Configurazione di SNMP in ACI

Sommario

Introduzione

Questo documento descrive la configurazione di Simple Network Management Protocol (SNMP) e trap SNMP in ACI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Individuazione fabric completata
- Connettività In-Band/Out-of-Band a Application Policy Infrastructure Controller (APIC) e switch fabric

- Contratti in-band/out-of-band configurati per consentire il traffico SNMP (porte UDP 161 e 162)
- Indirizzi di gestione dei nodi statici configurati per gli switch APIC e fabric nel tenant di gestione predefinito (senza questo, il pulling delle informazioni SNMP da un APIC non riesce)
- Comprendere il flusso di lavoro del protocollo SNMP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- APIC
- Browser
- ACI (Application Centric Infrastructure) con versione 5.2 (8e)
- Snmpwalk comando

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Cisco ACI fornisce il supporto per SNMPv1, v2c e v3, inclusi i MIB (Management Information Base) e le notifiche (trap). Lo standard SNMP consente a tutte le applicazioni di terze parti che supportano i diversi MIB di gestire e monitorare gli switch ACI Leaf & Spine e i controller APIC.

Tuttavia, i comandi di scrittura SNMP (Set) non sono supportati in ACI.

Il criterio SNMP viene applicato ed eseguito in modo indipendente sugli switch foglia e dorso e sui controller APIC. Poiché ciascun dispositivo ACI dispone di una propria entità SNMP, è necessario monitorare separatamente più dispositivi APIC in un cluster APIC e gli switch. Tuttavia, l'origine dei criteri SNMP viene creata come criterio di controllo per l'intera struttura ACI.

Per impostazione predefinita, il protocollo SNMP utilizza la porta **UDP 161** per il polling e la porta **162** per i TRAP.

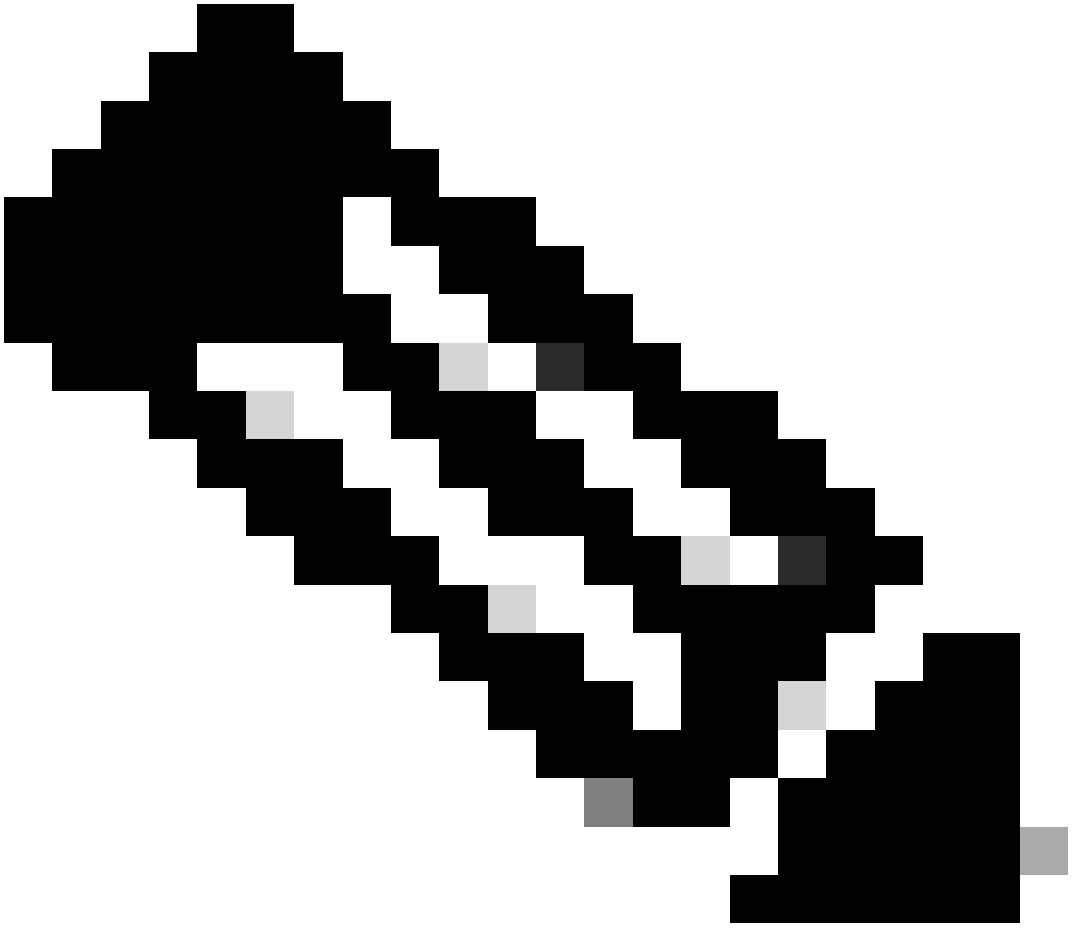
Informazioni sugli ambiti SNMP

Un concetto fondamentale e rapido di SNMP in ACI è che ci sono due ambiti da cui è possibile estrarre le informazioni SNMP:
1. Globale
2. Contesto VRF (Virtual Routing and Forwarding)

L'**ambito globale** consiste nel prelevare MIB dello chassis, quali il numero di interfacce, gli indici di interfaccia, i nomi di interfaccia, lo stato dell'interfaccia e così via, da un nodo foglia/dorso.

Contesto VRF I MIB specifici dell'**ambito** estraggono informazioni specifiche del VRF, ad esempio indirizzi IP e informazioni sul protocollo di routing.

Nell'elenco dei servizi di supporto MIB di Cisco ACI è disponibile un elenco completo dei MIB globali e dei MIB di contesto VRF supportati dagli switch fabric e APIC.

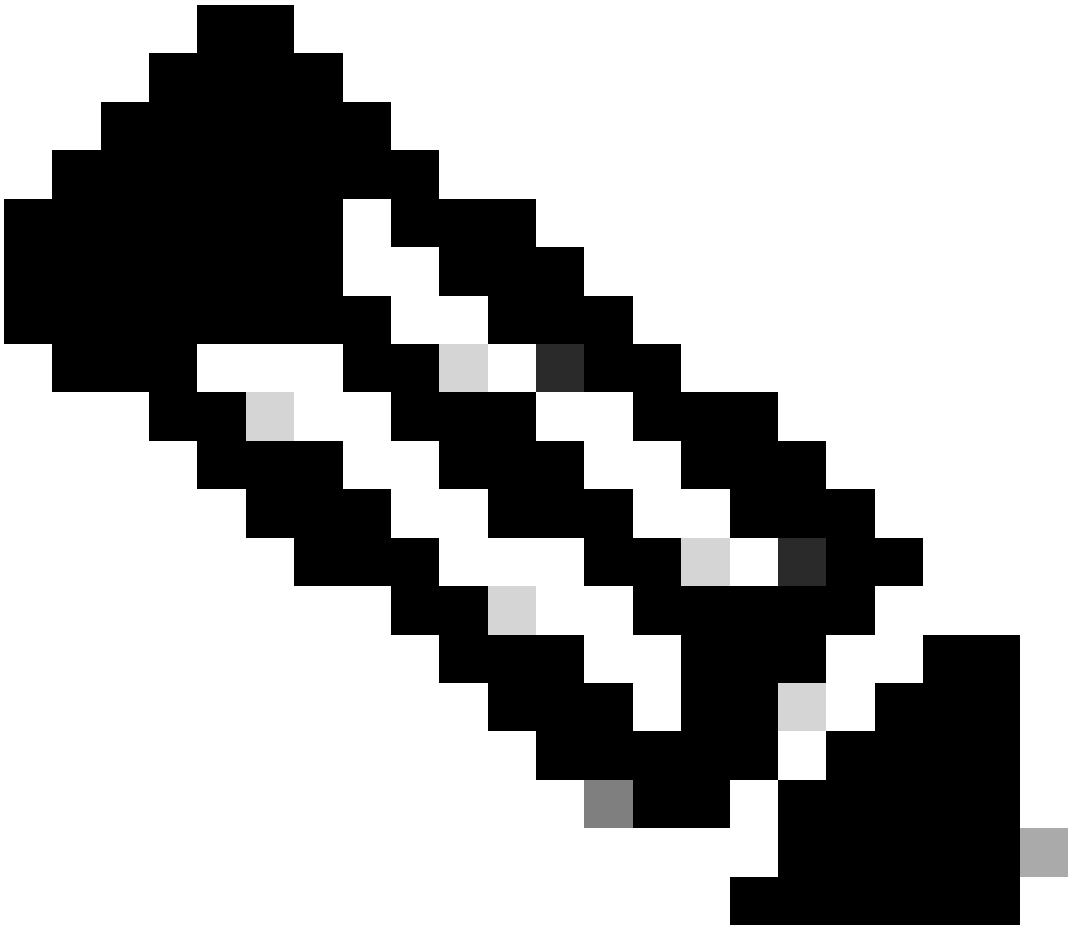


Nota: un MIB con ambito Globale dispone di una sola istanza nel sistema. I dati di un MIB globale si riferiscono all'intero sistema.

Un MIB con ambito specifico VRF può avere istanze per VRF nel sistema. I dati in un MIB specifico del VRF si riferiscono solo a tale VRF.

