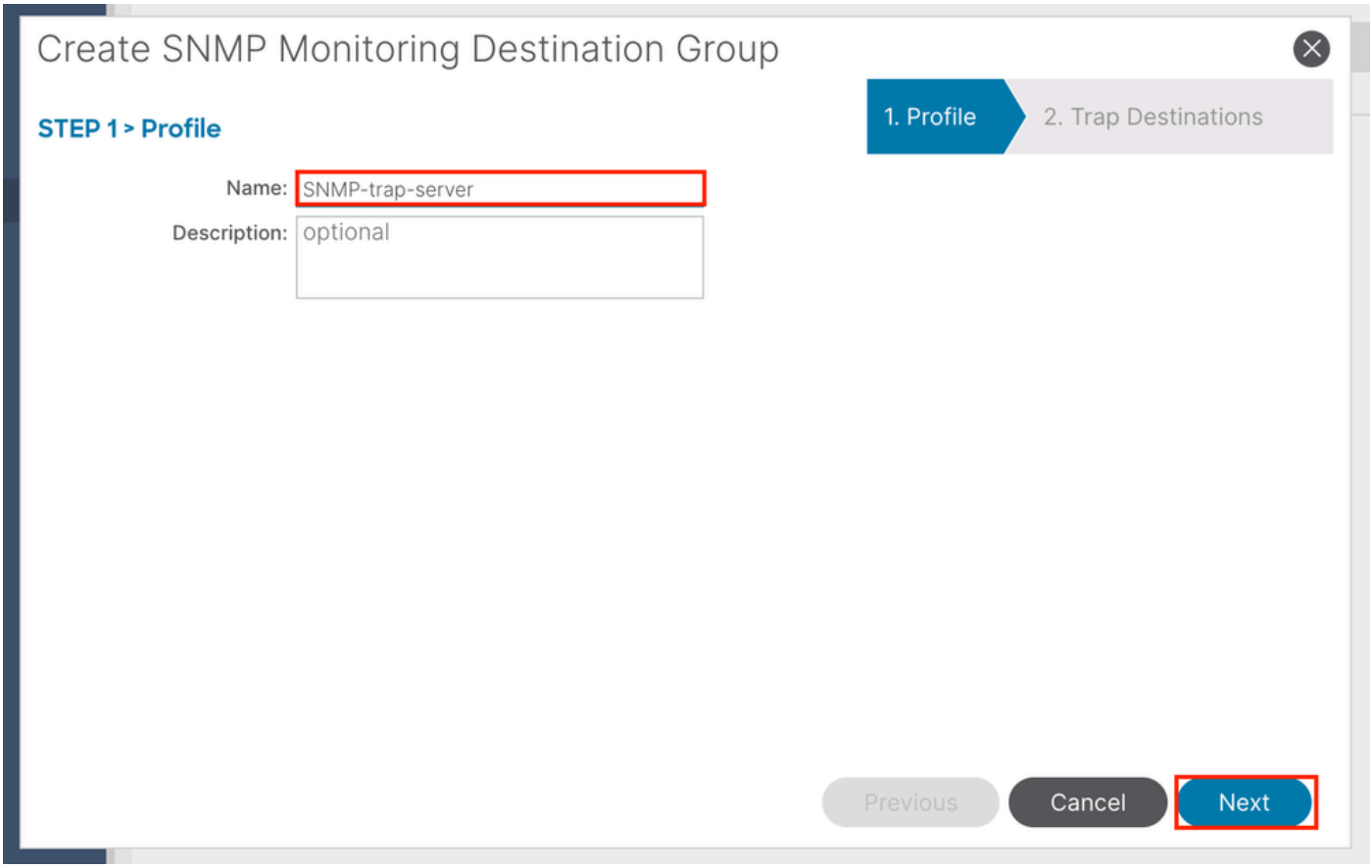
Nota: Sin los pasos 1-3 de la sección anterior, la configuración de SNMP TRAPs no es suficiente. Paso 2. en SNMP TRAP configuration está relacionado con las políticas de monitoreo para (acceso/estructura/arrendatario).

