Cisco ACI vCenter Plugin

This chapter contains the following sections:

- About Cisco ACI with VMware vSphere Web Client, page 1
- Getting Started with Cisco ACI vCenter Plugin, page 2
- Cisco ACI vCenter Plugin Features and Limitations, page 7
- Cisco ACI vCenter Plugin GUI, page 12
- Performing ACI Object Configurations, page 19
- Uninstalling the Cisco ACI with VMware vSphere Web Client, page 28
- Upgrading the Cisco ACI with VMware vSphere Web Client, page 29
- Troubleshooting the Cisco ACI vCenter Plugin Installation, page 29
- Reference Information, page 30

About Cisco ACI with VMware vSphere Web Client

The Cisco ACI vCenter plugin is a user interface that allows you to manage the ACI fabric from within the vSphere Web client.

This allows the VMware vSphere Web Client to become a single pane of glass to configure both VMware vCenter and the ACI fabric.

The Cisco ACI vCenter Plugin empowers virtualization administrators to define network connectivity independently of the networking team while sharing the same infrastructure.

No configuration of "in-depth" networking is done through the Cisco ACI vCenter Plugin. Only the elements that are relevant to virtualization administrators are exposed.

Cisco ACI vCenter Plugin Overview

The Cisco Application Centric Infrastructure (ACI) vCenter Plugin for the VMware vSphere Web Client, adds a new view to the GUI called Cisco ACI Fabric.
The Cisco Application Centric Infrastructure (ACI) vCenter Plugin does not change existing integration of ACI with vCenter, it allows you to configure an EPG, uSeg EPG, contract, tenant, VRF, and bridge domain from the VMware vSphere Web Client.

Cisco Application Centric Infrastructure (ACI) vCenter Plugin is stateless, fetches everything from Application Policy Infrastructure Controller (APIC) and does not store any information.

The following is a brief overview of the features provided by Cisco ACI vCenter Plugin:

For more detailed information, see Cisco ACI vCenter Plugin Features and Limitations, on page 7.

The Cisco ACI vCenter Plugin provides the possibility to create, read, update and delete (CRUD) the following object on the ACI Fabric:

- Tenant
- Application Profile
- EPG / uSeg EPG
- Contract
- VRF
- Bridge Domain

The Cisco ACI vCenter Plugin also provides a more limited operation regarding the usage of L2 and L3 Out, where all of the advanced configuration needs to be done in APIC beforehand.

- Pre-configured L2 and L3 Out can be used as providers or consumers of a contract.
- Cannot be created, edited or deleted.

The Cisco ACI vCenter Plugin also allows to consume pre-configured L4-L7 Services, by applying existing graph template to a Contract.

- Can use existing graph templates, not create them.
- Only empty mandatory parameter of the function profile will be displayed and configurable.

The Cisco ACI vCenter Plugin also has troubleshooting capabilities:

- Endpoint to Endpoint sessions (Faults, Audits, Events, Stats, Contract, Traceroute )

---

**Getting Started with Cisco ACI vCenter Plugin**

**Cisco ACI vCenter Plugin Software Requirements**

The Cisco ACI vCenter Plugin Software Requirements:
<table>
<thead>
<tr>
<th>Platform Series</th>
<th>Recommended Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>• 5.5 Linux Appliance</td>
</tr>
<tr>
<td></td>
<td>• 5.5 Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>• 6.0 Linux Appliance</td>
</tr>
<tr>
<td></td>
<td>• 6.0 Windows Server 2008</td>
</tr>
<tr>
<td>Application Policy Infrastructure Controller (APIC)</td>
<td>Release 2.1(1)</td>
</tr>
</tbody>
</table>

**Required APIC Configuration**

This section describes the required APIC configuration.

At least one VMM domain should already exists between the APIC and the vCenter where the plugin is being installed.

For more information, see the *Cisco Application Centric Infrastructure Fundamentals Guide*.

**Installing the Cisco ACI vCenter Plugin**

This section describes how to install the Cisco ACI vCenter Plugin. You must have working HTTPS traffic between your vCenter and APIC, as the vCenter will be downloading the plugin directly from the APIC.

If you cannot enable HTTPS traffic between your vCenter and APIC, and you wish to use your own web server to host the Cisco ACI vCenter Plugin zip file, see the Alternative Installation of the Cisco ACI vCenter Plugin, on page 30.

If you are using vCenter 5.5 (Update 3e or later) or vCenter 6.0 (Update 2 or later), follow the procedure in this section. If you are using an earlier release of vCenter 5.5 or 6.0, see the Alternative Installation of the Cisco ACI vCenter Plugin, on page 30.

To install a plugin, the vCenter must download the plugin from a Web Server. In the following procedure, the APIC is used as the Web Server, and the vCenter downloads the plugin directly from the APIC.

Prior to vCenter 5.5 Update 3e or vCenter 6.0 Update 2, vCenter uses TLSv1 for the HTTPS communication, which is now obsolete. For security reasons APIC only supports TLSv1.1 and TLSv1.2, therefore the vCenter will not be able to download the plugin from the APIC. The plugin must be put on a separate Web server, that allows TLSv1 or that does not use HTTPS.

**Before You Begin**

- Make sure all of the prerequisites are met.
  
  For more information, see the Cisco ACI vCenter Plugin Software Requirements, on page 2 and Required APIC Configuration, on page 3 sections.

- Ensure HTTPS traffic is allowed between your vCenter server and APIC.
Procedure

Step 1  Go to the following URL:

Example:
https://<API>/vcplugin

Step 2  Follow the instructions on that web page.

Connecting vCenter Plugin to your ACI Fabric

This section describes how to connect the vCenter plugin to your ACI fabric.

Note

• The registration is vCenter wide and it does not take into account the user that performs it. It is a configuration for the whole vCenter, not just for the logged in user that performs it.

• Role Based Access Control (RBAC) is based on the credentials used upon registration. Permission of the APIC account used for the registration defines configuration restriction on the vCenter Plugin.

You can connect the vCenter plugin to your ACI fabric, using one of the following ways:

| Connect the vCenter Plugin to your ACI fabric using credentials. | For more information, see Connecting vCenter Plugin to your ACI Fabric Using Credentials, on page 4. |
| Connect the vCenter Plugin to your ACI fabric using an existing certificate. | For more information, see Connecting vCenter Plugin to your ACI Fabric Using an Existing Certificate, on page 5. |
| Connect the vCenter Plugin to your ACI fabric by creating a new certificate. | For more information, see Connecting vCenter Plugin to your ACI Fabric by Creating a New Certificate, on page 6. |

Connecting vCenter Plugin to your ACI Fabric Using Credentials

This section describes how to connect vCenter Plugin to your ACI fabric using credentials.

