Intra-EPG Isolation Enforcement and Cisco ACI

This chapter contains the following sections:

Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or uSeg EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from on another within an EPG is desirable. For example, you may want to enforce intra-EPG isolation if the endpoint VMs in the same EPG belong to multiple tenants, or to prevent the possible spread of a virus.

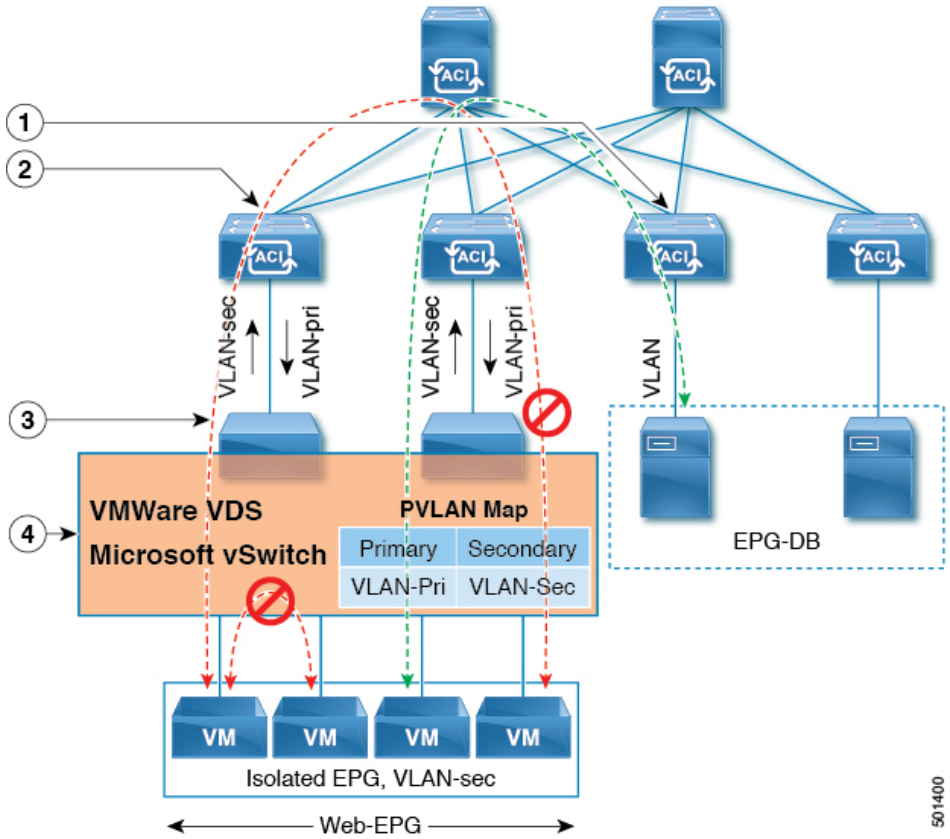
A Cisco ACI virtual machine manager (VMM) domain creates an isolated PVLAN port group at the VMware VDS or Microsoft Hyper-V Virtual Switch for each EPG that has intra-EPG isolation enabled. A fabric administrator specifies primary encapsulation or the fabric dynamically specifies primary encapsulation at the time of EPG-to-VMM domain association. When the fabric administrator selects the VLAN-pri and VLAN-sec values statically, the VMM domain validates that the VLAN-pri and VLAN-sec are part of a static block in the domain pool.

Note When intra-EPG isolation is not enforced, the VLAN-pri value is ignored even if it is specified in the configuration.

VLAN-pri/VLAN-sec pairs for the VMware VDS or Microsoft Hyper-V Virtual Switch are selected per VMM domain during the EPG-to-domain association. The port group created for the intra-EPG isolation EPGs uses the VLAN-sec tagged with type set to `PVLAN`. The VMware VDS or the Microsoft Hyper-V Virtual Switch and fabric swap the VLAN-pri/VLAN-sec encapsulation:

- Communication from the Cisco ACI fabric to the VMware VDS or Microsoft Hyper-V Virtual Switch uses VLAN-pri.
- Communication from the VMware VDS or Microsoft Hyper-V Virtual Switch to the Cisco ACI fabric uses VLAN-sec.

