Cisco Application Centric Infrastructure

# Configuring SNMP for ACI

## Pre-requisites

1. To allow SNMP communications, you must configure an "out-of-band (OOB) contract" in the "mgmt" tenant to allow SNMP traffic. SNMP traffic typically uses UDP port 161 for SNMP requests.
2. Configure the APIC OOB IP addresses in the "mgmt" tenant. Although the OOB addresses are configured during APIC setup, the addresses must be explicitly configured in the "mgmt" tenant before the OOB contract will take effect.

## About SNMP

ACI provides SNMPv1, v2, and v3 support, including Management Information Bases (MIBs) and notifications (traps). The SNMP standard allows any third-party applications that support the different MIBs to manage and monitor the ACI fabric.

- SNMP read queries (Get, Next, Bulk, Walk) are supported by leaf, spine switches and by APIC.
- SNMP write commands (Set) are not supported by leaf, spine switches or by APIC.
- SNMP traps (v1, v2c, and v3) are supported by leaf and spine switches and by APIC.
- SNMPv3 is supported by leaf and spine switches and by APIC.

Note: A maximum of 10 trap receivers are supported. If you configure more than 10, some will not receive notifications. (Servers listen in on port 162. ACI agents listen in on port 161.)

For the complete list of MIBs supported in ACI, see http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html.

## Allowing SNMP Access to the APIC Controllers

Unlike Fabric switches, a contract is required in order for the APIC to allow SNMP. For SNMP to successfully contact your APICs, you will need configure a couple of items:

1. Ensure that your OOB contract permits SNMP (Ports 161/162).
2. Ensure that you have Node Management Addresses in Tenant Mgmt configured for all of your APICs.

## Step 1 – Management Contracts (Out-of-band and Inband)

If you already have OOB or Inband Contracts defined inside of Tenant Mgmt, you will need to add the appropriate filters to your contracts for SNMP (UDP-161 and UDP-162). *Note: If you are using a permit any contract, then you can skip this step.*

**1. Add UDP-161 to existing Contract** (if you are not using default/common or permit any)

1. Tenants > Tenant mgmt > Security Policies
2. Expand Out-of-Band Contracts
    1. Edit existing OOB Contract
    2. Select OOB Subject
    3. Select OOB Filter
    4. Review filter and add (if necessary) UDP-161
3. If you also have Inband Mgmt Connectivity configured, also verify the INB contract filter to permit UDP-161.

**2. Verify you are providing Out-of-Band Contract in Tenant mgmt**

1. Tenant > Tenant mgmt > Node Management EPGs > Out-of-Band EPG default.
2. Under the "Provided Out-of-Band Contracts" in the policy window, provide the appropriate contract. (This could be a the default/common contract, or a specific contract you have created and modified).

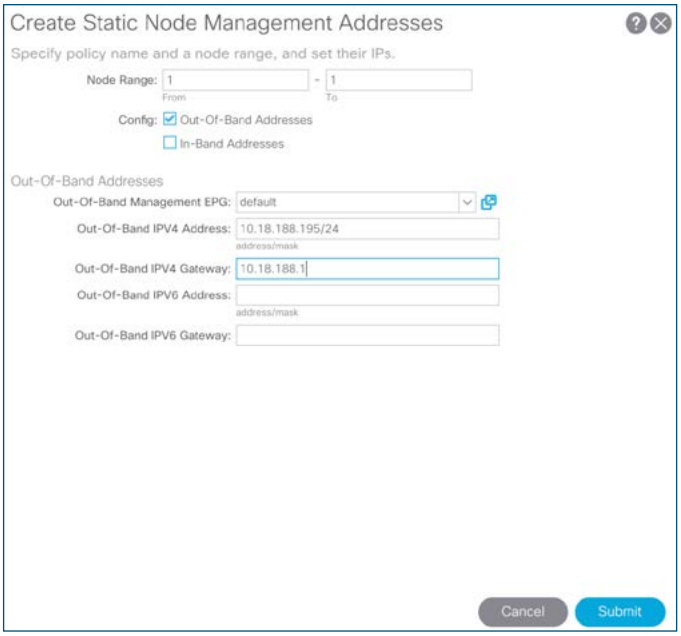
**3. Verify you are consuming Out-of-Band Contract in Tenant mgmt**

