Configuring SNMP in APIC

Configuring the SNMP Policy Using the GUI

This procedure configures and enables the SNMP policy on ACI switches.

Before you begin

To allow SNMP communications, you must configure the following:

- Configure an out-of-band contract allowing SNMP traffic. SNMP traffic typically uses UDP port 161 for SNMP requests.
- Configure the APIC out-of-band IP addresses in the 'mgmt' tenant. Although the out-of-band addresses are configured during APIC setup, the addresses must be explicitly configured in the 'mgmt' tenant before the out-of-band contract will take effect.

Procedure

Step 1 In the menu bar, click **Fabric**.

Step 2 In the submenu bar, click **Fabric Policies**.

Step 3 In the **Navigation** pane, expand **Pod Policies**.

Step 4 Under **Pod Policies**, expand **Policies**.

Step 5 Right-click **SNMP** and choose **Create SNMP Policy**.

As an alternative to creating a new SNMP policy, you can edit the **default** policy fields in the same manner as described in the following steps.

Step 6 In the SNMP policy dialog box, perform the following actions:

a) In the **Name** field, enter an SNMP policy name.

b) In the **Admin State** field, select **Enabled**.

c) (Optional) In the **SNMP v3 Users** table, click the **+** icon, enter a **Name**, enter the user's authentication data, and click **Update**.

This step is needed only if SNMPv3 access is required.

d) In the **Community Policies** table, click the + icon, enter a **Name**, and click **Update**.

The community policy name can be a maximum of 32 characters in length. The name can contain only letters, numbers and the special characters of underscore (_), hyphen (-), or period (.). The name cannot contain the @ symbol.

e) In the **Trap Forward Servers** table, click the + icon, enter the **IP Address** of the external server and click **Update**.

Step 7 Required: To configure allowed SNMP management stations, perform the following actions in the SNMP policy dialog box:

a) In the **Client Group Policies** table, click the + icon to open the **Create SNMP Client Group Profile** dialog box.
b) In the **Name** field, enter an SNMP client group profile name.
c) From the **Associated Management EPG** drop-down list, choose the management EPG.
d) In the **Client Entries** table, click the + icon.
e) Enter a client's name in the **Name** field, enter the client's IP address in the **Address** field, and click **Update**.

Note When an SNMP management station connects with APIC using SNMPv3, APIC does not enforce the client IP address specified in the SNMP client group profile. For SNMPv3, the management station must exist in the **Client Entries** list, but the IP address need not match, as the SNMPv3 credentials alone are sufficient for access.

Step 8 Click **OK**.

Step 9 Click **Submit**.

Step 10 Under **Pod Policies**, expand **Policy Groups** and choose a policy group or right-click **Policy Groups** and choose **Create POD Policy Group**.

You can create a new pod policy group or you can use an existing group. The pod policy group can contain other pod policies in addition to the SNMP policy.

Step 11 In the pod policy group dialog box, perform the following actions:

a) In the **Name** field, enter a pod policy group name.
b) From the **SNMP Policy** drop-down list, choose the SNMP policy that you configured and click **Submit**.

Step 12 Under **Pod Policies**, expand **Profiles** and click **default**.

Step 13 In the **Work pane**, from the **Fabric Policy Group** drop-down list, choose the pod policy group that you created.

Step 14 Click **Submit**.

Step 15 Click **OK**.

Configuring SNMP Traps

Configuring an SNMP Trap Destination Using the GUI

This procedure configures the host information for an SNMP manager that will receive SNMP trap notifications.

Note ACI supports a maximum of 10 trap receivers. If you configure more than 10, some will not receive notifications.

Procedure

Step 1 In the menu bar, click **Admin**.

Step 2 In the submenu bar, click **External Data Collectors**.

Step 3 In the **Navigation** pane, expand **Monitoring Destinations**.

Step 4 Right-click **SNMP** and choose **Create SNMP Monitoring Destination Group**.

Step 5 In the **Create SNMP Monitoring Destination Group** dialog box, perform the following actions:

a) In the **Name** field, enter an SNMP destination name and click **Next**.

b) In the **Create Destinations** table, click the **+** icon to open the **Create SNMP Trap Destination** dialog box.

c) In the **Host Name/IP** field, enter an IPv4 or IPv6 address or a fully qualified domain name for the destination host.

d) Choose the **Port** number and SNMP **Version** for the destination.

e) For SNMP v1 or v2c destinations, enter one of the configured community names as the **Security Name** and choose **noauth** as **v3 Security Level**.