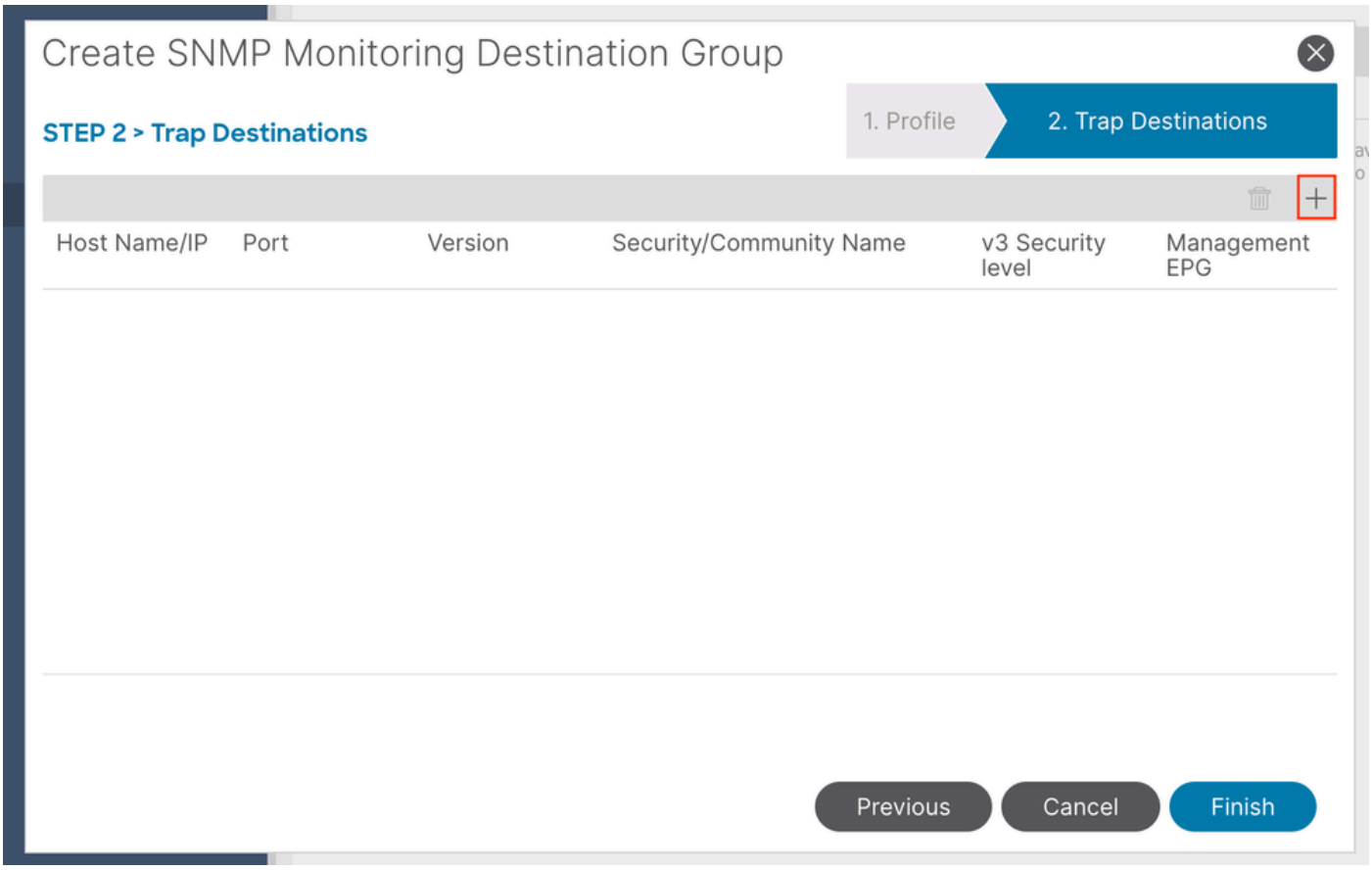
Para configurar las TRAMPAS SNMP en ACI, necesita los dos pasos además de los pasos 1, 2 y 3 de la sección anterior.