1. Tenant > Tenant mgmt > External Management Network Instance Profiles > *YourInstanceProfile.*
2. Consume the same contract which you provided in the previous step.
3. Enter the subnets which are allowed to have access to the APIC. (0.0.0.0/0 will permit all.)

## Step 2 – Check to ensure APICs are configured in the Node Management Addresses

Tenant > Tenant mgmt > Node Management Addresses > Static Node Management Addresses

- Configure a separate entry for each of your APICs
    - Node IDs for your APIC will range from 1-3 (assuming you have a 3-node APIC cluster).




*Tenant > Tenant mgmt > Node Management Addresses > Static Node Management Addresses*

# Configuring SNMP for Your Fabric Switches

There are two different places where you need to configure SNMP for your ACI Fabric Switches in the GUI:

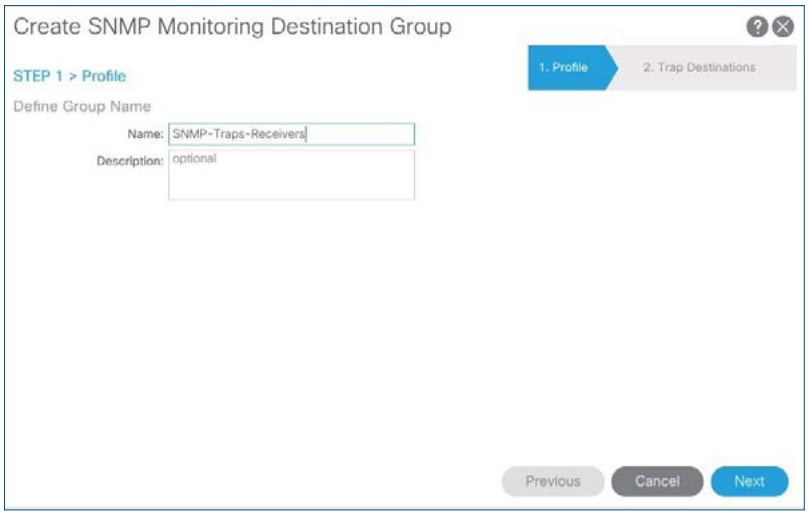
- Under Admin Tab
- Under Fabric Tab

# Under Admin Tab

## Traps

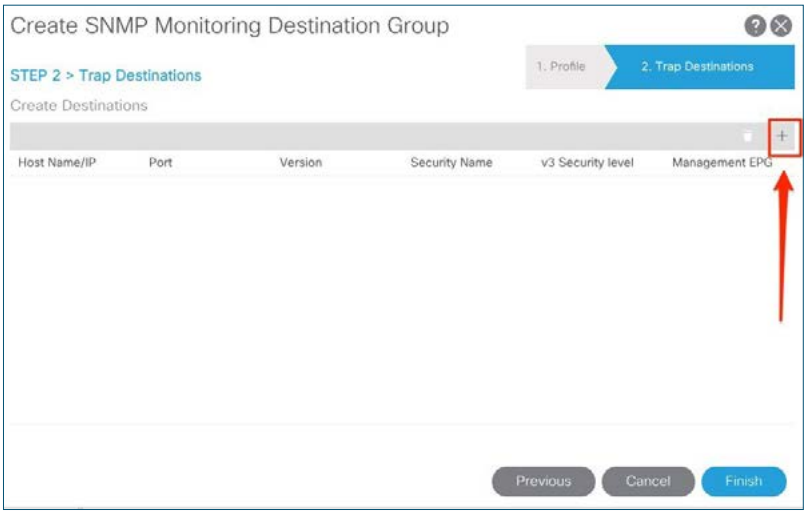
Trap Destinations are configured here.