An SNMP v1 or v2c security name can be a maximum of 32 characters in length. The name can contain only letters, numbers and the special characters of underscore (_), hyphen (-), or period (.). For SNMP v2c, the @ symbol is also allowed.

f) For SNMP v3 destinations, enter one of the configured SNMP v3 user names as **Security Name** and choose the desired **v3 Security Level**.

An SNMP v3 security name can be a maximum of 32 characters in length. The name must begin with an uppercase or lowercase letter, and can contain only letters, numbers, and the special characters of underscore (_), hyphen (-), period (.), or the @ symbol.

g) From the **Management EPG** drop-down list, choose the management EPG.

h) Click **OK**.

i) Click **Finish**.

Configuring an SNMP Trap Source Using the GUI

This procedure selects and enables a source object within the fabric to generate SNMP trap notifications.

Procedure

Step 1 In the menu bar, click **Fabric**.

Step 2 In the submenu bar, click **Fabric Policies**.

Step 3 In the **Navigation** pane, expand **Monitoring Policies**.

You can create an SNMP source in the **Common Policy**, the **default** policy, or you can create a new monitoring policy.

Step 4 Expand the desired monitoring policy and choose **Callhome/SNMP/Syslog**.

If you chose the **Common Policy**, right-click **Common Policy**, choose **Create SNMP Source**, and follow the instructions below for that dialog box.

Step 5 In the **Work** pane, from the **Monitoring Object** drop-down list, choose **ALL**.

Step 6 From the **Source Type** drop-down list, choose **SNMP**.

Step 7 In the table, click the **+** icon to open the **Create SNMP Source** dialog box.

Step 8 In the **Create SNMP Source** dialog box, perform the following actions:

a) In the **Name** field, enter an SNMP policy name.

b) From the **Dest Group** drop-down list, choose an existing destination for sending notifications or choose **Create SNMP Monitoring Destination Group** to create a new destination.

The steps for creating an SNMP destination group are described in a separate procedure.

c) Click **Submit**.

Accessing Context-Specific MIBs

Associating the SNMP Context With a VRF Using the GUI

Each context (private network) supports its own instance of a context-specific MIB. To determine which MIBs are context-specific, see the *Cisco ACI MIB Support List*.

This procedure creates an SNMP context associated with a context within a tenant (VRF).

Procedure

Step 1 On the menu bar, click **Tenants** and, in the submenu, click the desired tenant.

Step 2 In the **Navigation** pane, expand **Networking** and **Private Networks**.

Step 3 Under **Private Networks**, select the context to be associated with the context-specific MIBs.

Step 4 Right-click the desired context and choose **Create SNMP Context**.

Step 5 In the **Create SNMP Context** dialog box, perform the following actions:

a) In the **Name** field, type a name for the SNMP context.

b) (Optional) In the **Community Profiles** table, click the **+** icon, type the name of an existing community.

This step associates the SNMP context with an existing SNMP policy, simplifying the SNMP community string used to access the context-specific MIBs. The SNMP community must already be defined in the SNMP policy applied under **Fabric > Fabric Policies > Pod Policies > SNMP**.

Note With this association, the SNMP community becomes bound to this SNMP context and provides access only to context-specific OIDs, regardless of whether it previously provided access to fabric-level OIDs.

c) Click **Submit**.

Accessing the Context-Specific MIBs

A context (private network) supports its own instance of a context-specific MIB. You can access the context-specific MIBs using the `snmpwalk` command.

The following examples show how to access the context-specific BGP MIB using these example settings:

- The SNMP version is SNMPv2c, specified by `snmpwalk -v2c`.
- The example community name is `cisco1`.
- An SNMP context has been configured and named `snmp-t2-context2` using the procedure described in Associating the SNMP Context With a VRF Using the GUI, on page 4.
- The SNMP context configuration procedure contains an optional step to associate the SNMP context (`snmp-t2-context2`) with an existing community profile (`cisco1`). The examples include an example with this step and an example without this step.
- The SNMP agent of the context is 192.20.0.123.

Example 1

This example shows how to retrieve a non-context-specific MIB named ifTable.

```
linuxhost:> snmpwalk -v2c -c cisco1 192.20.0.123 ifTable
```

Example 2

This example shows how to retrieve a context-specific MIB named bgp when the SNMP context has not been associated with the community name. In this case, the context must be addressed using the format *community-name@snmp-context-name*.

```
linuxhost:> snmpwalk -v2c -c cisco1@snmp-t2-context2 192.20.0.123 bgp
```

Example 3

This example shows how to retrieve a context-specific MIB named bgp when the SNMP context has been associated with the community name. In this case, the SNMP context name can be omitted and the context is addressed using only the community name.

```
linuxhost:> snmpwalk -v2c -c cisco1 192.20.0.123 bgp
```