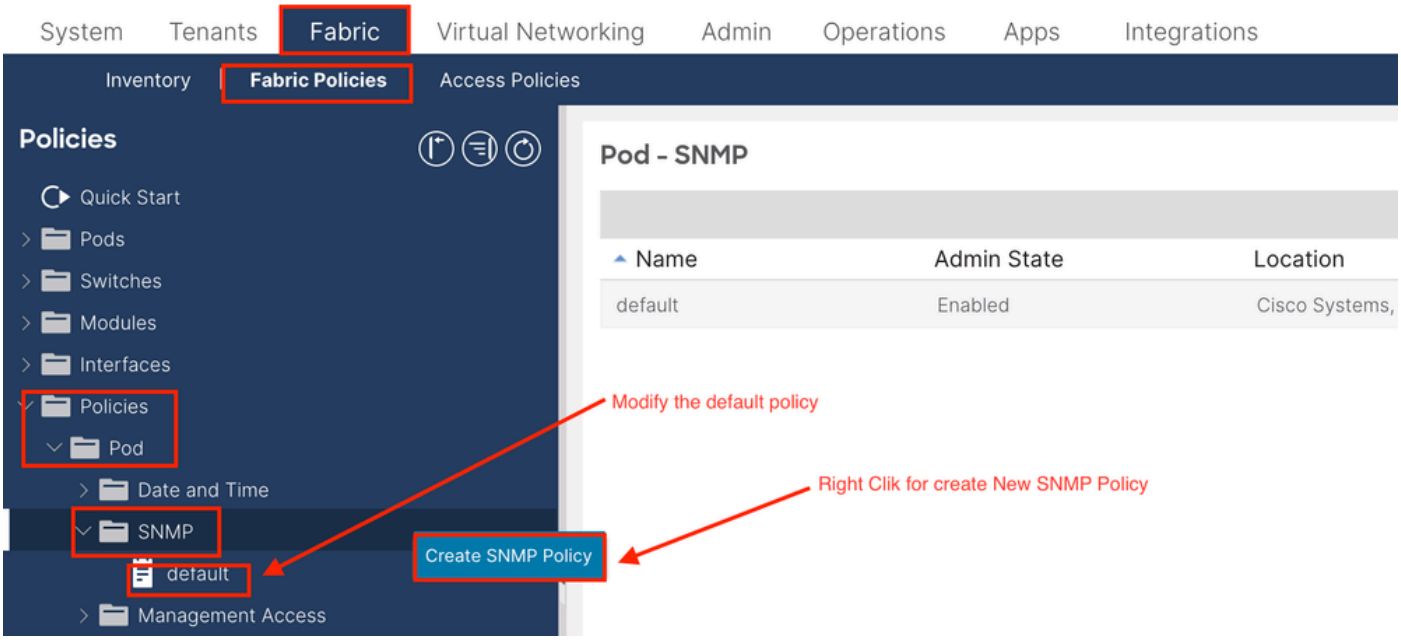
Fasi di configurazione (per entrambi gli ambiti di contesto globale e VRF)

Passaggio 1. Configura criterio infrastruttura SNMP



Nota: qui vengono specificate le impostazioni SNMP, ad esempio i criteri della community SNMP e i criteri dei gruppi di client SNMP.

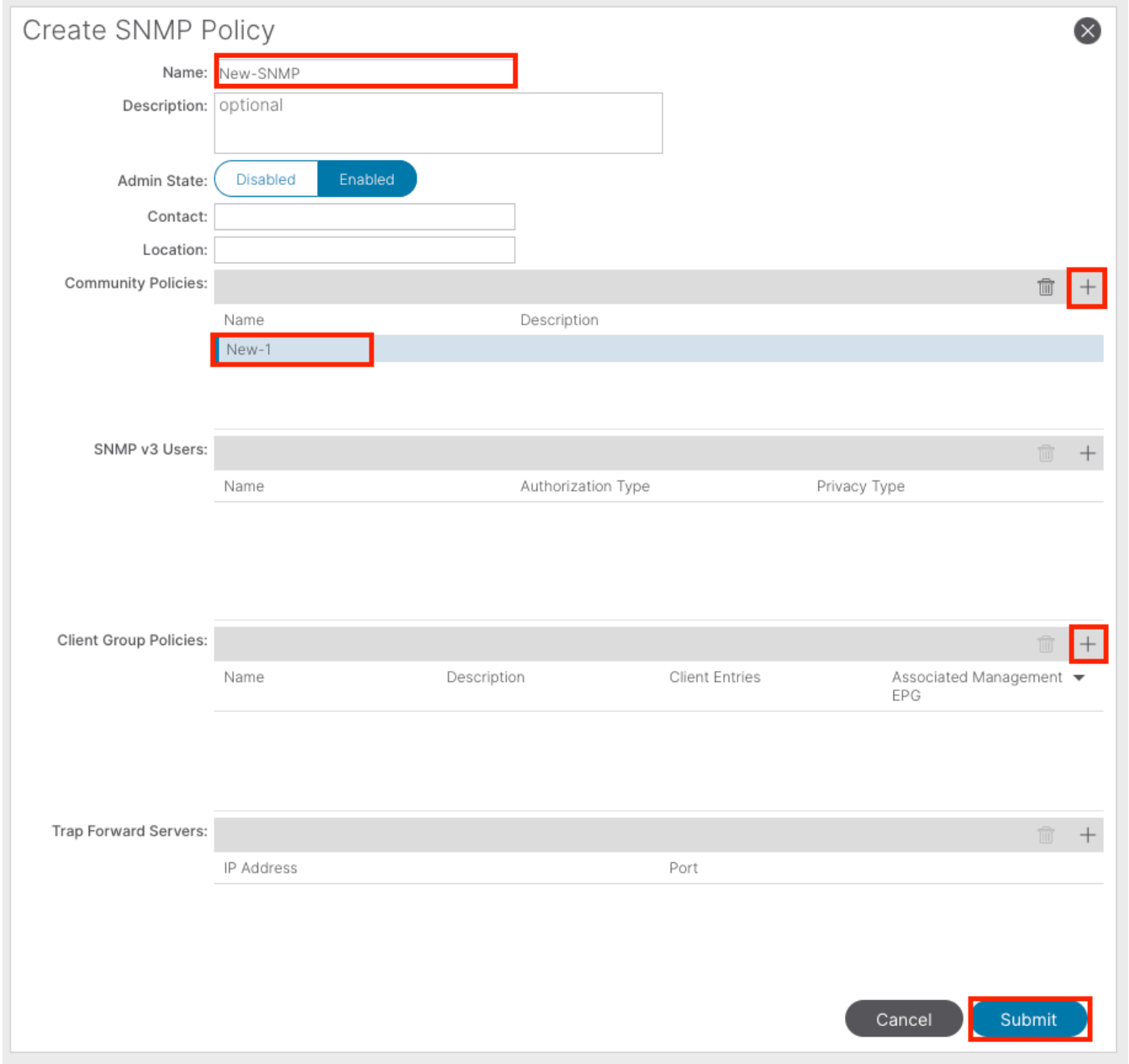
Il primo passaggio nella configurazione del protocollo SNMP consiste nella creazione dei criteri di infrastruttura SNMP necessari. Per creare le policy di fabric SNMP, accedere al percorso dell'interfaccia grafica Web di APICFabric > Fabric Policies > Policies > Pod > SNMP.



È possibile creare un nuovo criterio SNMP o modificare quello predefinito.

Nel documento, i criteri SNMP sono denominati **New-SNMP** e utilizzano la versione SNMP v2c, pertanto gli unici campi necessari a questo scopo sono i criteri della community e i criteri del gruppo client.

Il campo Nome criterio comunitario definisce la stringa della community SNMP da utilizzare. Nel nostro caso, **New-1**. Vedete dove queste due stringhe della comunità arrivano più tardi.



Nome: il nome del criterio SNMP. Il nome può contenere da 1 a 64 caratteri alfanumerici.

Descrizione: descrizione del criterio SNMP. La descrizione può contenere da 0 a 128 caratteri alfanumerici.

Stato amministrazione: lo stato amministrativo del criterio SNMP. Lo stato può essere abilitato o disabilitato. Gli stati sono:

- enabled - lo stato admin è enabled
- disabled - lo stato admin è disabled

L'impostazione predefinita è **disattivata**.

Contatto: le informazioni di contatto per il criterio SNMP.

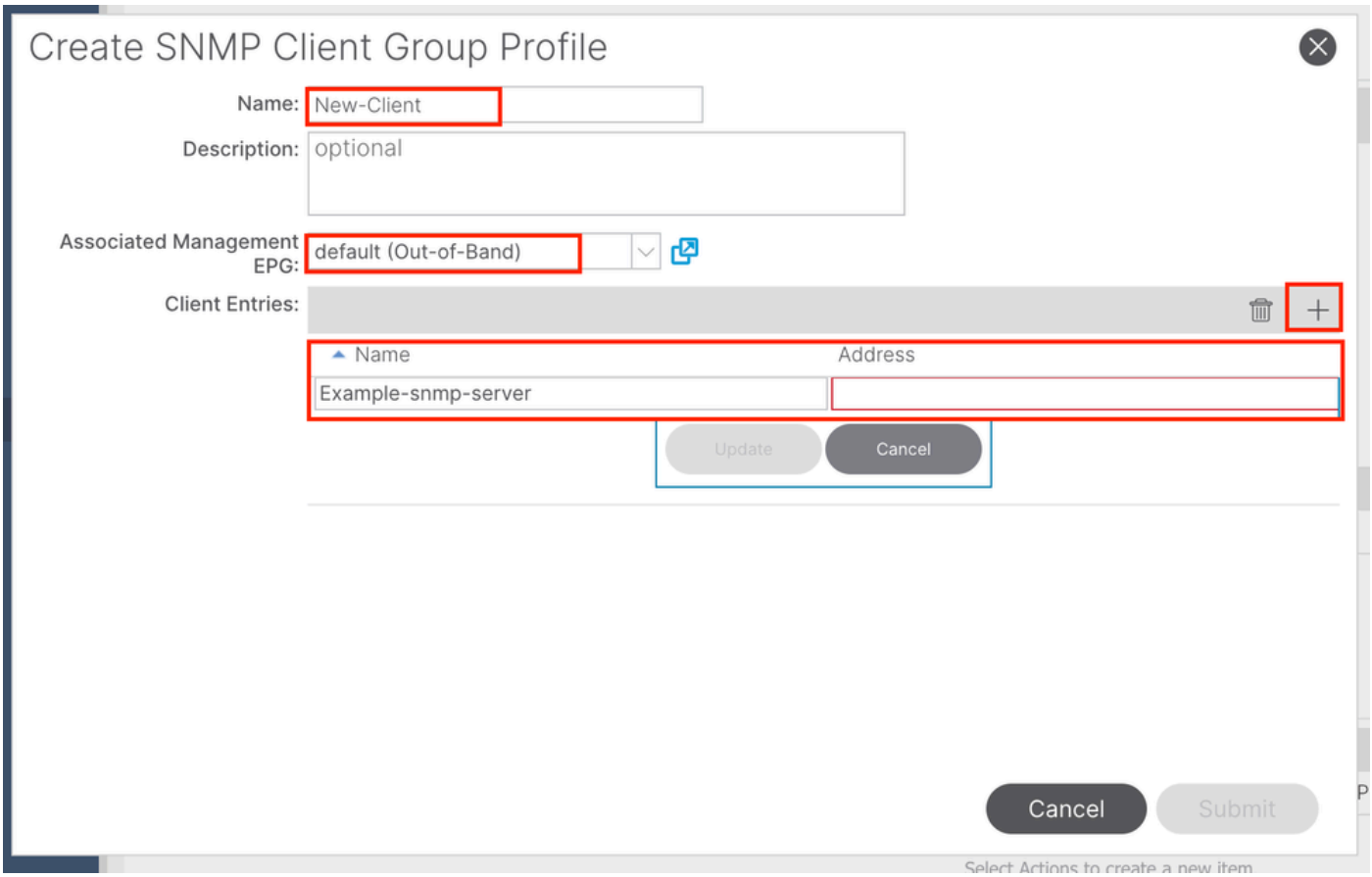
Percorso: il percorso del criterio SNMP.