Before You Begin

Ensure the Cisco ACI vCenter Plugin is installed. For more information, see Installing the Cisco ACI vCenter Plugin, on page 3.
**Procedure**

**Step 1** Log into the VMware vSphere Web Client.

**Step 2** In the Navigator pane, choose **Cisco ACI Fabric**.

**Step 3** In the Getting Started pane, choose **Connect vSphere to your ACI Fabric**.

**Step 4** In the Register a new ACI Fabric dialog box, click **Yes** to register a new ACI fabric.

**Step 5** In the Register a new APIC Node dialog box, perform the following actions:
   a) In the IP/FQDN field, enter the IP address or the fully qualified domain name (FQDN).
   b) In the Use Certificate field, do not put a check in the Use Certificate check box to use APIC authentication.
   c) In the Username field, enter the user name (admin).
   d) In the Password field, enter the password.
   e) Click **OK**.

**Step 6** In the Information dialog box, click **OK**.
   The APIC node was successfully added to the ACI fabric.

**Step 7** In the ACI Fabric pane, you will see the new registered APIC discover the other APICs. The Cisco ACI vCenter Plugin always uses a single APIC for its requests. It will however switch the APIC, if the APIC currently used is no longer available.

---

**Connecting vCenter Plugin to your ACI Fabric Using an Existing Certificate**

This section describes how to connect the vCenter plugin to your ACI fabric using an existing certificate.

**Before You Begin**

- A certificate is already setup on the APIC for the admin user.
- You have the name and private key of the certificate.

**Procedure**

**Step 1** Log in to the VMware vSphere Web Client.

**Step 2** In the Navigator pane, choose **Cisco ACI Fabric**.

**Step 3** In the Getting Started pane, choose **Connect vSphere to your ACI Fabric**.

**Step 4** In the Register a new ACI Fabric dialog box, click **Yes** to register a new ACI fabric.

**Step 5** In the Register a new APIC Node dialog box, perform the following actions:
   a) In the IP/FQDN field, enter the IP address or the fully qualified domain name (FQDN).
   b) In the Use Certificate field, check the Use Certificate check box.

**Step 6** In the Action section, choose **Use an existing certificate**.

**Step 7** In the Name field, enter the certificate name.

**Step 8** In the Private Key section, paste the private key of the certificate.

**Step 9** Click **Check Certificate**.
The status switches to Connection Success.

Note If connection failure is displayed, check that the certificate name and private key are correct, and try again.

Step 10 Click OK.
Step 11 In the Information dialog box, click OK.  
The APIC node was successfully added to the ACI fabric.
Step 12 In the ACI Fabric pane the newly registered APIC discovers the other APICs.  
The Cisco ACI vCenter Plugin always uses a single APIC for its requests. If the currently used APIC is no longer available, the Cisco ACI vCenter Plugin switches APICs.

Connecting vCenter Plugin to your ACI Fabric by Creating a New Certificate

This section describes how to connect the vCenter plugin to your ACI fabric by creating a new certificate.

Before You Begin

• Ensure the plugin is installed.
• You have access to the APIC admin credentials.

Procedure

Step 1 Log into the VMware vSphere Web Client.
Step 2 In the Navigator pane, choose Cisco ACI Fabric.
Step 3 In the Getting Started pane, choose Connect vSphere to your ACI Fabric.
Step 4 In the Register a new ACI Fabric dialog box, click Yes to register a new ACI fabric.
Step 5 In the Register a new APIC Node dialog box, perform the following actions:
   a) In the IP/FQDN field, enter the IP address or the fully qualified domain name (FQDN).
   b) In the Use Certificate field, check the Use Certificate check box.
Step 6 In the Action field, choose Generate a new certificate.
Step 7 In the Name field, enter the new certificate name.
Step 8 Click the Generate certificate button.
Step 9 Copy the displayed certificate.  
From -----BEGIN CERTIFICATE----- included, to -----END CERTIFICATE----- included.
Step 10 Add this certificate to the admin user in APIC. Make sure to use the same certificate name.  
a) Log into the APIC GUI as admin.
   b) On the menu bar, choose Admin.
   c) In the Navigation pane, expand Security Management > Local Users > admin.
   d) In the Work pane, in the User Certificate section, click the plus icon to add the certificate.
   e) In the Name field, enter the certificate name.
   f) In the Data field, paste the certificate content that you copied in step 8.
g) Click Submit.

**Step 11** In the vCenter Plugin, click Check Certificate.  
The status changes to Connection Success.

**Note** If a Connection Failure message displays, check that the certificate is correctly added on the APIC  
and that the certificate names are the same.

**Step 12** Click OK.  
**Step 13** In the Information dialog box, click OK.  
The APIC node is successfully added to the ACI fabric.

**Step 14** In the ACI Fabric pane, the newly registered APIC discovers the other APICs.  
The Cisco ACI vCenter Plugin always uses a single APIC for its requests. If the currently used APIC is no  
longer available, the Cisco ACI vCenter Plugin switches APICs.

---

**Cisco ACI vCenter Plugin Features and Limitations**

This section describes the possible operations provided by the Cisco ACI vCenter plugin, for all object types  
it manages. It also goes over intentional configuration limitations.

For more information about the objects, see the *Cisco Application Centric Infrastructure Fundamentals Guide*.

**Tenants**

The Cisco ACI vCenter Plugin allows CRUD operations on the Tenant object. The following attributes are  
exposed in the plugin:

- Name: The name of the tenant.
- Description (Optional): The description of the tenant.

When a tenant is created by the plugin, a VRF `<tenant_name>_default` and a Bridge Domain  
`<tenant_name>_default` connected to that VRF are automatically created inside. An Application Profile  
`<tenant_name>_default` is also created inside it.

The infrastructure Tenant (infra) and the management Tenant (mgmt) are not exposed in the plugin.

**Note** The tenants visible in the plugin will also depends on the permissions associated with the account used  
while registering the ACI fabric into the plugin.