Goto Admin > External Data Collectors > Monitoring Destinations > SNMP > [right click] Create SNMP Monitoring Destination Group



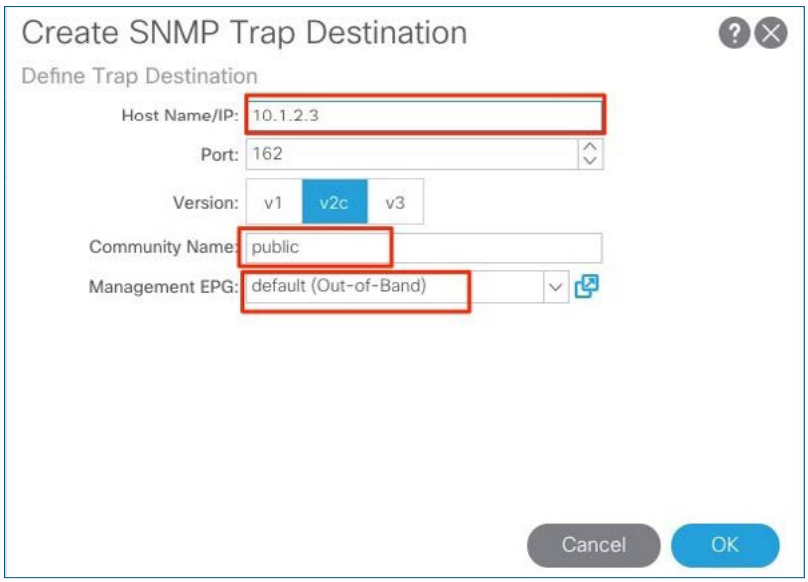

Step 1. Profile
Give it a name (e.g. SNMP-Traps-Receivers), then click Next.

STEP 2 > Trap Destinations
Click the '+' sign to add NMS Servers (receivers).




Then add the destination servers. The required parameters here are Server IP (or hostname if DNS is configured), Community password, and Management EPG. An example is below:

Host IP: 10.1.2.3
Community Name: public
Management EPG: default (Out-of-Band)
<<<<<<<<<<< This out-of-band management was configured separately and is a pre-requisite for SNMP to work.




Then click Finish.
Repeat the above process to configure more destinations for SNMP traps.

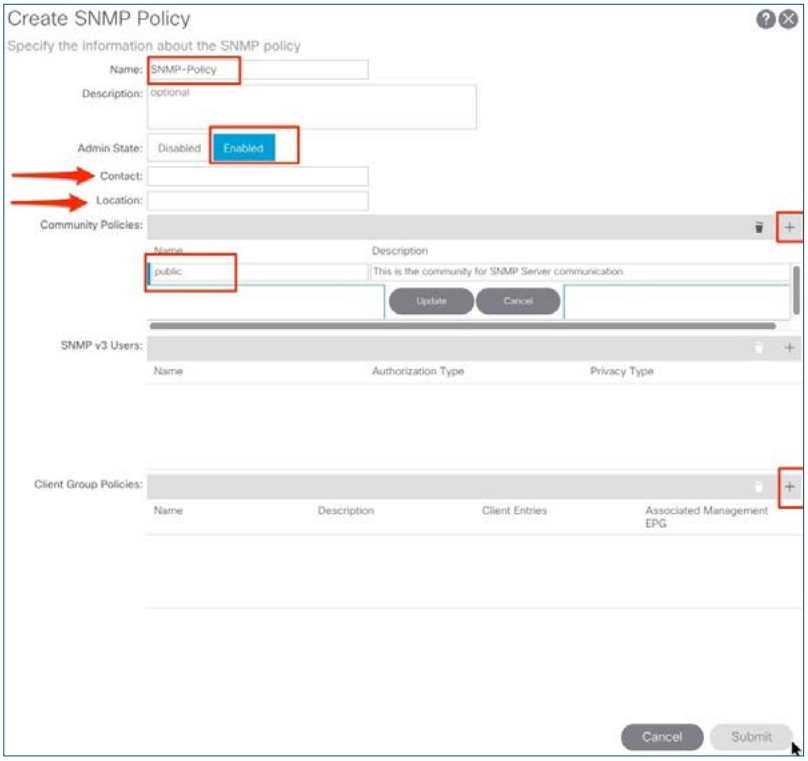
This has completed the task of configuring NMS servers to receive traps. You will use this server IP (or a set of servers) as destinations in other parts of the configuration as well.