Utenti SNMP v3 - il profilo utente SNMP viene utilizzato per associare gli utenti alle policy SNMP per il monitoraggio dei dispositivi in una rete.

Policy comunitarie - il profilo della community SNMP consente di accedere alle statistiche del router o dello switch per il monitoraggio.

Criteri di gruppo client:

Il passaggio successivo consiste nell'aggiungere il profilo o i Criteri di gruppo del client. Lo scopo di Criteri di gruppo/Profilo client è quello di definire quali IP/subnet sono in grado di prelevare i dati SNMP da APIC e switch fabric:



Nome: il nome del profilo del gruppo client. Il nome può contenere da 1 a 64 caratteri alfanumerici.

Descrizione: la descrizione del profilo del gruppo di client. La descrizione può contenere da 0 a 128 caratteri alfanumerici.

Gruppo endpoint di gestione associato (EPG, Associated Management End Point Group): il nome distinto di un gruppo di endpoint attraverso il quale è possibile accedere al VRF. La lunghezza massima supportata per le stringhe è di 255 caratteri ASCII. Il valore predefinito è l'accesso di gestione fuori banda EPG del tenant di gestione.

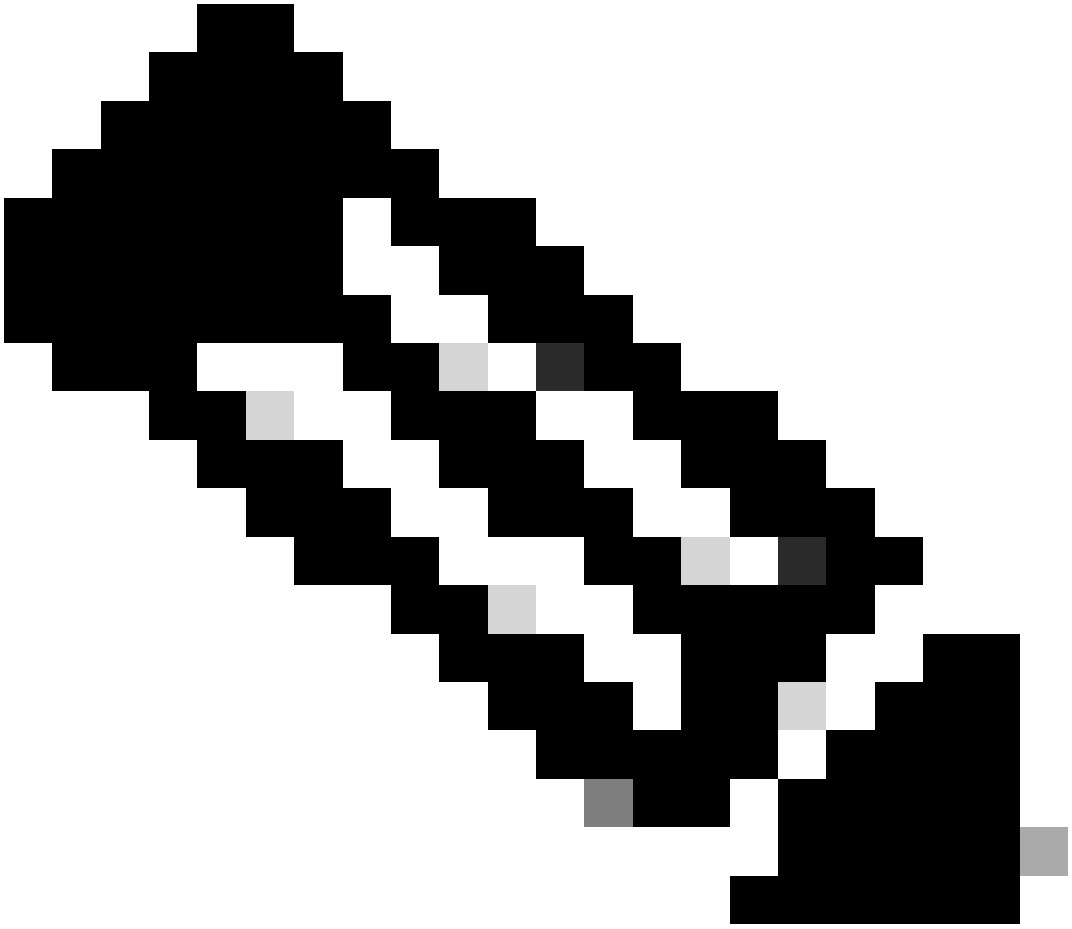
Voci client: indirizzo IP del profilo client SNMP.

Nel documento, Criteri di gruppo/Profilo client è denominato **New-Client**.

In Criteri di gruppo/Profilo client è necessario associare l'EPG di gestione preferito. È necessario assicurarsi che il Management EPG scelto disponga dei contratti necessari per consentire il traffico SNMP (porte UDP 161 e 162). A scopo dimostrativo, nel documento viene utilizzata la gestione fuori banda predefinita EPG.

L'ultimo passaggio consiste nel definire le **voci client** in modo da consentire a IP specifici o a intere subnet di accedere ai dati ACI SNMP. È disponibile una sintassi per definire un indirizzo IP specifico o un'intera subnet:

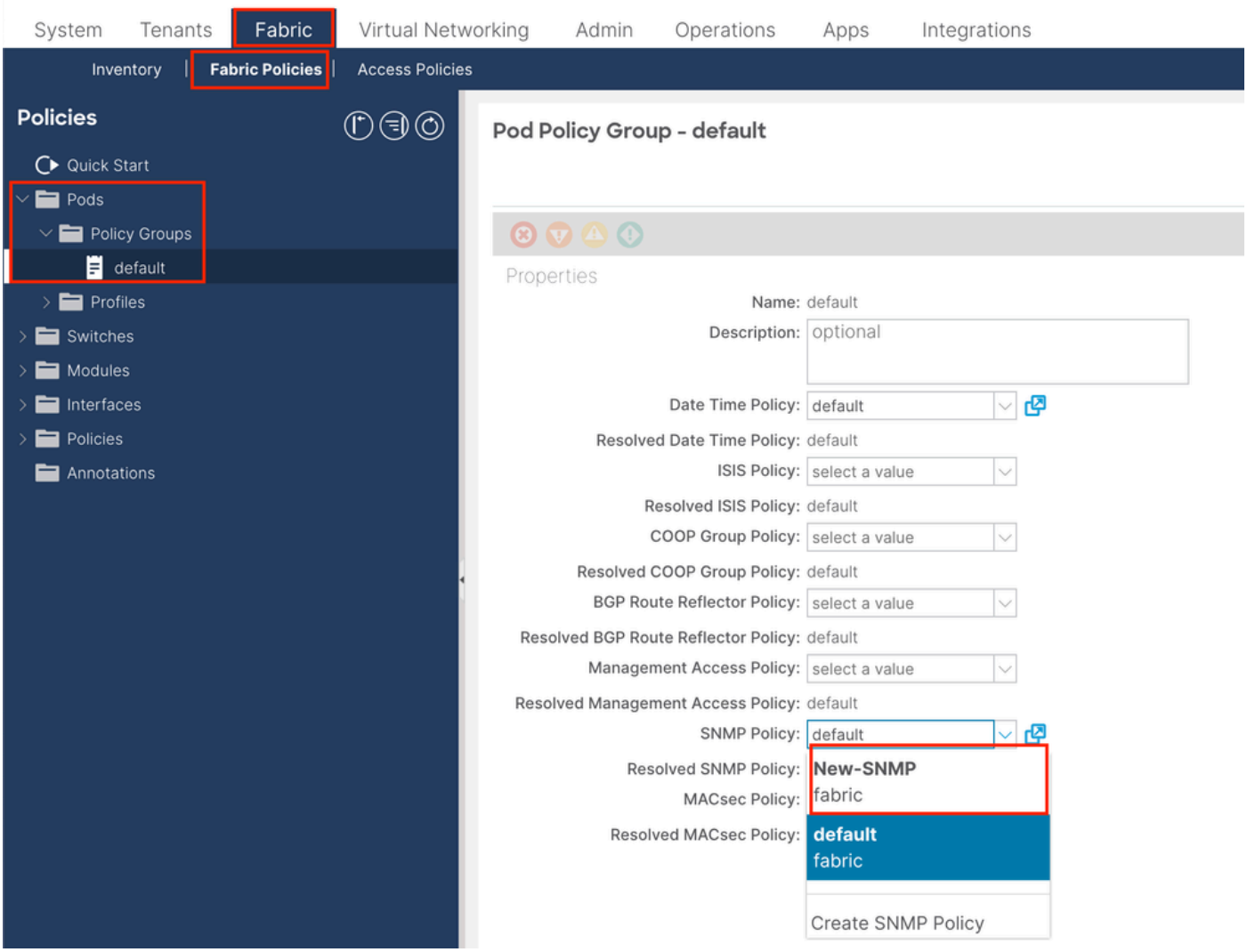
- IP host specifico: 192.168.1.5
- Intera subnet: 192.168.1.0/24



Nota: non è possibile utilizzare 0.0.0.0 nella voce client per consentire a tutte le subnet (se si desidera consentire a tutte le subnet di accedere a MIB SNMP, lasciare vuote le voci client).