**Application Profiles**

The Cisco ACI vCenter Plugin allows CRUD operations on the Application Profile objects. The following  
attributes are exposed in the plugin:

- Name: The name of the Application Profile.
- Description (Optional): The description of the Application Profile.
Endpoint Groups

The Cisco ACI vCenter Plugin allows CRUD operations on the Endpoint Group objects. The following attributes are exposed in the plugin:

- Name: The name of the Endpoint Group.
- Description (Optional): The description of the Endpoint Group.
- Bridge Domain: The Bridge Domain associated with this Endpoint Group.
- Intra-EPG Isolation: This allows to deny all traffic between the virtual machines that are connected to an EPG. By default, all virtual machines in the same EPG can talk to each other.
- Distributed Switch: The DVS/AVS where the EPG is deployed. This correspond to the association with a VMM domain in ACI.

By default, all EPGs created with the plugin are associated with the VMM Domain pointing to the vCenter where the plugin is used. If there are multiple VMM Domains pointing to the same vCenter, you must choose at least one, in the form of selected on which DVS to deploy the EPG.

Allow micro-segmentation (only for DVS, not AVS): This allows you to create a "Base EPG". All the virtual machines connected to this EPG are candidates to apply micro-segmentation rules of a uSeg EPG. Micro-segmented EPG rules only applies to virtual machine that are connected to a "Base EPG".

Note

All EPGs are considered as base EPGs if the distributed switch is AVS.

An EPG linked to a VMM domain pointing to the vCenter where the plugin is being used is displayed as "Virtual." Other EPGs are displayed as "Physical."

Update and Delete actions are only authorized for EPGs linked to a VMM domain that is pointing to the vCenter (Virtual). Others EPGs (Physical) are read-only. Updates are still authorized to make EPGs consume or provide contracts, regardless of their VMM domain.

uSeg EPGs

The Cisco ACI vCenter Plugin allows CRUD operations on the micro-segemented EPG objects. The following attributes are exposed in the plugin:

- Name: The name of the micro-segemented EPG.
- Description (Optional): The description of the micro-segemented EPG.
- Bridge Domain: The Bridge Domain associated with this micro-segemented EPG.
- Intra-EPG Isolation: This allows to deny all traffic between the virtual machines that are connected to an EPG. By default, all virtual machines in the same EPG can talk to each other.
- Distributed Switch: The DVS/AVS where the EPG is deployed. This correspond to the association with a VMM domain in ACI.

By default, all EPGs created with the plugin are associated with the VMM Domain pointing to the vCenter where the plugin is used. If there are multiple VMM Domains pointing to the same vCenter, you must choose at least one, in the form of selected on which DVS to deploy the EPG.

- Micro-segmentation attributes: List of rules that decide which VM belongs to this micro-segemented EPG. Rules options include: IP, MAC, VM name, OS, Host, VM id, VNIC, Domain, Data Center, Custom Attribute.
Domain attributes (VMM Domain) only allow you to select VMM domains to the local vCenter. You choose a domain by selecting the corresponding DVS/AVS.

Custom attributes can only be chosen. They cannot be set by the plugin. They must be set by the VMware vSphere Client. To create custom labels, see: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005720

**Note**

**L2 and L3 External Networks**

Layer 2 and Layer 3 External Networks must be created and configured on the APIC by the network administrator. They are read-only on the vCenter Plugin.

The only plugin operations permitted on these objects are to make them consume or provide contracts.

The visible information for an L3 External Network is:

- **Name:** The name of the L3 External Network
- **Subnets:** External subnets represented by this L3 external network
- **VRF:** The VRF this L3 External Network belongs to
- **Connected Bridge Domains:** The Bridge Domains connected to this L3 External Network

The visible information for an L2 External Network is:

- **Name:** The name of the L2 External Network
- **Bridge Domain:** The bridge domain associated with this Bridge Domain
- **VLAN ID:** The VLAN ID associated with this L2 External Network

**VRF**

The Cisco ACI vCenter Plugin allows CRUD operations on the VRF objects. The following attributes are exposed in the plugin:

- **Name:** The name of the VRF
- **Description (Optional):** The description of the VRF
- **Enforce policies:** Determine if the contracts need to be enforced for the EPG in this VRF.

**Bridge Domains**

The Cisco ACI vCenter Plugin allows CRUD operations on the Bridge Domain objects. The following attributes are exposed in the plugin:

- **Name:** The name of the Bridge Domain
- **Description (Optional):** The description of the Bridge Domain
- **Private Subnets:** List of gateways for this Bridge Domain.
Note

• Shared and advertised subnets are read only. They cannot be configured by the plugin. Only the private subnets can be added or deleted.
• If the Bridge Domain has been connected to an L3/L2 Out by the APIC, it cannot be deleted.

Contracts

The Cisco ACI vCenter Plugin allows CRUD operations on the Contract objects. The following attributes are exposed in the plugin:

• Name: The name of the contract
• Description (Optional): The description of the contract.
• Consumers: The consumers for the contract (EPG, uSeg EPGs, L2/L3 External Networks)
• Providers: The providers for the contract (EPG, uSeg EPGs, L2/L3 External Networks)
• Filters: List of filters associated with the contract
• Apply both direction: Indicate if the specified Filters are applying only from consumers to providers or also from providers to consumers.
• L4-L7 Graph Template: It is possible to associate existing graph template to a Contract. See L4-L7 Service section below.

Note

• Subject is not exposed. The plugin only manages contracts with a single subject. Contracts with multiple subjects are seen, but not editable.
• If the consumer and the contract are not in the same tenant, a contract interface is automatically created (named to _Tenant-name_contract-name).

Filters

The Cisco ACI vCenter Plugin allows CRUD operations on the Filter objects. All parameters from the APIC are exposed.

L4-L7 Services

• L4-L7 services can only be added on contracts that have a single provider.
• The graph template cannot be created by the plugin (only consume existing graph templates)
  • The graph template must be configured so that it contains:
    • Association with devices
    • Association with a function profile
  • Only support graph templates with a maximum of two nodes
The Function Profile folders naming and hierarchy must be valid as the plugin does not allow folder manipulation.

- Only empty mandatory parameters of the function profile are editable by the plugin.

Graph connectors can be configured.

- All parameters from the APIC are exposed
- You can only consume redirect policies, if needed, not create them

Troubleshooting

- Only endpoint to endpoint troubleshooting sessions are supported.

  - You can choose an existing session or create a new one
  - The physical topology (spine / leaf) is not displayed.
  - The topology display is VM-centric, focusing on Host, VM, vNIC, and the EPG the vNICs connect to

- Available information in a session:

  - Faults
  - Contracts: A table listing all the Contract/Filters/Entries between the two EPGs (hit counts are not displayed)
  - Drop/Stats
  - Audits/Events
  - Traceroute

- Atomic Counter and SPAN are not available

- A more basic troubleshooting tool is available between objects that are not endpoints (VM, EPG, L3 Out), that only display configured contracts between two selected objects.