Figure 1: Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch



Note these details regarding this illustration:

1. EPG-DB sends VLAN traffic to the Cisco ACI leaf switch. The Cisco ACI egress leaf switch encapsulates traffic with a primary VLAN (PVLAN) tag and forwards it to the Web-EPG endpoint.
2. The VMware VDS or Microsoft Hyper-V Virtual Switch sends traffic to the Cisco ACI leaf switch using VLAN-sec. The Cisco ACI leaf switch drops all intra-EPG traffic because isolation is enforced for all intra VLAN-sec traffic within the Web-EPG.
3. The VMware VDS or Microsoft Hyper-V Virtual Switch VLAN-sec uplink to the Cisco ACI Leaf is in isolated trunk mode. The Cisco ACI leaf switch uses VLAN-pri for downlink traffic to the VMware VDS or Microsoft Hyper-V Virtual Switch.
4. The PVLAN map is configured in the VMware VDS or Microsoft Hyper-V Virtual Switch and Cisco ACI leaf switches. VM traffic from WEB-EPG is encapsulated in VLAN-sec. The VMware VDS or Microsoft Hyper-V Virtual Switch denies local intra-WEB EPG VM traffic according to the PVLAN tag. All intra-ESXi host or Microsoft Hyper-V host VM traffic is sent to the Cisco ACI leaf using VLAN-Sec.

Related Topics

For information on configuring intra-EPG isolation in a Cisco AVS environment, see Intra-EPG Isolation Enforcement for Cisco AVS, on page 6.

Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the GUI

Procedure

Step 1 Log into Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the left navigation pane expand the **Application Profiles** folder and appropriate application profile.

Step 4 Right-click the **Application EPGs** folder and then choose **Create Application EPG**.

Step 5 In the **Create Application EPG** dialog box, complete the following steps:

a) In the **Name** field, add the EPG name.
b) In the **Intra EPG Isolation** area, click **Enforced**.
c) In the **Bridge Domain** field, choose the bridge domain from the drop-down list.
d) Associate the EPG with a bare metal/physical domain interface or with a VM Domain.

- For the VM Domain case, check the **Associate to VM Domain Profiles** check box.
- For the bare metal case, check the **Statically Link with Leaves/Paths** check box.

e) Click **Next**.
f) In the **Associated VM Domain Profiles** area, click the + icon.
g) From the **Domain Profile** drop-down list, choose the desired VMM domain.

For the static case, in the **Port Encap (or Secondary VLAN for Micro-Seg)** field, specify the secondary VLAN, and in the **Primary VLAN for Micro-Seg** field, specify the primary VLAN. If the Encap fields are left blank, values will be allocated dynamically.

Note For the static case, a static VLAN must be available in the VLAN pool.

Step 6 Click **Update** and click **Finish**.

Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the NX-OS Style CLI

Procedure

Step 1 In the CLI, create an intra-EPG isolation EPG:

Example:

The following example is for VMware VDS:

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
```

```
  tenant Tenant_VMM
    application Web
      epg intraEPGDeny
        bridge-domain member VMM_BD
        vmware-domain member PVLAN encap vlan-2001 primary-encap vlan-2002 push on-demand
        vmware-domain member mininet
          exit
        isolation enforce
        exit
      exit
    exit
apic1(config-tenant-app-epg)#
```

Example:

The following example is for Microsoft Hyper-V Virtual Switch:

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
  tenant Tenant_VMM
    application Web
      epg intraEPGDeny
        bridge-domain member VMM_BD
        microsoft-domain member domain1 encap vlan-2003 primary-encap vlan-2004
        microsoft-domain member domain2
          exit
        isolation enforce
        exit
      exit
    exit
apic1(config-tenant-app-epg)#
```

Step 2 Verify the configuration:

Example:

```
 show epg StaticEPG detail
Application EPg Data:
Tenant              : Test_Isolation
Application         : PVLAN
AEPg                : StaticEPG
BD                  : VMM_BD
uSeg EPG            : no
Intra EPG Isolation : enforced
Vlan Domains        : VMM
Consumed Contracts  : VMware_vDS-Ext
Provided Contracts  : default,Isolate_EPG
Denied Contracts    :
Qos Class           : unspecified
Tag List            :
VMM Domains:
Domain                Type       Deployment Immediacy  Resolution Immediacy  State
   Encap       Primary
Encap
 --------------------  ---------  --------------------  --------------------  --------------
  ----------  ----------
 DVS1                  VMware     On Demand             immediate             formed
    auto        auto

Static Leaves:
 Node        Encap             Deployment Immediacy  Mode                Modification Time
```

```
----------  ----------------  --------------------  ------------------
------------------------------

Static Paths:
 Node        Interface                       Encap             Modification Time

 ----------  ------------------------------  ----------------  ------------------------------

 1018        eth101/1/1                      vlan-100          2016-02-11T18:39:02.337-08:00

 1019        eth1/16                         vlan-101          2016-02-11T18:39:02.337-08:00


Static Endpoints:
 Node        Interface          Encap             End Point MAC      End Point IP Address
         Modification Time
 ----------  ------------------------------  ----------------  ------------------
------------------------------  --------------------------------

Dynamic Endpoints:
Encap: (P):Primary VLAN, (S):Secondary VLAN
 Node        Interface            Encap             End Point MAC      End Point IP Address
         Modification Time
 ----------  ------------------------------  ----------------  ------------------
------------------------------  --------------------------------
1017        eth1/3               vlan-943(P)       00:50:56:B3:64:C4  ---
      2016-02-17T18:35:32.224-08:00
                                 vlan-944(S)
```

Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the REST API

Procedure

Step 1 Send this HTTP POST message to deploy the application using the XML API.

Example:

```
POST https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml
```

Step 2 For a VMware VDS or Microsoft Hyper-V Virtual Switch deployment, include one of the following XML structures in the body of the POST message.

Example:

The following example is for VMware VDS:

```
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
          <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
          <fvRsBd tnFvBDName="bd" />
          <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
          <fvRsDomAtt encap="vlan-2001" instrImedcy="lazy" primaryEncap="vlan-2002"
resImedcy="immediate" tDn="uni/vmmp-VMware/dom-DVS1”>
```

```
    </fvAEPg>
 </fvAp>
</fvTenant>
```

Example:

The following example is for Microsoft Hyper-V Virtual Switch:

```
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
          <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
          <fvRsBd tnFvBDName="bd" />
         <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
       <fvRsDomAtt tDn="uni/vmmp-Microsoft/dom-domain1”>
 <fvRsDomAtt encap="vlan-2004" instrImedcy="lazy" primaryEncap="vlan-2003"
 resImedcy="immediate" tDn="uni/vmmp-Microsoft/dom-domain2”>
   </fvAEPg>
 </fvAp>
</fvTenant>
```

Intra-EPG Isolation Enforcement for Cisco AVS

By default, endpoints with an EPG can communicate with each other without any contracts in place. However, you can isolate endpoints within an EPG from each other. In some instances, you might want to enforce endpoint isolation within an EPG to prevent a VM with a virus or other problem from affecting other VMs in the EPG.

You can configure isolation on all or none of the endpoints within an application EPG; you cannot configure isolation on some endpoints but not on others.

Isolating endpoints within an EPG does not affect any contracts that enable the endpoints to communicate with endpoints in another EPG.

Isolating endpoints within an EPG will trigger a fault when the EPG is associated with Cisco AVS domains in VLAN mode.

Note Using intra-EPG isolation on a Cisco AVS microsegment (uSeg) EPG is not currently supported. Communication is possible between two endpoints that reside in separate uSeg EPGs if either has intra-EPG isolation enforced, regardless of any contract that exists between the two EPGs.