Passaggio 2. Applica criterio SNMP al gruppo di criteri POD (gruppo di criteri fabric)

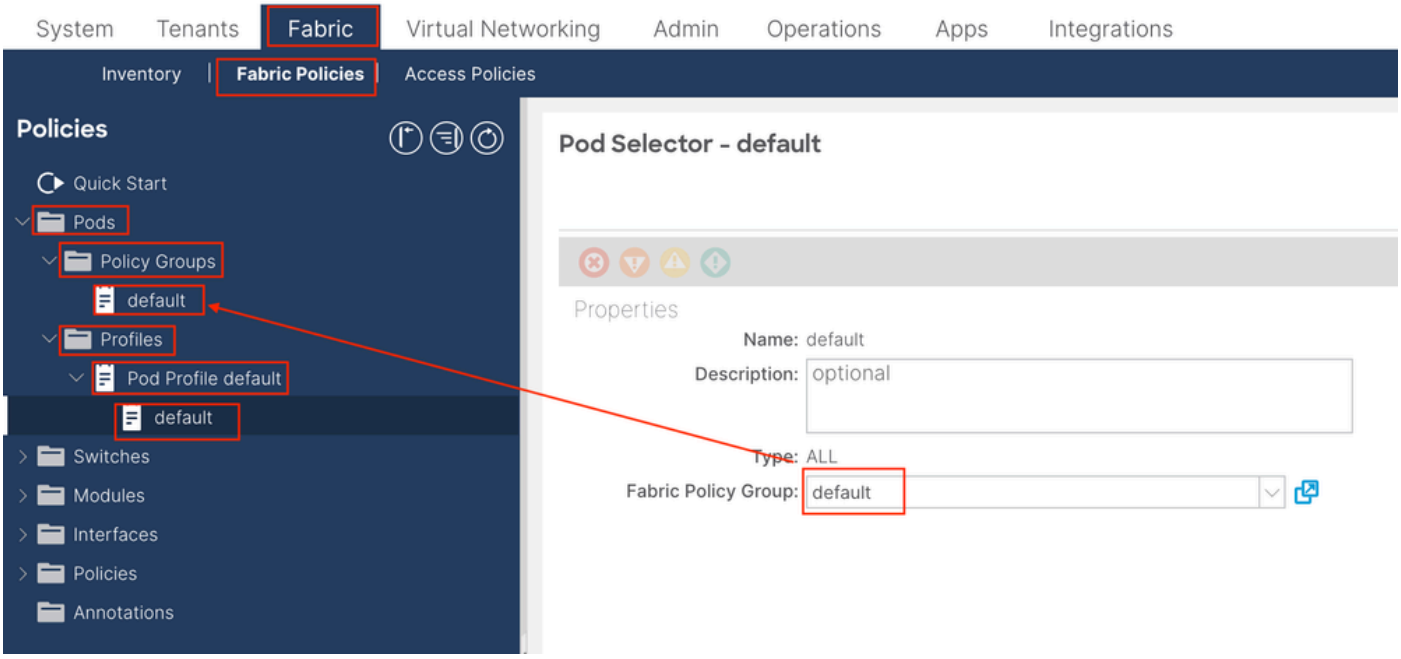
Per applicare questa configurazione, selezionare il percorso dell'interfaccia utente grafica Web APIC;Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP (impostazione predefinita nel documento).



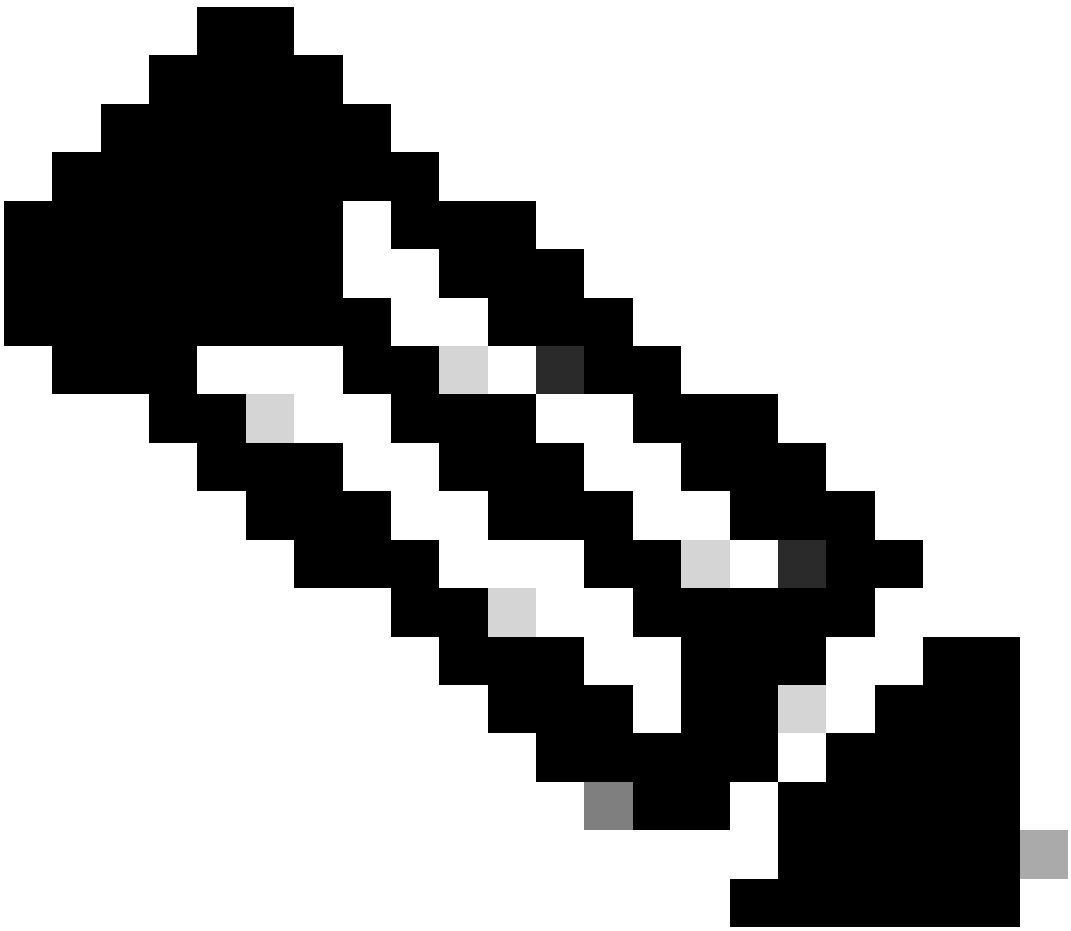
Nel riquadro a destra è presente un campo per i criteri SNMP. Dall'elenco a discesa, scegliere il criterio SNMP appena creato e inviare le modifiche.

Passaggio 3. Associare il gruppo di criteri POD al profilo del POD

Nel documento, usate il profilo predefinito del baccello per semplificare l'operazione. A tale scopo, selezionare il percorso dell'interfaccia utente grafica per il Web di APIC;Fabric > Fabric Policies > Pods > Profiles > POD_PROFILE (impostazione predefinita nel documento).



In questa fase, configurare il protocollo SNMP di base per i MIB globali.