- A view of VMs and their connection to EPGs is available.

  - For a given VM, it is possible to view the EPGs to which its vNICs are connected.

- If a L4-L7 connector is used as source or destination of a troubleshooting session, then it is expected to get the following error on the Contract section of the troubleshooting wizard:

  The feature required the source and destination endpoint to both be part on an EPG.

  You can safely ignore the error message.
Cisco ACI vCenter Plugin GUI

Cisco ACI vCenter Plugin GUI Architecture Overview

This section describes the Cisco ACI vCenter Plugin GUI architecture Overview.

Main Menu

*Figure 1: Main Menu*
### Cisco ACI vCenter Plug-in Overview

This section describes the Cisco ACI vCenter plug-in GUI overview.

#### Note

All of the times for faults, stats, event and audits are shown in the local timezone of the browser. If the APIC’s time zone does not match the time zone of your system, the time stamp can have a different time zone.

#### Home

In the VMware vSphere Web Client, in the Navigation pane, choose Home. In the Work pane displays the following tabs:

- **Getting Started**

  The bottom of the Getting Started pane enables you to do the following things:

  - Click Create a new Tenant to create a new tenant.
  - Click Create a new Application Profile to create a new application profile.
• Click **Create a new Endpoint Group** to create a new endpoint group.

• Click the **Cisco Application Centric Infrastructure (ACI)** link to explore the ACI website.

**About** tab

The **About** pane displays the Cisco ACI vCenter plug-in version.

**ACI Fabric**

In the VMware vSphere Web Client, in the **Navigator** pane, choose **Cisco ACI Fabric**. In the **Work** pane displays the following tabs:

• **ACI Fabric** tab

The **ACI Fabric** pane enables you to do the following things:

• Click **Register a new ACI Fabric / ACI Node** to register a new ACI fabric or ACI node.

• View information about the current APIC states of the fabric.

---

**Note**

When the plug-in detects APIC as unavailable, it stops trying to connect to it and will not update its status anymore. To avoid having to wait for the timeout that comes with trying to connect to an unresponsive APIC. Click **Reload** to refresh the APIC state. This forces it to try to reconnect to each APIC, even to the unavailable ones. This updates their status, if they are available again.

• **Tenants** tab

The **Tenants** pane enables you to do the following things:

• Manage the different tenants present in the registered ACI Fabrics.

• Click **Create a new Tenant** to create a new tenant.

• View the different tenants.

If you select a tenant in the table, you can delete a tenant if you click **Delete Tenant <tenant_name>**.
If you select a tenant in the table, you can edit the tenant description if you right-click the `<tenant_name>` and choose Edit settings.

**Figure 2: ACI Fabric - Home**

**Application Profile**

In the VMware vSphere Web Client, in the Navigator pane, choose Cisco ACI Fabric > Application Profile. In the Work pane enables you to do the following things:

- Choose an active tenant and the application profile.
- Click Create a new Application Profile to create a new application profile.
- Use the Drag and drop to configure section to drag and drop the different elements to configure your Application Profiles fully. The elements are:
  - Endpoint Group
  - uSeg
  - L3 External Network
  - L2 External Network
  - Contract
- View the Policy, Traffic Stats, Health, Faults, Audit Logs, and Events by using the tabs.

In the Policy tab, you can switch back to Consumer and Provider view or traffic view.
Networking

In the VMware vSphere Web Client, in the Navigator pane, choose Cisco ACI Fabric > Networking. In the Work pane enables you to do the following things:

- Set up your own addressing for all endpoint groups by creating isolated VRFs that are populated with bridge domains. An endpoint group will be associated with one bridge domain.
- Choose an active tenant.
- Use the Drag and drop to configure section to drag and drop the following elements:
  - VRF
  - Bridge Domain

Note
The available Layer 3 and Layer 2 endpoint groups are displayed here, but are not configurable.

Troubleshooting

In the VMware vSphere Web Client, in the Navigator pane, choose Cisco ACI Fabric > Troubleshooting. In the Work pane displays the following tabs:

- Policy Checker tab
  The Policy Checker tab enables you to select two entities (Virtual Machine, endpoint group, Layer 3 external network or endpoint), and view all of the contracts and Layer 4 to Layer 7 services that are enforced between those 2 entities.

  You can also start a troubleshooting session between two endpoints:
  - Choose the time frame of the session in the From, To and fixed time check box.
  - You can configure the time frame by putting a check in the Fix Time check box.
  - In the Source Destination section, you can choose the source and destination endpoints. Click on Start Troubleshooting session to start a new troubleshooting session.
  - In the Troubleshooting Session, you can inspect faults, configured contracts, event, audits, and traffic stats.
  - You can start a trace route between the two endpoints if you click Traceroute.
  - You can click the icon next to an elements to get details that correspond to the category that you chose in the left pane.
  - You can get a topology that represents, for each endpoint, the corresponding vNIC, VM, and host, and the EPG to which the vNIC is connected.

- Virtual Machines tab
  This view is to visualize if the network interface cards of your virtual machine are connected to any endpoint groups.
  - You can restrict the list by using the search field.
  - You view each of the VMs if the vNICs are connected to an EPG.
You can quickly view if the associated EPG has good health or any faults, and view the tenant and application profile to which it belongs.

Resources

**Network**

In the VMware vSphere Web Client, in the **Navigator** pane, choose **Cisco ACI Fabric > Resources > Network**. In the **Work** pane displays the following tabs:

- **Endpoint Groups** tab
  
  Configure the network infrastructure by creating endpoint groups. Each endpoint group has a corresponding VMware Distributed Port Group where you can connect your virtual machines. You can organize your different endpoint groups into application profiles.

  - Choose an active tenant.
  - Click **Create a new Application Profile** to create a new application profile.
  - Choose an application in the table and click **Create a new Endpoint Group** to create a new endpoint group.
  - View the table to see the application profiles and endpoint groups of an active tenant.
  - Choose an endpoint group to view all of the VMs that are connected to it.

- **VRFs** tab
  
  For all endpoint groups, you can setup your own addressing by creating isolated VRFs that are populated with bridge domains. An endpoint group will be associated with one bridge domain.

  - Choose an active tenant.
  - Click **Create a new VRF** to create a new VRF.
  - Click **Create a new Bridge Domain** to create a new bridge domain.
  - View the table to see the VRFs.