Configuring Intra-EPG Isolation for Cisco AVS Using the GUI

Follow this procedure to create an EPG in which the endpoints of the EPG are isolated from each other.

The port that the EPG uses must belong to one of the VM Managers (VMMs).

Note This procedure assumes that you want to isolate endpoints within an EPG when you create the EPG. If you want to isolate endpoints within an existing EPG, select the EPG in Cisco APIC, and in the **Properties** pane, in the **Intra EPG Isolation** area, choose **Enforced**, and then click **SUBMIT**.

Before you begin

Make sure that Cisco AVS is in VXLAN mode.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Tenants**, expand the folder for the tenant, and then expand the **Application Profiles** folder.

Step 3 Right-click an application profile, and choose **Create Application EPG**.

Step 4 In the **Create Application EPG** dialog box, complete the following actions:

a) In the **Name** field, enter the EPG name.
b) In the **Intra EPG Isolation** area, click **Enforced**.
c) From the **Bridge Domain** drop-down list, choose the bridge domain.
d) Check the **Associate to VM Domain Profiles** check box.
e) Click **Next**.
f) In the **Associate VM Domain Profiles** area, click the plus icon, and from the **Domain Profile** drop-down list, choose the desired VMM domain.
g) Click **Update** and click **FINISH**.

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choosing Statistics to View for Isolated Endpoints on Cisco AVS and Viewing Statistics for Isolated Endpoints on Cisco AVS in this guide.

Configuring Intra-EPG Isolation for Cisco AVS Using the NX-OS Style CLI

Before you begin

Make sure that Cisco AVS is in VXLAN mode.

Procedure

In the CLI, create an intra-EPG isolation EPG:

Example:

```
# Command: show running-config
tenant TENANT1
  application APP1
```

```
    epg EPG1
      bridge-domain member VMM_BD
      vmware-domain member VMMDOM1
      isolation enforce <---- This enables EPG into isolation mode.
      exit
   exit
exit
```

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choosing Statistics to View for Isolated Endpoints on Cisco AVS and Viewing Statistics for Isolated Endpoints on Cisco AVS in this guide.

Configuring Intra-EPG Isolation for Cisco AVS Using the REST API

Before you begin

Make sure that Cisco AVS is in VXLAN mode.

Procedure

Step 1 Send this HTTP POST message to deploy the application using the XML API.

Example:

```
   POST
https://192.0.20.123/api/mo/uni/tn-ExampleCorp.xml
```

Step 2 For a VMM deployment, include the XML structure in the following example in the body of the POST message.