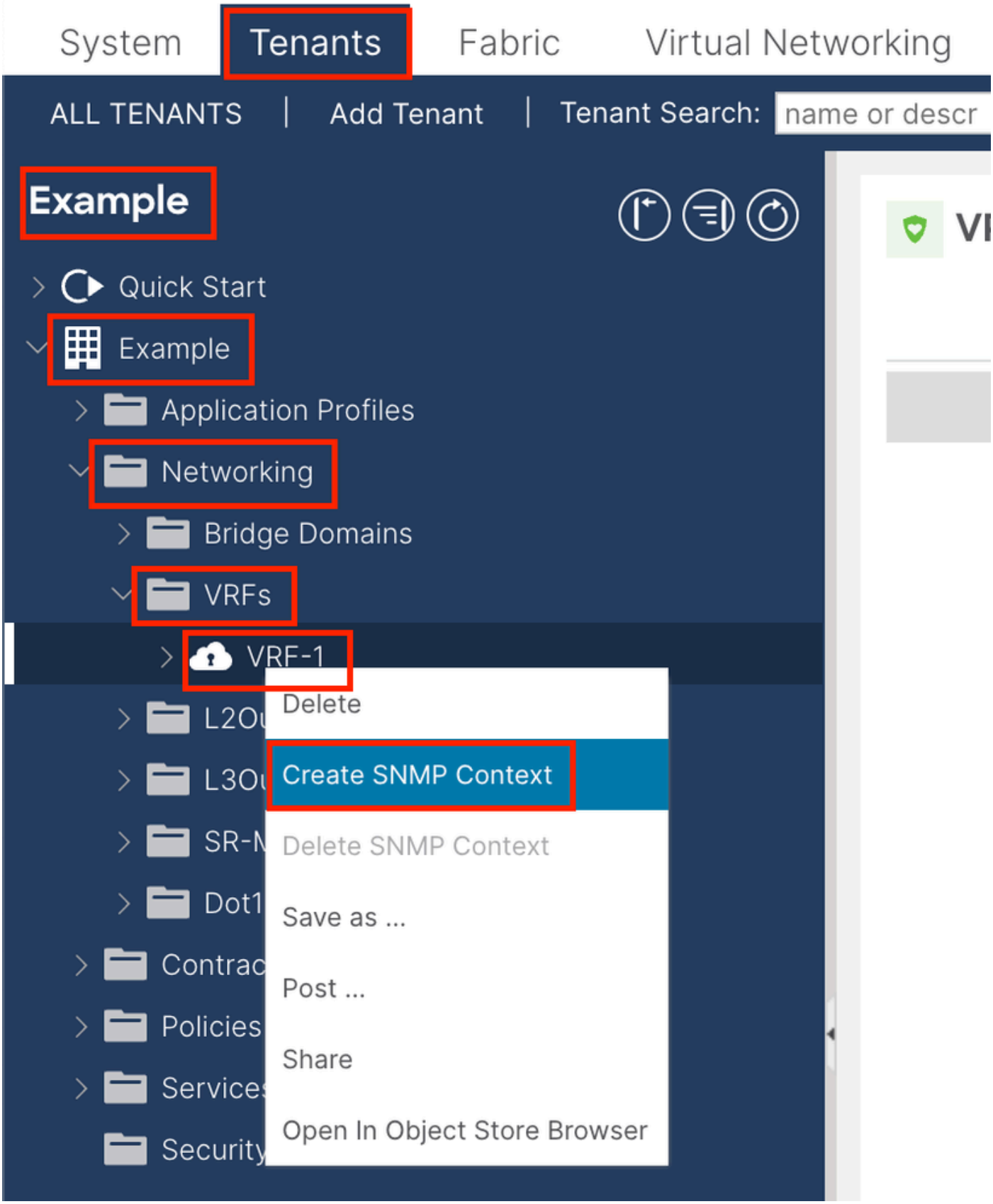


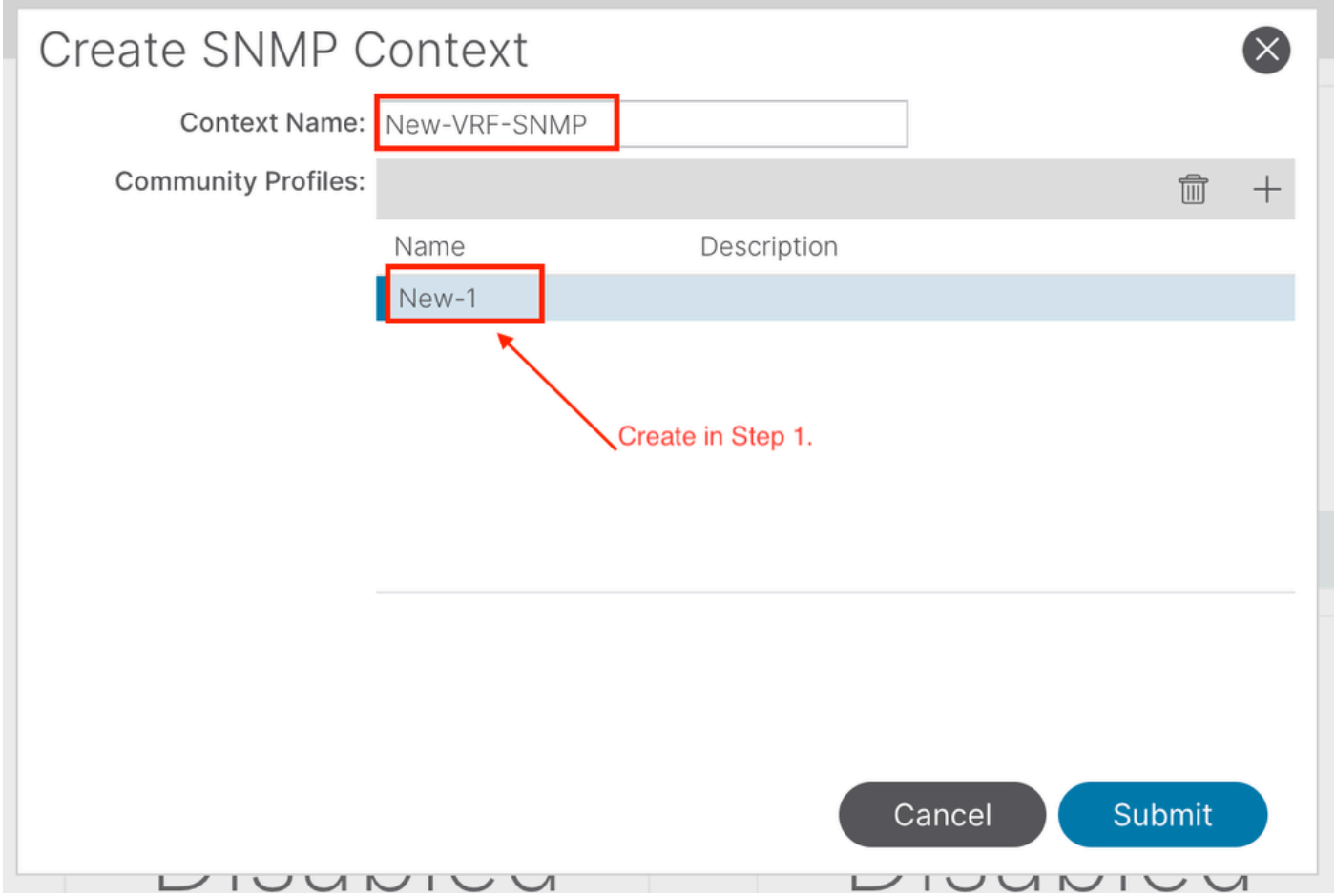
Nota: a questo punto, tutti i passaggi necessari (passaggi 1-3) per la configurazione SNMP sono stati completati e l'ambito MIB globale è stato utilizzato in modo implicito. In questo modo, è possibile eseguire una procedura SNMP per qualsiasi nodo ACI o APIC.

Passaggio 4. Configurazione degli ambiti di contesto VRF

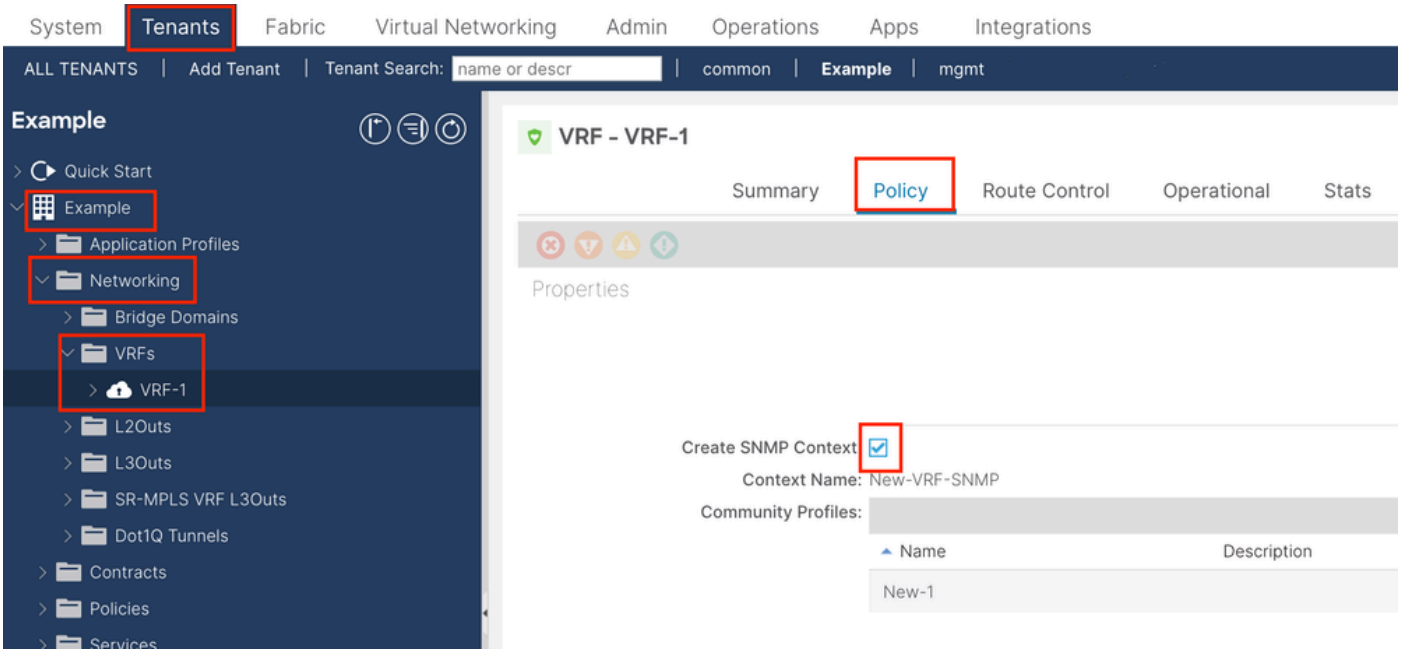
Dopo aver associato una stringa della community a un contesto VRF, tale stringa della community specifica non può essere utilizzata per eseguire il pull dei dati SNMP dell'ambito globale. Pertanto, è necessario creare due stringhe della community SNMP se si desidera estrarre sia i dati SNMP dell'ambito globale che quelli del contesto VRF.

In questo caso, le stringhe della community create in precedenza (nel passaggio 1.), ovvero (**New-1**), utilizzano **New-1** per l'ambito del contesto VRF e **VRF-1** personalizzato nel tenant **esempio** personalizzato. A tale scopo, selezionare il percorso dell'interfaccia utente grafica del Web APICTenants > 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



Dopo aver inviato la configurazione, è possibile verificare la configurazione del contesto SNMP applicata facendo clic con il pulsante sinistro del mouse sul VRF, passando alla scheda Criteri del VRF e scorrendo verso il basso il riquadro:

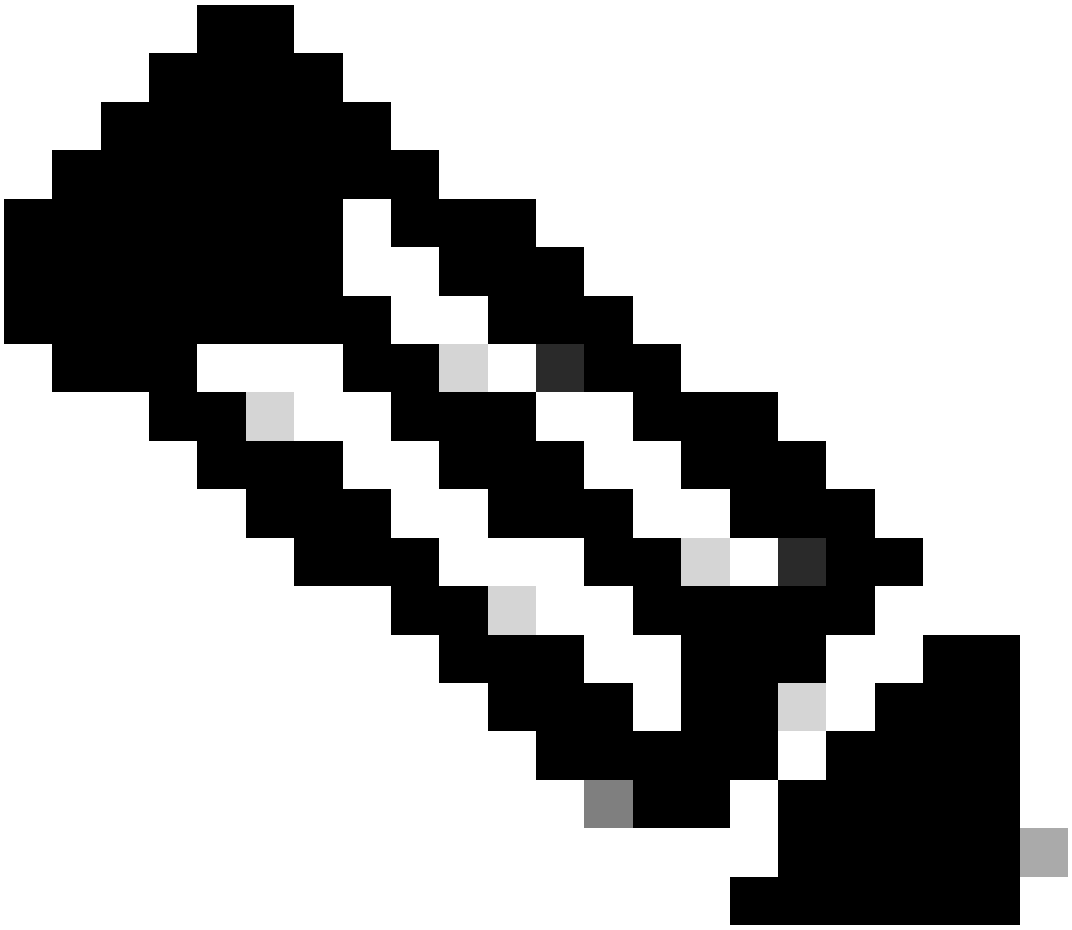


Per disabilitare un contesto SNMP su un VRF, è possibile deselezionare la casella di controllo **Crea contesto SNMP** (visualizzata nella schermata), oppure fare clic con il pulsante destro del mouse sul VRF e scegliere **Elimina contesto SNMP**.

Configurazione di TRAP SNMP tramite GUI

Le TRAP SNMP vengono inviate al server SNMP (SNMP Destination/Network Management Systems (NMS)) senza polling, mentre il nodo ACI/APIC invia la TRAP SNMP una volta che si verifica l'errore/l'evento (condizione definita).