**Security**

In the VMware vSphere Web Client, in the **Navigator** pane, choose **Cisco ACI Fabric > Resources > Security**. In the **Work** pane displays the following tabs:

- **Contracts** tab
  
  Contracts allows you to define security policies between different endpoint groups and security policies between endpoint groups and Layer 3 and Layer 2 external networks.

  - Choose an active tenant.
  - Click **Create a new Contract** to create a new contract.
  - View the table to see the contracts.

- **Filters** tab
Filters are entities that match a given type of traffic (based on protocol, port, etc.). They are used by contracts to define the authorized services between endpoint groups and Layer 3 external networks.

- Choose an active tenant.
- Click **Create a new Filter** to create a new filter.
- View the table to see the filters.

**External Connectivity**

In the VMware vSphere Web Client, in the **Navigator** pane, choose **Cisco ACI Fabric > Resources > External Connectivity**. In the **Work** pane displays the following tabs:

- **L3 External Networks** tab
  Layer 3 external networks are defined by the APIC administrator. You have the possibility to consume the defined networks in your contracts and Layer 4 to Layer 7 services, in order to bring external connectivity to your infrastructure.
  - Choose an active tenant.
  - View the table to see the Layer 3 external networks.

- **L2 External Networks** tab
  Layer 2 external networks are defined by the APIC administrator. You have the possibility to consume the defined networks in your Contracts and Layer 4 to Layer 7 services, in order to bring external connectivity to your infrastructure.
  - Choose an active tenant.
  - View the table to see the Layer 2 external networks.

**L4-7 Services**

In the VMware vSphere Web Client, in the **Navigator** pane, choose **Cisco ACI Fabric > Resources > External Connectivity**. In the **Work** pane displays the following:

- Layer 4 to Layer 7 services enables you to add pre-provisioned firewalls and load balancers between your endpoint groups and Layer 3 external networks.
  - Choose an active tenant.
  - View the table to see the Layer 4 to Layer 7 graph instances currently deployed inside the tenant.

**GUI Tips**

This section provides GUI tips.

- You can right-click on ACI object displayed in tables or in graph, to get associated actions.
- When a Virtual Machine object is displayed inside a table in the vCenter plugin, you can double-click on it to navigate to that Virtual Machine in the vSphere Web Client.
Performing ACI Object Configurations

Creating a New Tenant

This section describes how to create a new tenant.

Before You Begin

Ensure that an ACI fabric is registered. For more information, see Connecting vCenter Plugin to your ACI Fabric Using Credentials, on page 4.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log into the VMware vSphere Web Client.</td>
</tr>
<tr>
<td>2</td>
<td>In the Work pane, choose Cisco ACI Fabric.</td>
</tr>
<tr>
<td>3</td>
<td>In the Navigator pane, choose ACI Fabric.</td>
</tr>
<tr>
<td>4</td>
<td>In the ACI Fabric pane, choose the Tenants tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the Tenants pane, click Create a new Tenant.</td>
</tr>
<tr>
<td>6</td>
<td>In the New Tenant dialog box, perform the following actions:</td>
</tr>
<tr>
<td></td>
<td>a) In the Enter a name for the Tenant field, enter the tenant name.</td>
</tr>
<tr>
<td></td>
<td>b) (Optional) In the Enter a description for the Tenant field, enter the description for the tenant.</td>
</tr>
<tr>
<td></td>
<td>c) Click OK.</td>
</tr>
</tbody>
</table>

Creating a New Application Profile

This section describes how to create a new application profile.

Before You Begin

- Ensure that a tenant has been created.

For more information, see Creating a New Tenant, on page 19.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log into the VMware vSphere Web Client.</td>
</tr>
<tr>
<td>2</td>
<td>In the Work pane, choose Cisco ACI Fabric.</td>
</tr>
<tr>
<td>3</td>
<td>In the Navigator pane, choose Resources &gt; Network.</td>
</tr>
<tr>
<td>4</td>
<td>In the Network pane, under the Endpoint Groups tab, perform the following actions:</td>
</tr>
<tr>
<td></td>
<td>a) From the Tenant drop-down list, choose the tenant name.</td>
</tr>
</tbody>
</table>
b) Click **Create a new Application Profile**.

**Step 5** In the **New Application Profile** dialog box, perform the following actions:

a) In the **Name** field, the application profile name.

b) (Optional) In the **Description** field, enter the description of the application profile name.

c) Click **OK**.

---

## Creating an EPG Using the Drag and Drop Method

This section describes how to create an endpoint group (EPG) using the drag and drop method.

**Before You Begin**

- Ensure that a tenant has been created.
  
  For more information, see Creating a New Tenant, on page 19.

- Ensure that an application profile has been created.
  
  For more information, see Creating a New Application Profile, on page 19.

**Procedure**

**Step 1** Log into the VMware vSphere Web Client.

**Step 2** In the **Navigator** pane, choose **Application Profile**.

**Step 3** In the **Application Profile** pane, perform the following actions:

a) In the **Tenant** field, from the drop-down list, choose a tenant.

b) In the **Application Profile** field, from the drop-down list, choose an application profile.

c) In the **Drag and drop to configure** element area, drag and drop **Endpoint Group**.

**Step 4** In the **New Endpoint Group** dialog box, perform the following actions:

a) In the **Name** field, enter the name of the endpoint group.

b) (Optional) In the **Description** field, enter the description of the EPG.

c) In the **Bridge Domain** field, choose any bridge domain from common or from the tenant where the EPG is created. The default bridge domain is common/default. Click the pen icon to choose another bridge domain.

**Step 5** In the **Distributed Switch** field, perform the following actions:

a) Put a check in at least one distributed switch check box to connect the EPG to the chosen distributed switches.

b) Put a check in the **Allow micro-segmentation** check box to allow micro-segmentation.

The **Allow micro-segmentation** check box only shows if the distributed switch is DVS. If the distributed switch is AVS, then the GUI does not show the **Allow micro-segmentation** check box. All EPGs are considered to be base EPGs if the distributed switch is AVS.

This allows you to create a base EPG. All of the virtual machines that are connected to this EPG are candidates to apply the micro-segmentation rules of a uSeg EPG. Micro-segmented EPG rules only apply to virtual machines that are connected to a base EPG.
c) Put a check in the Intra EPG isolation check box to isolate the EPG. This allows you to deny all traffic between the virtual machines that are connected to this EPG. This rule also applies to machines that are seen under a microsegmented EPG. By default, all virtual machines in the same EPG can talk to each other.