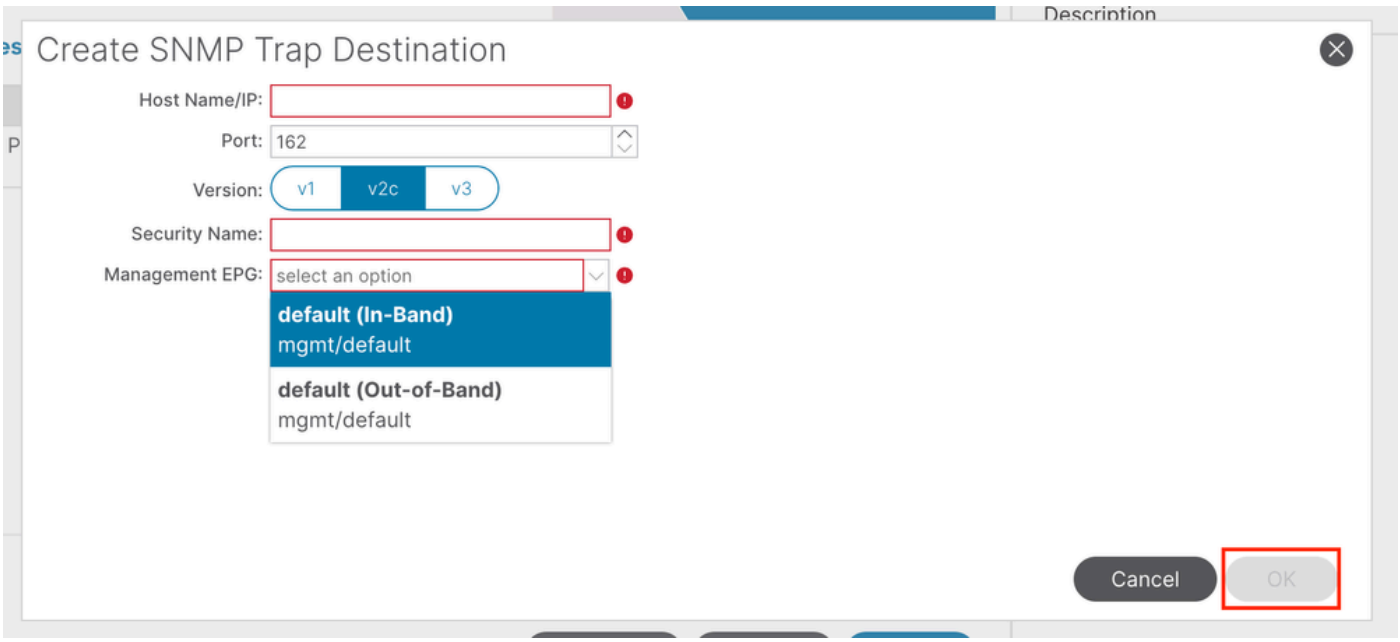
Paso 1. Configurar el servidor SNMP TRAP

Para hacerlo, navegue a la ruta de la GUI web de APIC; Admin > Eternal Data Collectors > Monitoring Destinations > SNMP.









Nombre de host/IP: el host para el destino de la trampa SNMP.

Puerto: el puerto de servicio del destino de trampa SNMP. El intervalo es de 0 (sin especificar) a 65535; el valor predeterminado es 162.

Versión: la versión CDP soportada para el destino de trampa SNMP. La versión puede ser:

-

v1: utiliza una coincidencia de cadena de comunidad para la autenticación de usuario.

- v2c: utiliza una coincidencia de cadena de comunidad para la autenticación de usuario.

- v3 - un protocolo interoperable basado en estándares para la administración de redes que proporciona acceso seguro a los dispositivos mediante una combinación de tramas de autenticación y cifrado a través de la red.

El valor predeterminado es **v2c**.

Security Name (Nombre de seguridad): el nombre de seguridad de destino de captura SNMP (nombre de comunidad). No puede contener el símbolo **@**.

v.3 Security Level (Nivel de seguridad): el nivel de seguridad SNMPv3 para la ruta de destino SNMP. El nivel puede ser:

- autenticación

- noauth

- priv

El valor predeterminado es noauth.