Example:

```
Example:
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd" />
      <fvRsDomAtt encap="vlan-2001" tDn="uni/vmmp-VMware/dom-DVS1”>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choosing Statistics to View for Isolated Endpoints on Cisco AVS and Viewing Statistics for Isolated Endpoints on Cisco AVS in this guide.

Choosing Statistics to View for Isolated Endpoints on Cisco AVS

If you configured intra-EPG isolation on a Cisco AVS, you need to choose statistics—such as denied connections, received packets, or transmitted multicast packets—for the endpoints before you can view them.

Procedure

Step 1 Log into Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the tenant navigation pane, choose **Application Profiles** > ***profile*** > **Application EPGs**, and then choose the EPG containing the endpoint the statistics for which you want to view.

Step 4 In the EPG **Properties** work pane, click the **Operational** tab to display the endpoints in the EPG.

Step 5 Double-click the endpoint.

Step 6 In the **Properties** dialog box for the endpoint, click the **Stats** tab and then click the check icon.

Step 7 In the **Select Stats** dialog box, in the **Available** pane, choose the statistics that you want to view for the endpoint and then use the right-pointing arrow to move them into the **Selected** pane.

Step 8 Click **SUBMIT**.

Viewing Statistics for Isolated Endpoints on Cisco AVS

If you configured intra-EPG isolation on a Cisco AVS, once you have chosen statistics for the endpoints, you can view them.

Before you begin

You must have chosen statistics to view for isolated endpoints. See "Choosing Statistics to View for Isolated Endpoints for Cisco AVS" in this guide for instructions.

Procedure

Step 1 Log into Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the tenant navigation pane, choose **Application Profiles** > ***profile*** > **Application EPGs**, and then choose the EPG containing the endpoint the statistics for which you want to view.

Step 4 In the EPG **Properties** work pane, click the **Stats** tab to display the statistics for the EPG.

The central pane displays the statistics that you chose earlier. You can change the view by clicking the table view or chart view icon on the upper right side of the work pane.

Intra-EPG Isolation Enforcement for Cisco ACI Virtual Edge

By default, endpoints with an EPG can communicate with each other without any contracts in place. However, you can isolate endpoints within an EPG from each other. For example, you may want to enforce endpoint isolation within an EPG to prevent a VM with a virus or other problem from affecting other VMs in the EPG.

You can configure isolation on all or none of the endpoints within an application EPG; you cannot configure isolation on some endpoints but not on others.

Isolating endpoints within an EPG does not affect any contracts that enable the endpoints to communicate with endpoints in another EPG.

Note Enforcing intra-EPG Isolation is not supported for the EPG that is associated with Cisco ACI Virtual Edge domains in VLAN mode. If you try to enforce intra-EPG isolation with such an EPG, a fault is triggered.

Note Using intra-EPG isolation on a Cisco ACI Virtual Edge microsegment (uSeg) EPG is not currently supported.

Note Proxy ARP is not supported for Cisco ACI Virtual Edge EPGs using VXLAN encapsulation and on which intra-EPG Isolation is enforced. Therefore, intra-subnet communication is not possible between intra-EPG isolated EPGs even though contracts are in place between those Cisco ACI Virtual Edge EPGs. (VXLAN).

Configure Intra-EPG Isolation for Cisco ACI Virtual Edge Using the GUI

Follow this procedure to create an EPG in which the endpoints of the EPG are isolated from each other.

The port that the EPG uses must belong to one of the VM Managers (VMMs).

Note This procedure assumes that you want to isolate endpoints within an EPG when you create the EPG. If you want to isolate endpoints within an existing EPG, select the EPG in Cisco APIC, and in the **Properties** pane, in the **Intra EPG Isolation** area, choose **Enforced**, and then click **SUBMIT**.

Before you begin

Make sure that VXLAN-related configuration is present on the Cisco ACI Virtual Edge VMM domain, particularly a Cisco ACI Virtual Edge fabric-wide multicast address and pool of multicast addresses (one per EPG).

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Tenants**, expand the folder for the tenant, and then expand the **Application Profiles** folder.

Step 3 Right-click an application profile, and choose **Create Application EPG**.

Step 4 In the **Create Application EPG** dialog box, complete the following steps:

a) In the **Name** field, enter the EPG name.

b) In the **Intra EPG Isolation** area, click **Enforced**.

c) From the **Bridge Domain** drop-down list, choose the bridge domain.

d) Check the **Associate to VM Domain Profiles** check box.

e) Click **Next**.

f) In the **Associate VM Domain Profiles** area, complete the following steps:

- Click the + (plus) icon, and from the **Domain Profile** drop-down list, choose the desired Cisco ACI Virtual Edge VMM domain.
- From the **Switching Mode** drop-down list, choose **AVE**.
- From the **Encap Mode** drop-down list, choose **VXLAN** or **Auto**.

  If you choose **Auto**, make sure that encapsulation mode of the Cisco ACI Virtual Edge VMM domain is VXLAN.
- (Optional) Choose other configuration options appropriate to your setup.

g) Click **Update** and click **Finish**.

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 13 and View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 14 in this guide.

Configure Intra-EPG Isolation for Cisco ACI Virtual Edge Using the NX-OS Style CLI

Before you begin

Make sure that VXLAN-related configuration is present on the Cisco ACI Virtual Edge VMM domain, particularly a Cisco ACI Virtual Edge fabric-wide multicast address and pool of multicast addresses (one per EPG).

Procedure

In the CLI, create an intra-EPG isolation EPG:

Example:

```
# Command: show running-config tenant Tenant2 application AP-1 epg EPG-61
  tenant Tenant2
    application AP-1
      epg EPG-61
```

```
        bridge-domain member BD-61
        vmware-domain member D-AVE-SITE-2-3
          switching-mode AVE
          encap-mode vxlan
          exit
        isolation enforce            # This enables EPG into isolation mode.
        exit
      exit
    exit
```

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 13 and View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 14 in this guide.

Configure Intra-EPG Isolation for Cisco ACI Virtual Edge Using the REST API

Before you begin

Make sure that VXLAN-related configuration is present on the Cisco ACI Virtual Edge VMM domain, particularly a Cisco ACI Virtual Edge fabric-wide multicast address and pool of multicast addresses (one per EPG).

Procedure

Step 1 Send this HTTP POST message to deploy the application using the XML API.

Example:

```
   POST
https://10.197.139.36/api/mo/uni/tn-Tenant2.xml
```

Step 2 For a VMM deployment, include the XML structure in the following example in the body of the POST message.

Example:

```
<fvTenant name="Tenant2" >
  <fvAp name="AP-1">
    <fvAEPg name="EPG-61" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <!-- pcEnfPref="unenforced" DISABLES ISOLATION-->
        <fvRsBd tnFvBDName="BD-61" />
        <fvRsDomAtt switchingMode="AVE" encapMode="vxlan" resImedcy="immediate"
tDn="uni/vmmp-VMware/dom-D-AVE-SITE-1-XXIII" >
        </fvRsDomAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 13 and View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 14 in this guide.

Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, choose statistics—such as denied connections, received packets, or transmitted multicast packets—for the endpoints. You can then view the statistics.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the tenant navigation pane, expand the **Application Profiles**, ***profile***, and **Application EPGs** folders, and then choose the EPG containing the endpoint the statistics for which you want to view.

Step 4 In the EPG **Properties** work pane, click the **Operational** tab to display the endpoints in the EPG.

Step 5 Double-click the endpoint.

Step 6 In the **Properties** dialog box for the endpoint, click the **Stats** tab and then click the check icon.

Step 7 In the **Select Stats** dialog box, in the **Available** pane, choose the statistics that you want to view for the endpoint, and then use the right-pointing arrow to move them into the **Selected** pane.

Step 8 Click **Submit**.

Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Virtual Networking Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, choose statistics—such as denied connections, received packets, or transmitted multicast packets—for the endpoints. You can then view the statistics.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM domain*** > **Controllers** > ***controller instance name*** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)*** > **.**

Step 3 Click the **Stats** tab.

Step 4 Click the tab with the check mark.

Step 5 In the **Select Stats** dialog box, click the statistics that you want to view in the **Available** pane, and then click the arrow pointing right to put them in the **Selected** pane.

Step 6 (Optional) Choose a sampling interval.

Step 7 Click **Submit**.

View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, once you have chosen statistics for the endpoints, you can view them.

Before you begin

You must have chosen statistics to view for isolated endpoints. See Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 13 in this guide for instructions.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the tenant navigation pane, expand the **Application Profiles**, ***profile***, and **Application EPGs** folders, and then choose the EPG containing the endpoint with statistics that you want to view.

Step 4 In the EPG **Properties** work pane, click the **Operational** tab to display the endpoints in the EPG.

Step 5 Double-click the endpoint with statistics that you want to view.

Step 6 In the **Properties** work pane for the endpoint, click the **Stats** tab.

The work pane displays the statistics that you chose earlier. You can change the view by clicking the table view or chart view icon on the upper left side of the work pane.

View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Virtual Networking Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, once you have chosen statistics for the endpoints, you can view them.

Before you begin

You must have chosen statistics to view for isolated endpoints. See Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 13 in this guide for instructions.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM name*** > **Controllers** > **controller instance name** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)***

Step 3 Click the **Stats** tab.

The central pane displays the statistics that you chose earlier. You can change the view by clicking the table view or chart view icon on the upper left side of the work pane.