# Under Fabric Tab

Under the Fabric menu, you will configure at two places:

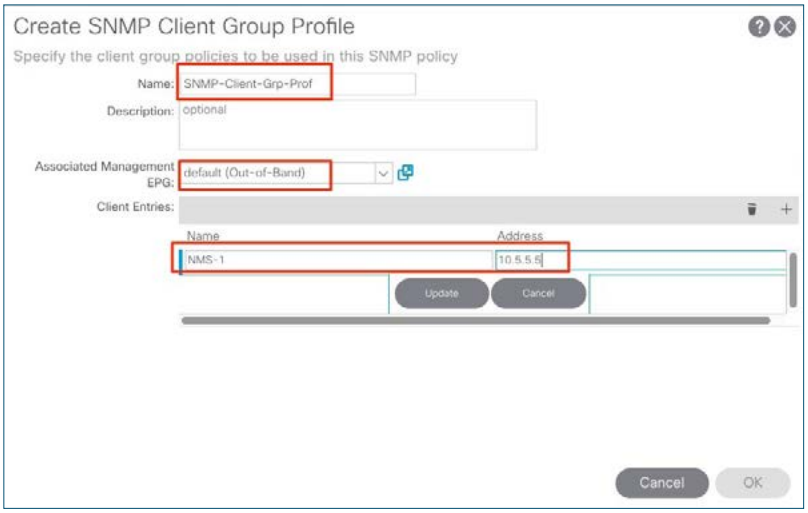
1. Monitoring Policies
2. **Pod Policies**

Go to Fabric > Fabric Policies > Pod Policies > SNMP >[right click] Create SNMP Policy. You will see the below screen and fill it according to the sample shown below.




Name – Give it a name.
Admin State – Enable.
Contact – Give a contact name here (optional).
Location – Give the location of the DC (optional).
Community Policies – Glick the "+" sign and enter. the community password here. Then hit Update. Then click the "+" sign under "Client Group Policies".

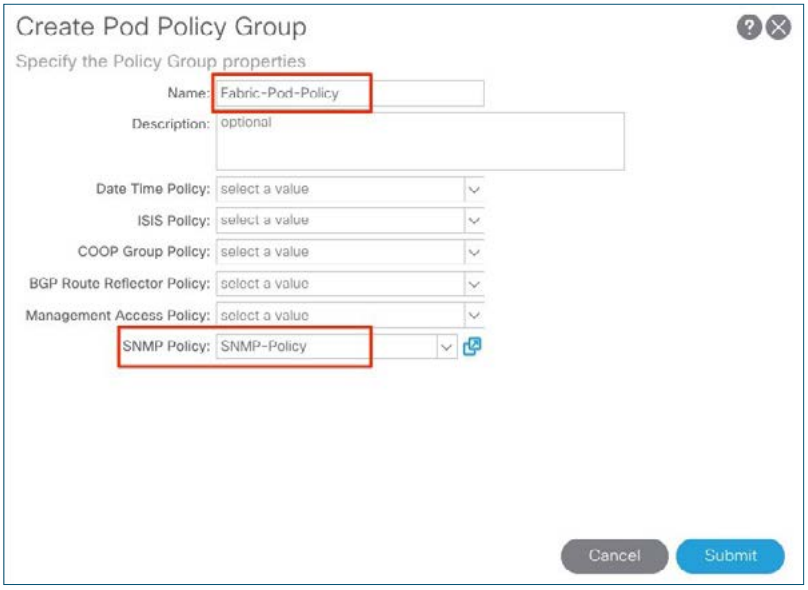
You will enter into a window titled "Create SNMP Client Group Profile". This is where we will enter the NMS server IP(s).