Step 6 Click OK to push the new EPG on APIC. You will see the new EPG that you created in the topology.

Creating a New uSeg EPG Using the Drag and Drop Method

This section describes how to create a new uSeg EPG using the drag and drop method.

Before You Begin

- Ensure that a tenant has been created
  For more information, see Create a New Tenant.
- Ensure that an application profile has been created.
  For more information, see Creating a New Application Profile, on page 19.
- (DVS only, not AVS) Ensure you have created a base EPG, and connected all the VMs that needs to participate in micro-segmentation to that base EPG. For more information, see Creating a new Endpoint Group.

Procedure

**Step 1** Log in to the VMware vSphere Web Client.

**Step 2** In the Navigator pane, choose Application Profile.

**Step 3** In the Application Profile pane, perform the following actions:

a) From the Tenant drop-down list, choose a tenant.

b) From the Application Profile drop-down list, choose an application profile.

c) In the Drag and drop to configure element area, drag and drop the uSeg into the topology.

**Step 4** In the New Endpoint Group dialog box, perform the following actions:

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

b) In the Description field, enter the description of the EPG.

**Step 5** In the Distributed Switch field, choose which distributed switch needs to be associated with that uSeg EPG. 

**Note** If there is only one DVS, no check box is displayed as it is chosen by default.

**Step 6** In the Bridge Domain field, choose any bridge domain from common or from the tenant where the uSeg EPG is created. The default bridge domain is common/default. Click the pen icon to select another bridge domain.

**Step 7** Put a check in the Intra EPG isolation check box to isolate the EPG.

**Step 8** In the Microsegmentation section, click the + icon.

**Step 9** In the New micro-segmentation Attribute dialog box, perform the following actions:
a) In the Name field, enter the name of the new attribute.
b) (Optional) In the Description field, enter the description of the new attribute.
c) In the Type section, choose the type on which to filter.
d) In the Operator section, choose Contains the operator you wish to use.
e) If available, click the Browse button to choose a specific object, instead of manually entering a value.
f) Click OK to add the new attribute to the uSeg EPG.

Step 10 Repeat Step 7 and Step 8 to add other attributes to the uSeg EPG.
Step 11 Click OK.

Creating a Contract Between Two EPGs Using the Drag and Drop Method

This section describes how to create a contract between two endpoint groups (EPGs) using the drag and drop method.

Before You Begin

• Ensure that two EPGs have been created.

For more information, see Creating an EPG Using the Drag and Drop Method, on page 20.

Procedure

Step 1 Log into the VMware vSphere Web Client.
Step 2 In the Work pane, choose Cisco ACI Fabric.
Step 3 In the Navigator pane, choose Application Profile.
Step 4 In the Application Profile pane, perform the following actions:
   a) From the Tenant drop-down list, choose a tenant.
   b) From the Application Profile drop-down list, choose an application profile.
Step 5 In the Drag and drop to configure element area, drag and drop the contract on the source EPG.
Step 6 Click on the destination EPG. An arrow will display, going from the source EPG to the destination EPG.
Step 7 In the New Contract dialog box, perform the following actions:
   a) In the Consumers field, verify that it displays the correct EPG.
   b) In the Providers field, verify that it displays the correct EPG.
   c) In the Name field, enter the name of the contract.
   d) (Optional) In the Description field, enter the description of the contract.
   e) In the Filters field, click the + icon to add filters to the contract.
   f) In the new dialog box, drag and drop all the filters you wish to add to the Contract from the list on the left to the list on the right and click OK.
   g) (Optional) Check the Configure L4-7 service check box to configure Layer 4 to Layer 7 services.
   h) Click OK to create the contract.
Adding an EPG to an Existing Contract Using Drag and Drop Method

This section describes how to add an EPG to an existing contract using the drag and drop method.

Before You Begin

• Ensure that a contract has been created.
• Ensure that an EPG has been created.

For more information, see Creating an EPG Using the Drag and Drop Method, on page 20.
• Ensure that the contract is visible on the Application Profile pane. For example, if another EPG of the Application Profile is already using the contract. If this is not the case, follow the steps of Adding an EPG to an Existing Contract using the Security Tab.

Procedure

Step 1
Log into the VMware vSphere Web Client. In the Navigator pane, choose Application Profile.

Step 2
In the Navigator pane, choose Application Profile.

Step 3
In the Application Profile pane, perform the following actions:
   a) From the Tenant drop-down list, choose a tenant.
   b) From the Application Profile drop-down list, choose an application profile.

Step 4
In the Drag and drop to configure element area, drag and drop the contract, and do one of the following:

• To have the EPG consume the contract:
   1 Drag and drop the Contract on the EPG that needs to consume the contract.
   2 Choose the relevant contract (an arrow is displayed going from the EPG to the contract), and click the contract to make the EPG consume the contract.

• To have the EPG provide the contract:
   1 Drag and drop the Contract on the contract that the EPG needs to provide.
   2 Choose the relevant contract (an arrow is displayed going from the contract to the EPG), and click the Contract to make the EPG provide that contact.

Adding an EPG to an Existing Contract using the Security Tab

Before You Begin

• Ensure that a contract has been created.
• Ensure that an EPG has been created.
For more information, see Creating an EPG Using the Drag and Drop Method, on page 20.

Procedure

Step 1 Log into the VMware vSphere Web Client.
Step 2 In the Navigator pane, choose Resources > Security.
Step 3 From the Tenant drop-down list, choose a tenant.
Step 4 Click on the contract where the EPG needs to be added in the list of contract.
Step 5 Click on the + icon of either the Consumers or Providers columns (to respectively have the EPG consume or provide the contract).
Step 6 From the menu that opens, choose Add Endpoint Groups.
Step 7 In the dialog box, perform the following actions:
   a) Expand the tenant where the EPG is located.
   b) Expand the Application Profile where the EPG is located.
   c) Drag and drop the EPG from the list on the left to the list on the right.
   d) Click OK.

Setting up L3 External Network

This section describes how to connect a Layer 3 external network.

Note
You cannot do any configuration with a Layer 3 external network. You can only set up a Layer 3 external network that exists in APIC.

Before You Begin

- Ensure that a Layer 3 (L3) external network on APIC is configured. For more information, see the ACI Basic Configuration Guide.
- Ensure that an EPG has been created. For more information, see Creating an EPG Using the Drag and Drop Method, on page 20.