Le trap SNMP sono abilitate in base all'ambito dei criteri in criteri di monitoraggio accesso/fabric/tenant. ACI supporta un massimo di 10 ricevitori Trap.

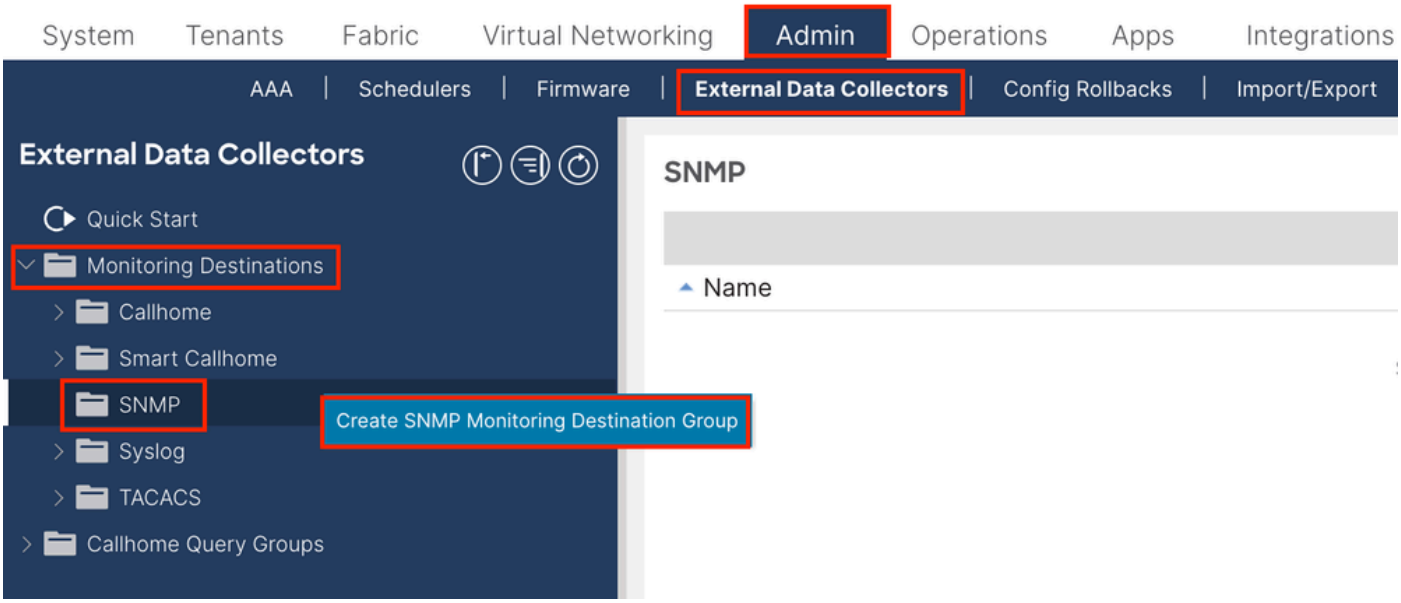


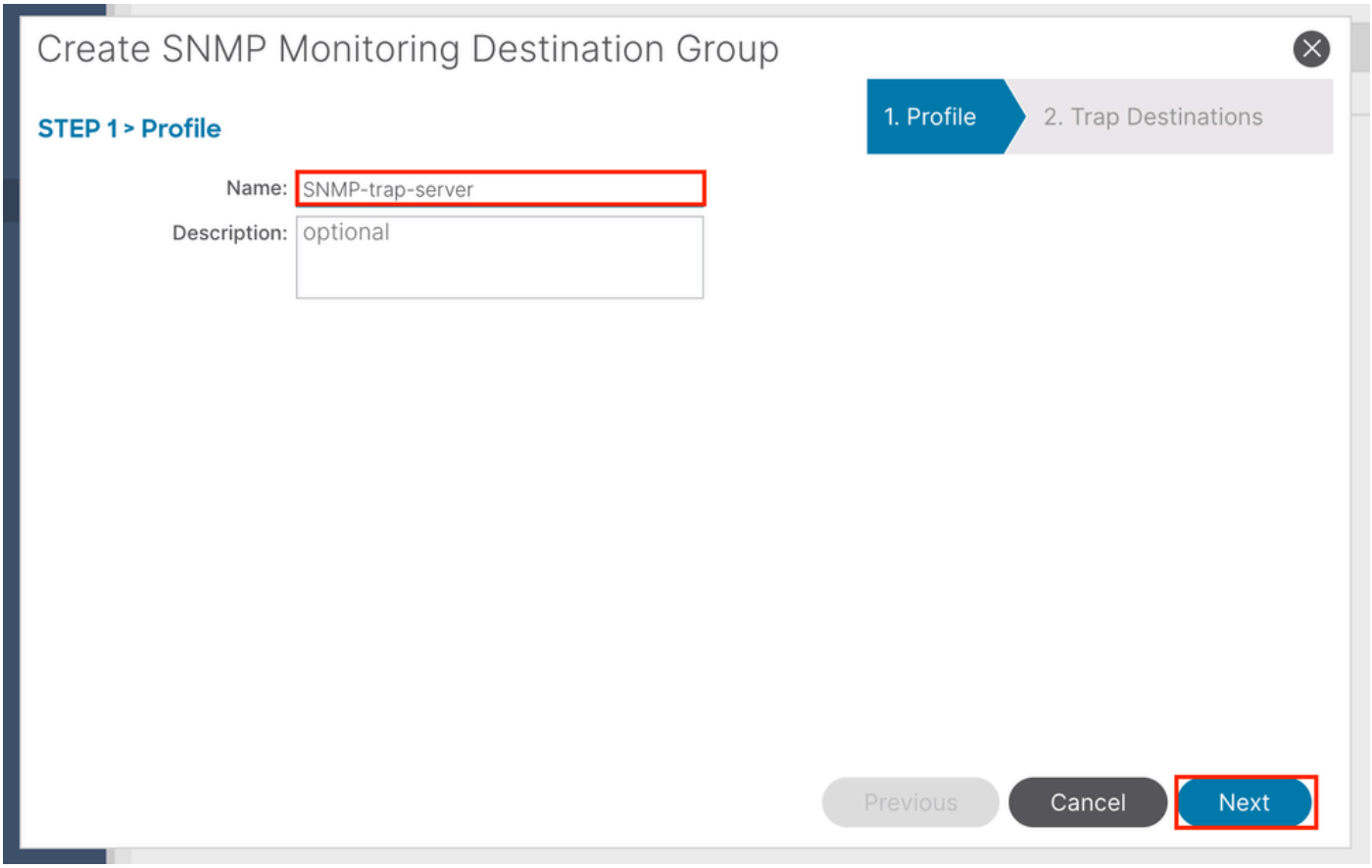
> **Nota**: senza i passaggi da 1 a 3 della sezione precedente, la configurazione delle TRAP SNMP non è sufficiente. Passaggio 2. Nella configurazione TRAP SNMP è correlato ai criteri di monitoraggio per (Access/Fabric/Tenant).

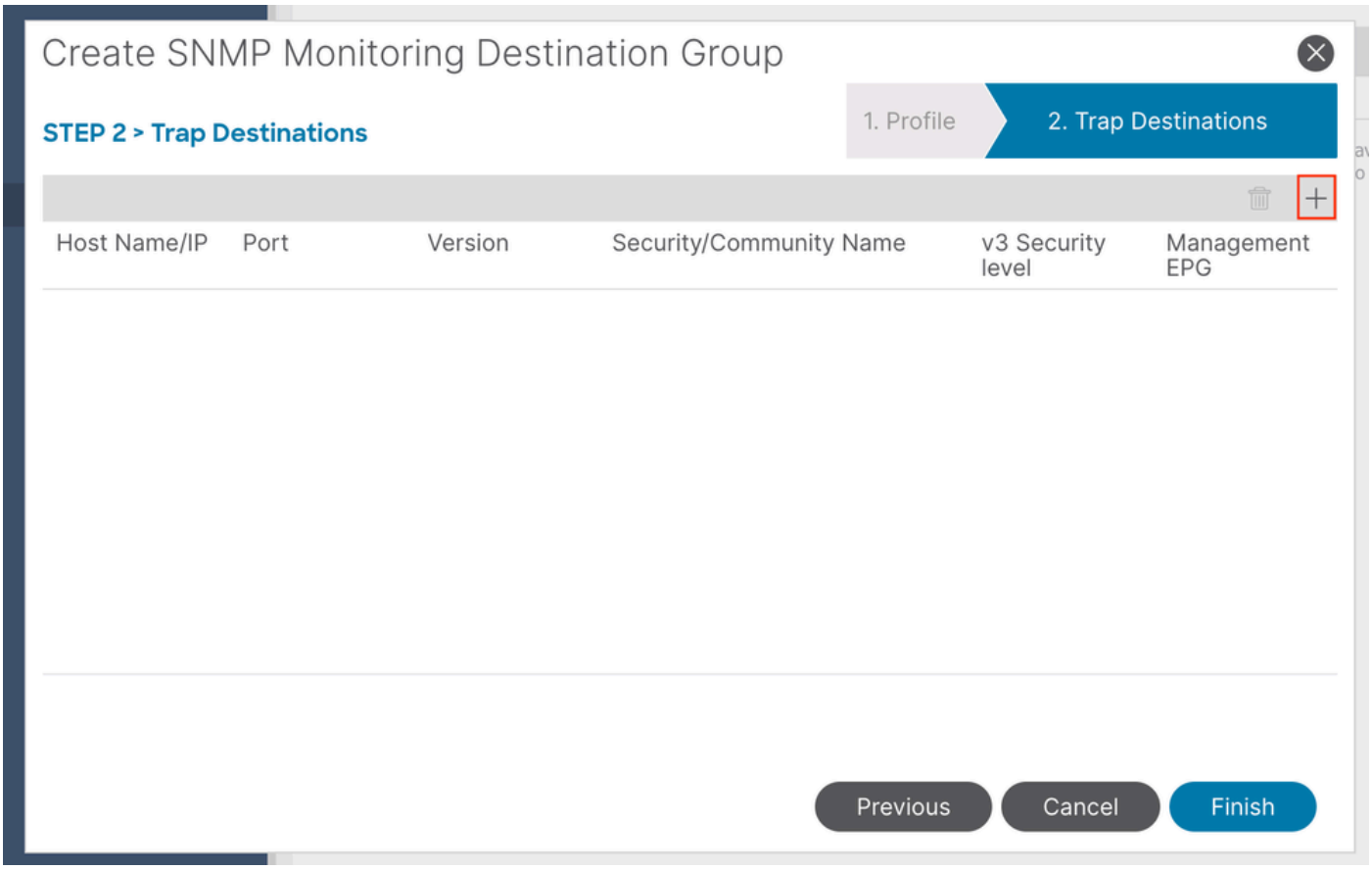
Per configurare le TRAP SNMP in ACI, è necessario eseguire i due passaggi oltre ai passaggi 1, 2 e 3 della sezione precedente.