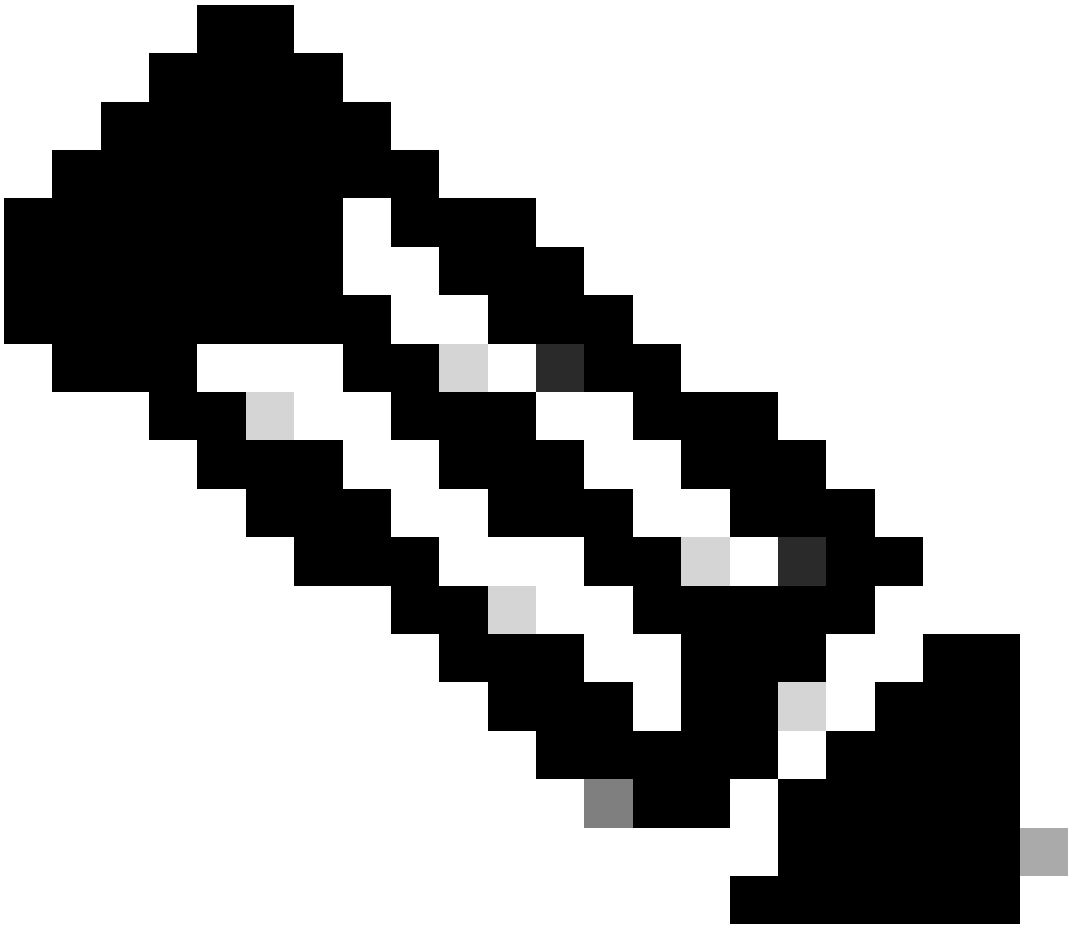
EPG de administración: el nombre del grupo de terminales de administración para el destino SNMP a través del cual se puede alcanzar el host remoto.

Paso 2. Configure el origen de SNMP TRAP en la política de supervisión (acceso/fabric/arrendatario)

Puede crear directivas de supervisión con tres ámbitos:

- Acceso: puertos de acceso, FEX, controladores de VM
- Fabric: puertos de fabric, tarjetas, chasis, ventiladores