Procedure

Step 1 Log in to the VMware vSphere Web Client.
Step 2 In the Navigator pane, choose Application Profile.
Step 3 In the Application Profile pane, perform the following actions:
   a) From the Tenant drop-down list, choose a tenant.
   b) From the Application Profile drop-down list, choose an application profile (app).
c) In the Drag and drop to configure element area, drag and drop the L3 External Network into the topology.

Step 4
In the Select an object dialog box, expand Tenant <tenant_name> (tenant1), choose the Layer 3 external network and click OK.

Step 5
In the Drag and drop to configure element area, drag and drop the Contract on top of the Layer 3 external network and drag to connect the EPG (WEB).

Step 6
In the New Contract dialog box, perform the following actions:
   a) In the Consumers field, verify that it displays the correct Layer 3 external network (L3ext).
   b) In the Providers field, verify that it displays the correct EPG (WEB).
   c) In the Name field, enter the name of the contract (L3ext-to-WEB).
   d) (Optional) In the Description field, enter the description of the contract.
   e) In the Filters field, you can add traffic filters by clicking the + icon.
   f) In the new dialog box, drag and drop all the filters you wish to add to the contract from the list on the left to the list on the right and click OK.
   g) (Optional) Check the Configure L4-7 service check box to configure Layer 4 to Layer 7 services.
   h) Click OK to create the contract.

The contract is connected to the Layer 3 external network in the topology.

Setting up L2 External Network

This section describes how to connect Layer 2 (L2) External Network.

Note
You cannot do any configuration with an L2 External Network. You can only set up an L2 External Network that exists in the APIC.

Before You Begin

- Ensure that a L2 external network on APIC is configured. For more information, see the ACI Basic Configuration Guide
- Ensure that an EPG exists.

Procedure

Step 1
Log in to the VMware vSphere Web Client.

Step 2
In the Navigator pane, choose Application Profile.

Step 3
In the Application Profile pane, perform the following actions:
   a) From the Tenant drop-down list, choose a tenant (tenant1).
   b) From the Application Profile drop-down list, choose Expenses.
   c) In the Drag and drop to configure element area, drag and drop the L2 External Network into the topology.
d) In the **Drag and drop to configure** element area, drag and drop the **Contract** on top of the L2 external network, and then drag to connect the EPG (WEB).

**Step 4**  
In the **New Contract** dialog box, perform the following actions:

a) In the **Consumers** field, verify that it displays the correct L2 External Network (L2ext).

b) In the **Providers** field, verify that it displays the correct EPG (WEB).

c) In the **Name** field, enter the name of the contract (L2ext-to-WEB).

d) In the **Description** field, enter the description of the contract.

e) In the **Filters** field, you can add traffic filters by clicking the + icon.

f) In the **new** dialog box, drag and drop all the filters you wish to add to the contract from the list on the left to the list on the right and click **OK**.

   (Optional) Check the **Configure L4-7 service** check box to configure Layer 4 to Layer 7 services.

h) Click **OK**.

The contract is connected to the L2 external network in the topology.

---

### Creating a VRF Using the Drag and Drop Method

This section describes how to create a VRF using the drag and drop method.

**Procedure**

**Step 1**  
Log into the VMware vSphere Web Client.

**Step 2**  
In the **Work** pane, choose **Networking**.

**Step 3**  
In the **Networking** pane, perform the following actions:

a) From the **Tenant** drop-down list, choose a tenant

b) In the **Drag and drop to configure** element area, drag and drop the VRF into the pane.

**Step 4**  
In the **New VRF** dialog box, perform the following actions:

a) In the **Name** field, enter the name of the VRF.

b) (Optional) In the **Description** field, enter the description of the VRF.

c) In the **Security** section, check the **Enforce Policies** check box. Enforce Policies determines if the security rules (Contracts) should be enforced or not for that VRF.

d) Click **OK**.

---

### Creating a Bridge Domain

This section describes how to create a bridge domain.

**Before You Begin**

- Ensure that a VRF (Private Network) exists.
**Procedure**

**Step 1** Log into the VMware vSphere Web Client.

**Step 2** In the **Navigator** pane, choose **Networking**.

**Step 3** In the **Networking** pane, perform the following actions:
- a) From the **Tenant** drop-down list, choose a tenant (tenant 1).
- b) In the **Drag and drop to configure** element area, drag and drop the Bridge Domain on top of the VRF in the topology.

**Step 4** In the **New Bridge Domain** dialog box, perform the following actions:
- a) In the **Name** field, enter the name of the bridge domain (BD2).
- b) (Optional) In the **Description** field, enter the description of the bridge domain.
- c) In the **Private Subnets** section, enter the private subnets (2.2.2.2/24) and click the + icon to add the subnet to the bridge domain.
- d) (Optional) Repeat substeps c and d to add the desired number of subnets to the bridge domain.
- e) Click **OK**.

The bridge domain connects to the VRF in the topology.

---

**Start a New Troubleshooting Session Between Endpoints**

This section describes how to start a new troubleshooting session between endpoints.

**Procedure**

**Step 1** Log into the VMware vSphere Web Client.

**Step 2** In the **Work** pane, choose **Cisco ACI Fabric**.

**Step 3** In the **Navigator** pane, choose **Troubleshooting**.

**Step 4** In the **Policy Checker** tab, in the **Session name** section, enter the new session name.

**Step 5** In the **Source and Destination** section, click **Select source**.

**Step 6** From the Menu that opens, click on **Select Endpoint**.

**Step 7** In the new dialog box that opens, select the endpoint to use as source and click **OK**.

**Step 8** In the **Source and Destination** section, click **Select destination**.

**Step 9** From the Menu that opens, click on **Select Endpoint**.

**Step 10** In the new dialog box that opens, select the endpoint to use as destination and click **OK**

**Step 11** Click **Start Troubleshooting Session**.

**Step 12** In the **Troubleshooting** pane, you can inspect the faults, configured contracts, event, audits and traffic stats. A topology displays your configuration for each endpoint, the corresponding vNIC, VM, host, and the EPG to which the vNIC is connected. You can click the icon next to an element to get details, corresponding to the category selected in the left pane.

**Step 13** In the **Navigation** pane, click **Traceroute** to start a trace route between the two endpoints.
Start an Existing Troubleshooting Session Between Endpoints

This section describes how to start an existing troubleshooting session between endpoints.

Before You Begin

Procedure

**Step 1** Log into the VMware vSphere Web Client, in the **Work** pane, choose **Cisco ACI Fabric**.

**Step 2** In the **Navigator** pane, choose **Troubleshooting**.

**Step 3** In the **Policy Checker** tab, in the **Session name** section, click **Select an existing session**.

a) In the **Select a section** dialog box, choose a troubleshooting session.
b) Click **OK**.