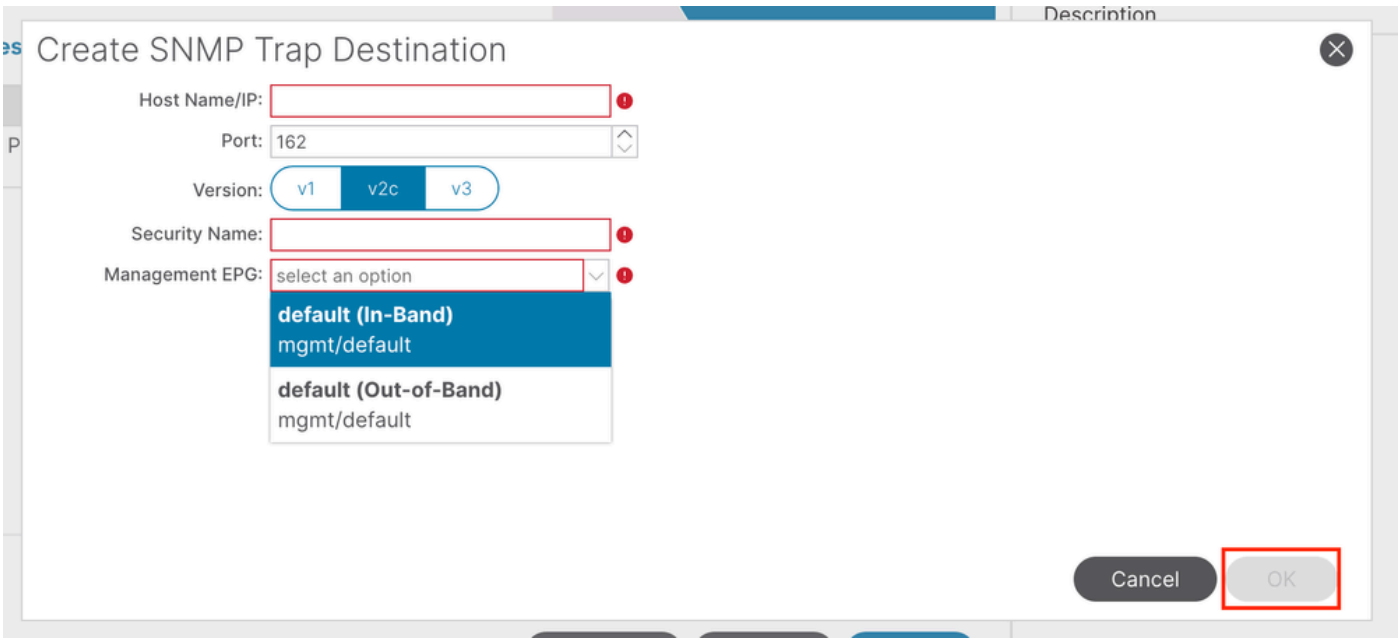
Passaggio 1. Configurazione del server TRAP SNMP

A tale scopo, selezionare il percorso dell'interfaccia utente grafica del Web APICAdmin > Eternal Data Collectors > Monitoring Destinations > SNMP.









Nome host/IP - l'host per la destinazione trap SNMP.

Porta: la porta di servizio della destinazione trap SNMP. L'intervallo è compreso tra 0 (non specificato) e 65535; il valore predefinito è 162.

Versione: la versione CDP supportata per la destinazione trap SNMP. La versione può essere:

- v1 - utilizza una stringa della community corrispondente per l'autenticazione utente.

- v2c: utilizza una stringa della community corrispondente per l'autenticazione utente.

- v3: un protocollo interoperabile basato su standard per la gestione della rete che fornisce un accesso sicuro ai dispositivi tramite una combinazione di autenticazione e crittografia dei frame sulla rete.

Il valore predefinito è **v2c**.

Nome sicurezza: il nome della sicurezza della destinazione trap SNMP (nome della community). Non può contenere il simbolo **@**.

v.3 Livello di protezione: il livello di protezione SNMPv3 per il percorso di destinazione SNMP. Il livello può essere:

- auth

- noauth

- privato

Il valore predefinito è **noauth**.

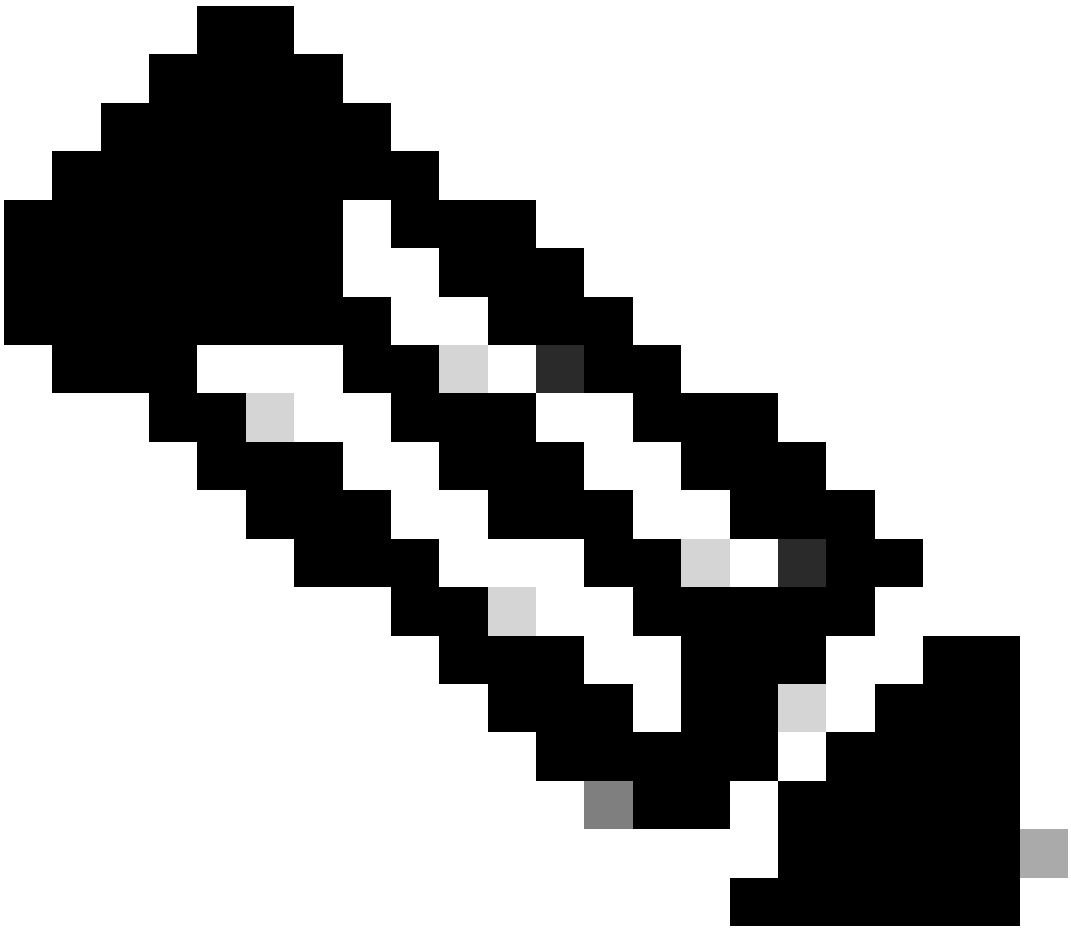
Management EPG: il nome del gruppo di endpoint di gestione per la destinazione SNMP attraverso cui è raggiungibile l'host remoto.

Passaggio 2. Configura origine TRAP SNMP in Criteri di monitoraggio (accesso/infrastruttura/tenant)

È possibile creare criteri di monitoraggio con i tre ambiti seguenti:

- Accesso - porte di accesso, FEX, controller VM
- Fabric - porte fabric, schede, chassis, ventole

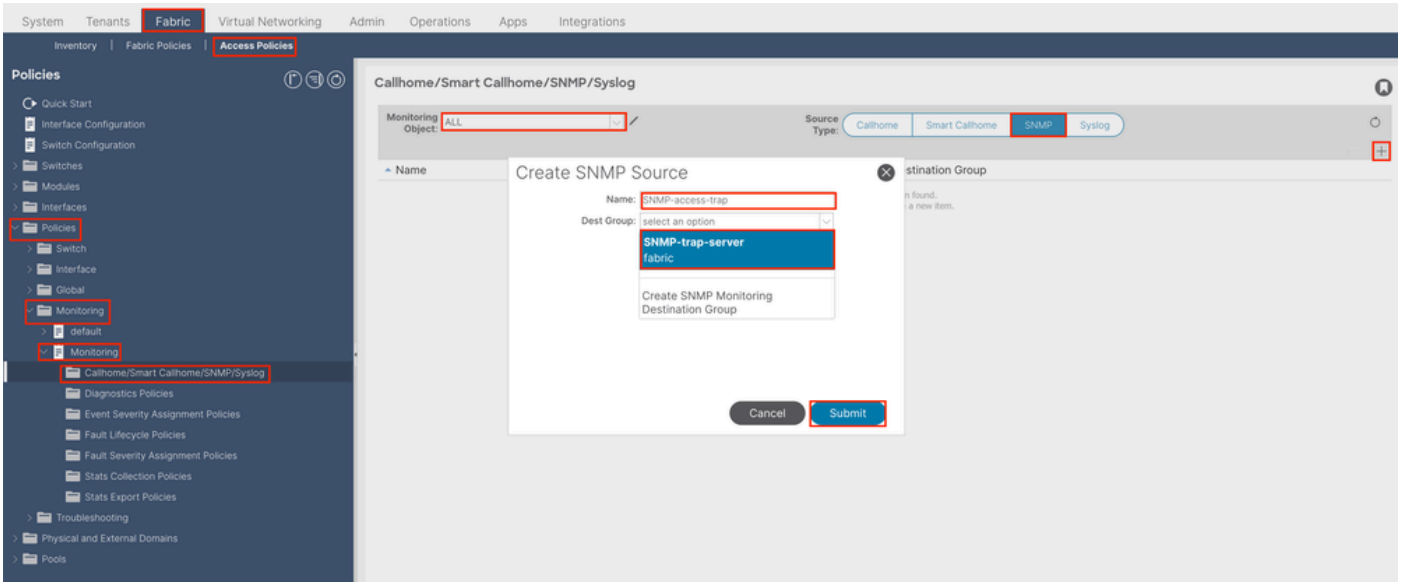
- Tenant - EPG, profili di applicazioni, servizi