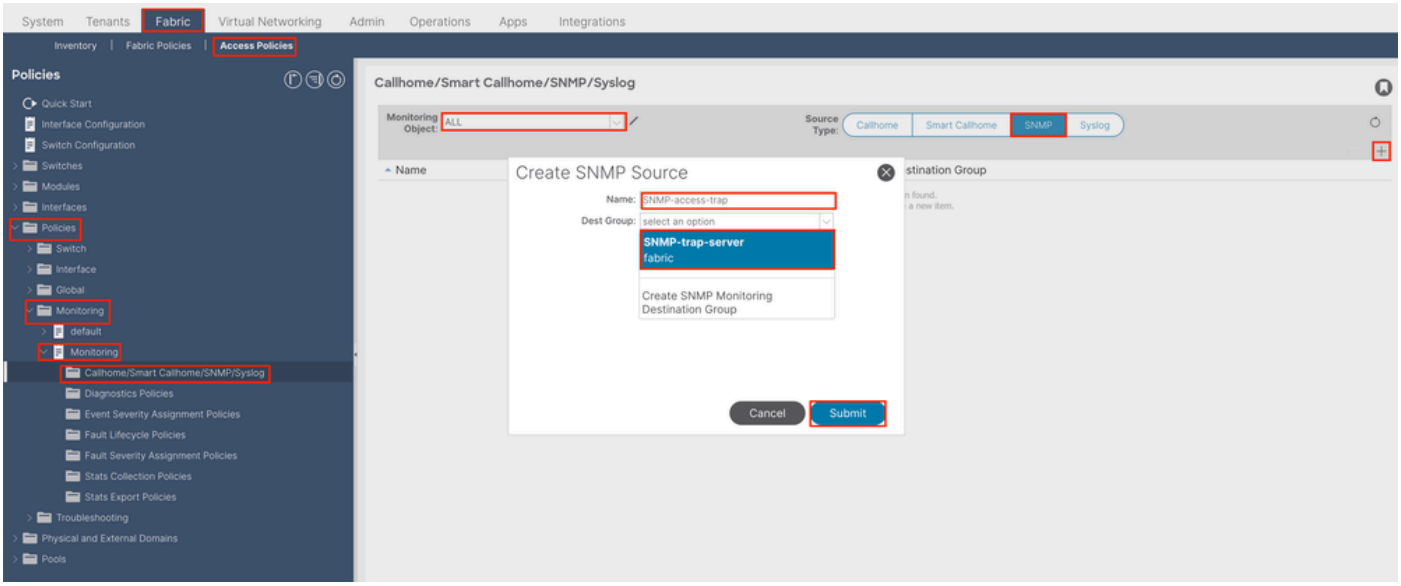
- Arrendatario: EPG, perfiles de aplicación y servicios