Name – Give it a name.
Associated Management EPG – Ghoose "default (Out-of-Band)".
Click the "+" sign under "Client Entries".
Add the NMS servers (host) name and IP address.
Hit Update.
Hit Submit.
Hit Submit again.

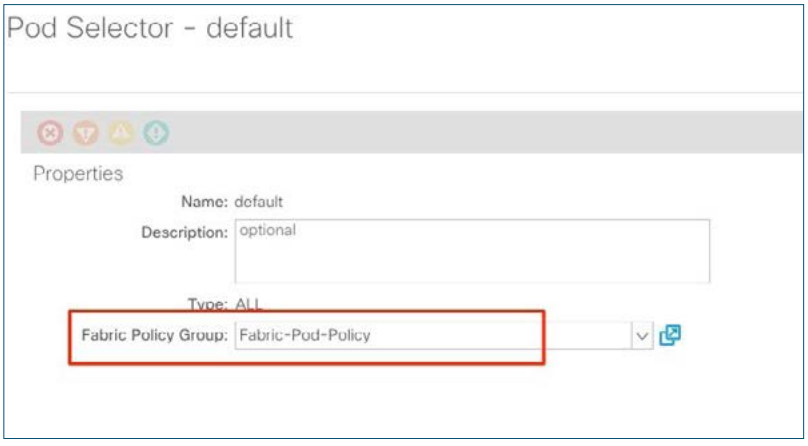
This completes this section.

Now go to Fabric > Fabric Policies > Pod Policies > Policy Group >[right click] Create Pod Policy Group. You will see the below screen and fill it according to the sample shown below.




Name – Give it a name.
SNMP Policy – Select the SNMP policy that you created earlier. In the example SNMP-Policy was created.
Hit Submit.

Now Go to Fabric > Fabric Policies > Pod Policies > Profile > Pod Profile default > default. You will see the below screen and fill it according to the sample shown below.




Choose the "Policy Group" that you created in the previous step. In the example it is "Fabric-Pod-Policy".
Hit Submit.

This concludes the configuration that needs to be performed under Pod Policies.

Next you will configure under the Monitoring Policies.

## 2. Monitoring Policies

Goto Fabric > Fabric Policies > Monitoring Policies > Common Policy > Callhome/SNMP/Syslog

This is to allow objects in MIT to send traps to the NMS station.

In the work pane, select SNMP and then from the tools icon ( ) select "Create SNMP Source".


Name – Gve it a name (e.g. SNMP-Source-Objects).
Dest Group – Use the previously created destination group. In the example "SNMP-Traps-Receivers" is used.
Hit Submit.

# Configuring Monitoring Policies

Administrators can create monitoring policies with the following four broad scopes:

1. Fabric Wide (**Common**): includes both fabric and access objects
2. Access (infra): access ports, FEX, VM controllers, etc.
3. Fabric: fabric ports, cards, chassis, fans, etc.
4. Tenant: EPGs, application profiles, services, etc.

In the example, Fabric Wide (Common) Policies is configured. You could also configure:

- Fabric policies (under Fabric > Fabric Policies > Monitoring Policies > default)
- Access policies (under Fabric > Access Policies > Monitoring Policies > default)
- Tenant policies (under Tenant > your-tenant-name > Monitoring Policies > [right click] Create Monitoring Policy

NOTE: To access context specific MIBs, you have to enable the tenant by right clicking on the VRF in the tenant and clicking "Create SNMP Context". See image to the right for reference.