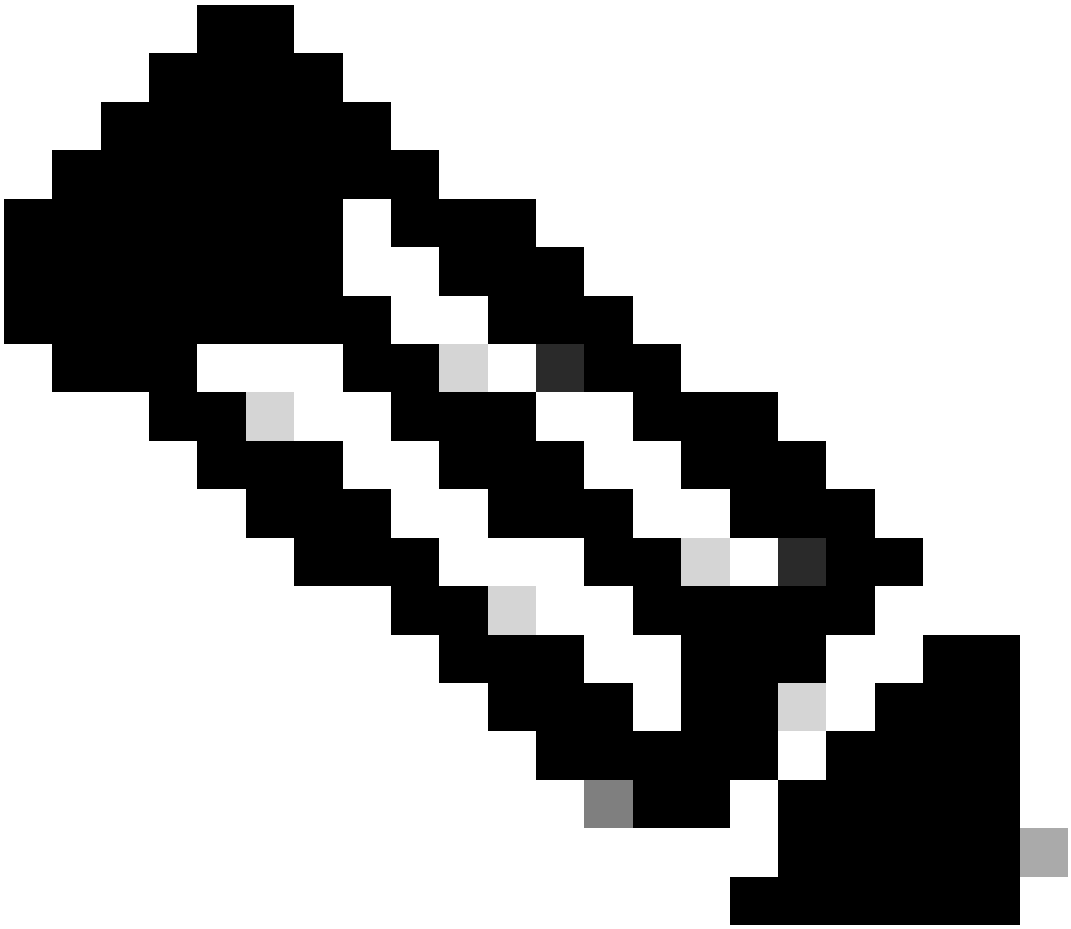


Nota: è possibile scegliere una qualsiasi combinazione di queste opzioni per eseguire la configurazione in base alle proprie esigenze.

Opzione 1. Definizione dell'origine SNMP in Criteri di accesso

A tale scopo, selezionare il percorso dell'interfaccia utente grafica del Web
APICFabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

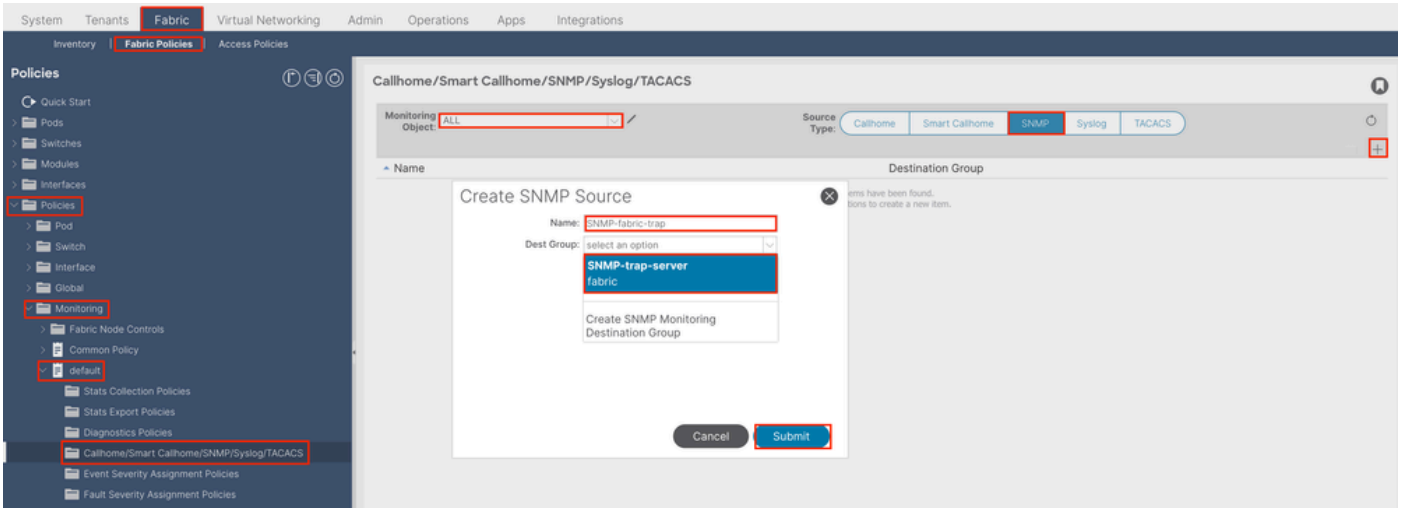

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog
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: è possibile utilizzare un criterio di monitoraggio personalizzato (se configurato) anziché quello predefinito. In questo caso, utilizzare quello predefinito. È possibile specificare l'oggetto di monitoraggio da monitorare. Tutti gli oggetti sono stati utilizzati in questa finestra.

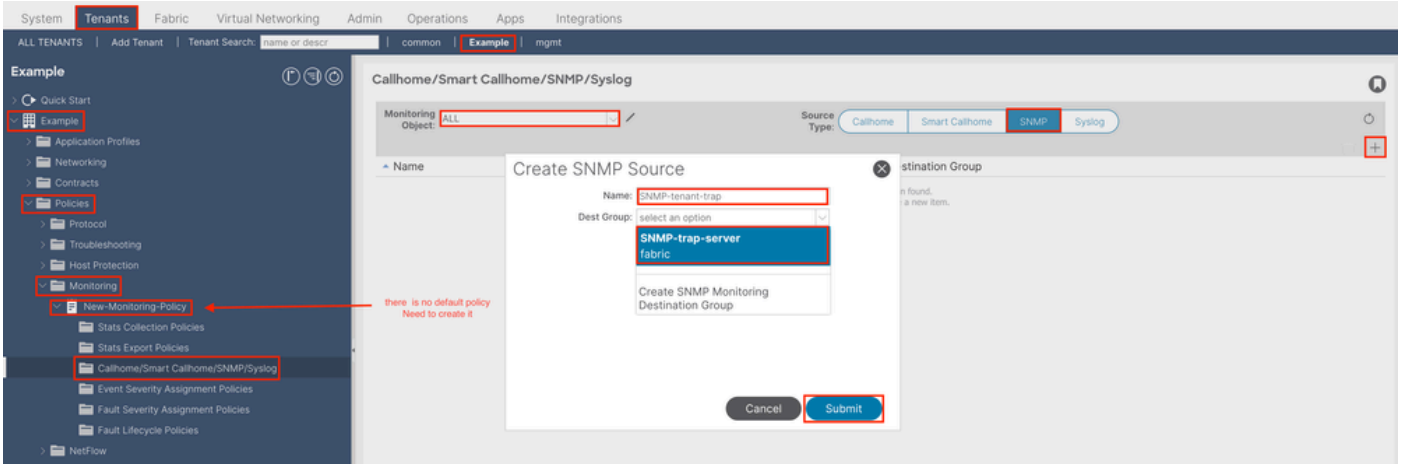
Opzione 2. Definizione dell'origine SNMP in Criteri fabric

A tale scopo, selezionare il percorso dell'interfaccia utente grafica del Web APICFabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Opzione 3. Definisci origine SNMP in Criteri tenant

A tale scopo, selezionare il percorso dell'interfaccia utente grafica del Web APICTenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Verifica

Utilizzare il comando snmpwalk per verificare

Innanzitutto, occorre prendere in considerazione il pull dei dati SNMP dall'ambito globale di uno switch foglia. L'utilizzo del comando

snmpwalk consente di eseguire queste operazionisnmpwalk -v 2c -c New-1 x.x.x.x.

Questo comando suddiviso rappresenta:

snmpwalk = L'eseguibile snmpwalk installato su MacOS/Linux/Windows

-v = Specifica la versione di SNMP da utilizzare

2c= Specifica l'utilizzo di SNMP versione 2c

-c= Specifica che una determinata stringa della community

New-1= La stringa della community viene utilizzata per il pull dei dati SNMP dell'ambito globale

x.x.x.x= Indirizzo IP di gestione fuori banda dello switch foglia

Risultato comando:

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

Nell'output del comando snipped, è possibile verificare che lo snmpwalk ha esito positivo e che sono state estratte informazioni specifiche dell'hardware. Se si lascia procedere lo snmpwalk, verranno visualizzati i nomi delle interfacce hardware, le descrizioni e così via.

Ora, procedere per recuperare i dati SNMP del contesto VRF, i contesti SNMP creati in precedenza, **New-VRF-SNMP** per i VRF utilizzando la stringa della community SNMP, **New-1**.

Poiché la stessa stringa della community viene utilizzata, **New-1**, in due contesti SNMP diversi, è necessario specificare il contesto SNMP da cui estrarre i dati SNMP. È disponibile la sintassi snmpwalk da utilizzare per specificare un particolare contesto SNMP; snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.

Come si può notare, per estrarre da un contesto SNMP specifico si utilizza il formato: COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

Uso dei comandi show della CLI

Su APIC:

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

Interruttore On:

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

Uso dei comandi Moquery della CLI

Su APIC/Switch:

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

Uso dei comandi CLI cat

Su APIC:

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

Risoluzione dei problemi

Controllare il processo snmpd

Interruttore On:

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

Su APIC:

```
ps aux | grep snmp
```

Se il processo è normale, contattare Cisco TAC per ulteriore assistenza.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).