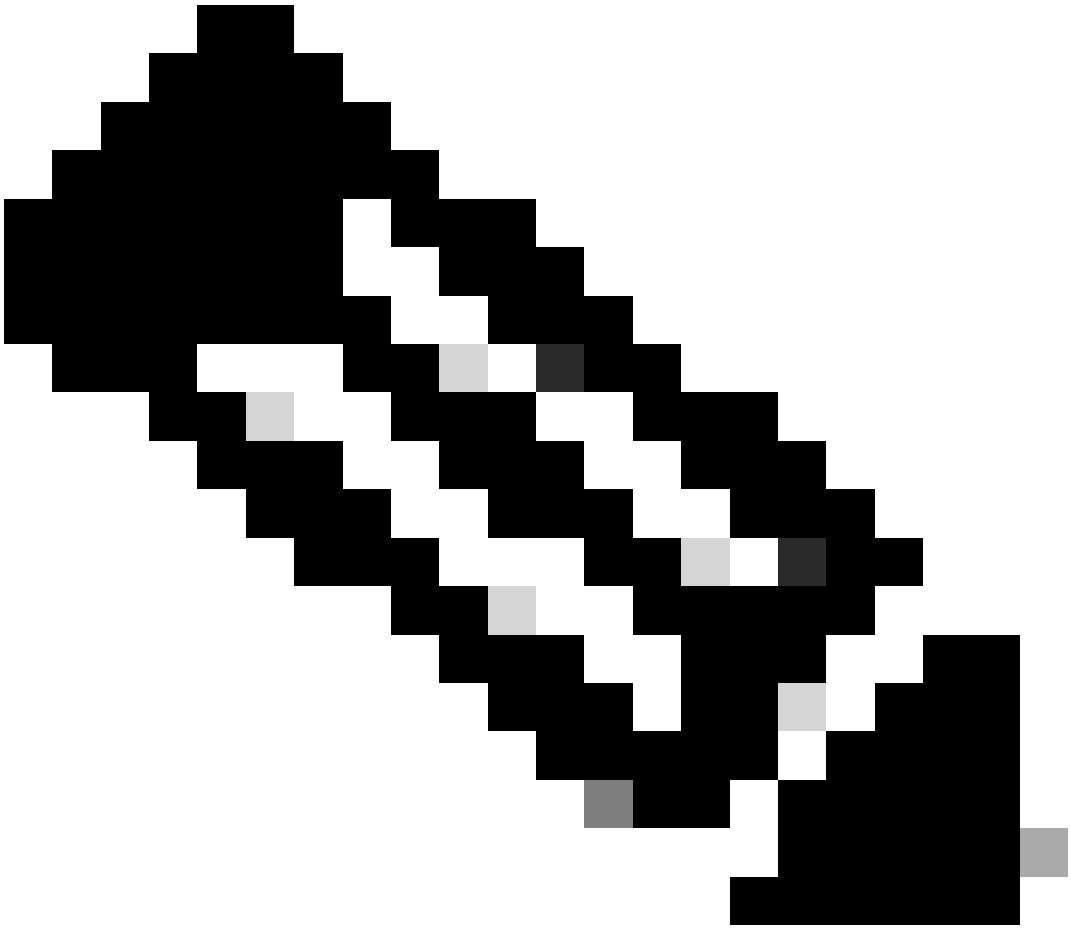


Nota: Puede elegir cualquiera de ellos o cualquier combinación de ellos con el fin de configurar de acuerdo con sus necesidades.

Opción 1. Defina el origen SNMP en Políticas de acceso

Para hacerlo, navegue a la ruta de la GUI web de APIC; Fabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

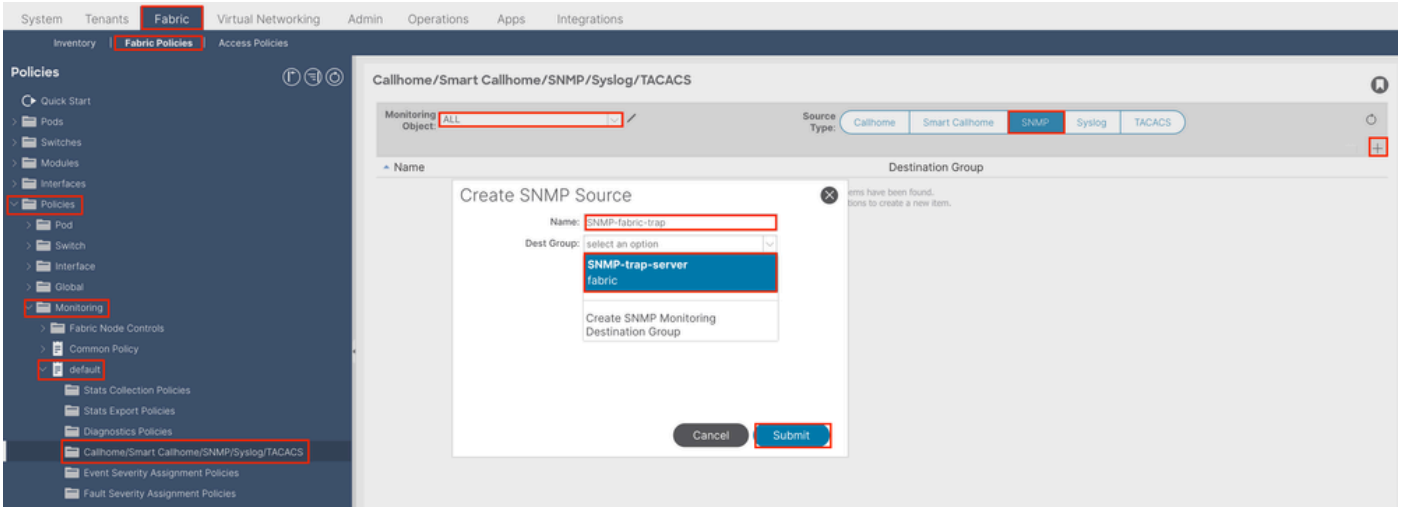

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog
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



Nota: Puede utilizar una política de supervisión definida personalizada (si está configurada) en lugar de la predeterminada. Utilice la predeterminada aquí. Puede especificar qué objeto de supervisión desea supervisar; aquí se utilizaron todos.

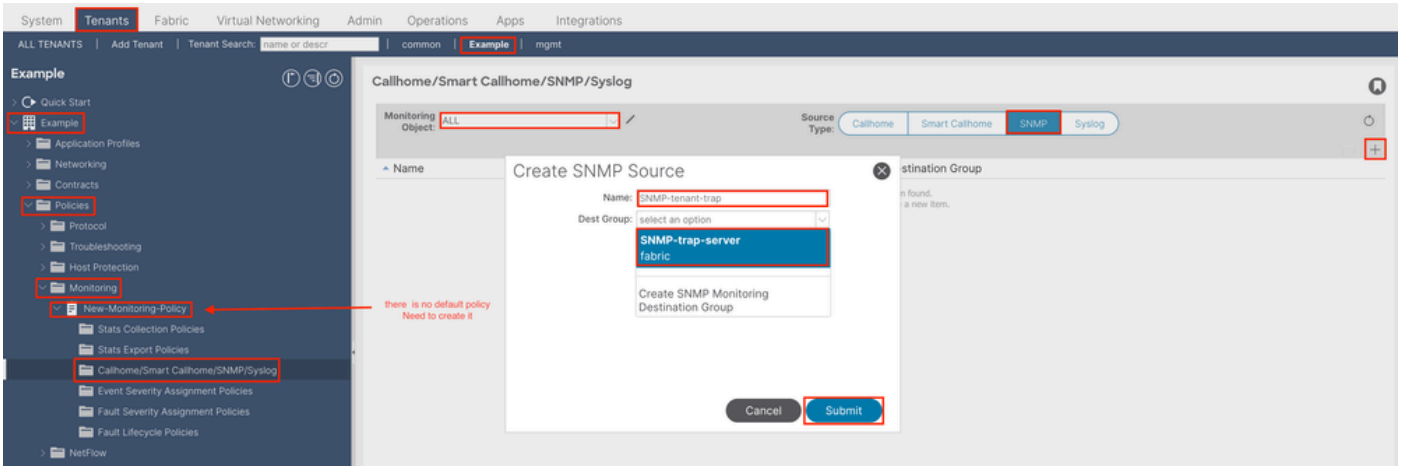
Opción 2. Defina el origen SNMP en las políticas de fabric

Para hacerlo, navegue a la ruta de la GUI web de APIC; Fabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Opción 3. Defina el origen SNMP en Políticas de arrendatario

Para hacerlo, navegue a la ruta de la GUI web de APIC; Tenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Verificación

Utilice el comando snmpwalk para verificar

En primer lugar, observe cómo extraer datos SNMP del ámbito global de un switch de hoja. El uso del comando snmpwalk puede hacer

precisamente eso; snmpwalk -v 2c -c New-1 x.x.x.x.

Este comando desglosado representa:

snmpwalk = El ejecutable snmpwalk instalado en MacOS/Linux/Windows

-v = Especifica la versión de SNMP que desea utilizar

2c= Especifica que se está utilizando SNMP versión 2c

-c= Especifica que una cadena de comunidad determinada

New-1= La cadena de comunidad se utiliza para extraer datos SNMP de ámbito global

x.x.x.x= Dirección IP de administración fuera de banda de mi switch de hoja

Resultado del comando:

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

En el resultado del comando snipped, puede ver que snmpwalk es exitoso y que se extrajo información específica del hardware. Si deja que el snmpwalk continúe, verá los nombres de la interfaz de hardware, las descripciones, etc.

Ahora, proceda a recuperar los datos SNMP del Contexto VRF, los contextos SNMP creados anteriormente, **New-VRF-SNMP** para los VRFs que utilizan la cadena de comunidad SNMP, **New-1**.

Dado que se utiliza la misma cadena de comunidad, **New-1**, en dos contextos SNMP diferentes, debe especificar de qué contexto SNMP desea extraer los datos SNMP. Existe la sintaxis snmpwalk que necesita utilizar para especificar un contexto SNMP determinado; snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.

Puede ver que para extraer de un contexto SNMP específico, utiliza el formato:
COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

Uso de los comandos Show de CLI

En APIC:

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

En el switch:

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

Uso de comandos Moquery de CLI

En APIC/Switch:

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

Uso de comandos cat de CLI

En APIC:

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

Troubleshoot

Verifique el proceso snmpd

En el switch:

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

En APIC:

```
ps aux | grep snmp
```

Si el proceso es normal, póngase en contacto con el TAC de Cisco para obtener más ayuda.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).