You can only do endpoint to endpoint troubleshooting.

**Step 4** Click **Start Troubleshooting Session**.

**Step 5** In the **Troubleshooting** pane, you can inspect the faults, configured contracts, event, audits and traffic stats. A topology displays your configuration for each endpoint, the corresponding vNIC, VM, host, and the EPG to which the vNIC is connected. You can click the icon next to an elements to get details, corresponding to the category selected in the left pane.

**Step 6** In the **Navigation** pane, click **Traceroute** to start a trace route between the two endpoints.

Uninstalling the Cisco ACI with VMware vSphere Web Client

This section describes how to uninstall the Cisco ACI with VMware vSphere Web Client.

Procedure

**Step 1** Uninstall the Cisco ACI with VMware vSphere Web Client, enter the following URL:

**Example:**
https://<VCENTER_IP>/mob/?moid=ExtensionManager&method=unregisterExtension

**Step 2** In the **Parameters** section, in the **Value** field, enter **com.cisco.aciPlugin** and click **Invoke Method**.

**Step 3** Log into the VMware vSphere Web Client to ensure the **Cisco ACI Fabric** is not present in the GUI.

**Note** If you were already logged into the VMware vSphere Web Client, you need to log out and log back in to ensure that the **Cisco ACI Fabric** is not present.
Upgrading the Cisco ACI with VMware vSphere Web Client

This section describes how to upgrade the Cisco ACI with VMware vSphere Web Client.

Procedure

To upgrade the Cisco ACI with VMware vSphere Web Client, you must follow the install procedure. For more information, see Installing the Cisco ACI vCenter Plugin, on page 3.

Troubleshooting the Cisco ACI vCenter Plugin Installation

This section describes how to troubleshoot the Cisco ACI vCenter Plugin installation.

If the Cisco ACI vCenter Plugin is not seen the VMware vSphere Web Client GUI, perform the following actions:

- Make sure the .zip file can be downloaded from the vCenter by ensuring that HTTPS/HTTP traffic is working between the vCenter and web server where the .zip is hosted.
- Ensure that you have enabled HTTP download if you are using a HTTP web server.
- Ensure that the Thumbprint used is correct if you are using HTTPS.
- Check if the registration has happened by going to the following URL: https://<VCENTER_IP>/mob?moid=ExtensionManager&doPath=extensionList%5b%2ecom%2ecisco%2eaciPlugin%5d. You should see the Cisco ACI vCenter Plugin details.

If you do not and the page is blank, this indicates that the registration did not succeed. This means an error occurred while executing the registration script. To resolve this, you must perform the installation procedure again and note if an error is displayed by the registration scripts.

- Check the vSphere Web Client logs.
  
  * Linux Appliance: /var/log/vmware/vsphere-client/logs/vsphere_client_virgo.log
  
  * 5.5 Windows 2008: C:\ProgramData\VMware\vSphere Web Client\serviceability\logs\vsphere_client_virgo.log
  
  * 6.0 Windows 2008: %ALLUSERSPROFILE%\VMware\vCenterServer\logs\vsphere-client\logs\vsphere_client_virgo.log

  * Searching for ‘vcenter-plugin’ or ‘com.cisco.aciPlugin’ in the log displays relevant information about the install/upgrade.

An Example of a successful upgrade:

```
Downloading plugin package from https://172.23.137.72/vcenter-plugin-2.0.343.6.zip (no proxy defined)
[2016-05-31T19:32:56.872Z] [INFO ] m-catalog-manager-pool-11128 70002693 100019 200004 com.vmware.vise.vim.cm.CmCatalogManager
Detected service providers (ms):206
```
Reference Information

Alternative Installation of the Cisco ACI vCenter Plugin

This section describes how to install the Cisco ACI vCenter Plugin. If you cannot enable HTTPS traffic between your vCenter and APIC and you wish to use your own web server to host the Cisco ACI vCenter Plugin zip file, follow this procedure.

Before You Begin

- Make sure that all the prerequisites are met.
  
  For more information, see Cisco ACI vCenter Plugin Software Requirements, on page 2.
  
  For more information, see Required APIC Configuration, on page 3.
- Have a PowerCLI console available.
  
  For more information, see VMware's documentation.

Procedure

Step 1 Make the .zip file available on a Web server.

a) If the Web server is not HTTPS: By default, vCenter will only allow a download from HTTPS sources. To allow from HTTP, open and edit the following configuration file for your vCenter version:

- vCenter 5.5 Linux Appliance: /var/lib/vmware/vsphere-client/webclient.properties
- vCenter 6.0 Linux Appliance: /etc/vmware/vsphere-client/webclient.properties
- vCenter 5.5 Windows 2008: %ALLUSERSPROFILE%\VMware\vSphere Web Client\webclient.properties
- vCenter 6.0 Windows 2008: C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\webclient.properties

b) Add allowHttp=true at the end of the file.
Step 2  Run the script by using the PowerCLI console:
   a) Open a PowerCLI console.
   b) Run the ACIPlugin-Install.ps1 script.
      When prompted, enter the following information:
      • In the vCenter IP / FQDN field, enter the vCenter where the plugin needs to be installed.
      • In the Plugin .zip file URL field, enter the URL where the vCenter will be able to download the plugin.
         Note  Ensure you have not renamed the .zip file.
      • If you are using HTTP, leave the SHA1 Thumbprint field empty. Otherwise, enter the SHA1 Thumbprint of the Web server used. The fields are separated with colons. For example:
   c) In the dialog box, enter the root privilege credentials of the vCenter.
   Python Script:
      The requirement is to use Python 2.7.9 or higher, pyvmomi package installed in the python environment.
      a) Run the Python script.
         When prompted, enter the following information:
         • In the vCenter IP field, enter the vCenter where the plugin needs to be installed.
         • In the vCenter Username & Password field, enter the root privilege credentials of the vCenter.
         • In the Plugin .zip file URL field, enter the URL where the vCenter will be able to download the plugin.
            Ensure you have not renamed the .zip file.
         • In the Https server thumbprint field, Leave this empty, if you are using HTTP. Otherwise, enter the SHA1 Thumbprint of the Web server used. The fields are separated with colons. For example:
            Note  There is also a deploy.cfg file available, where you can pre-enter your information. You can then run the script with the file as argument. For example:
                   $ python deployPlugin.py deploy.cfg

Step 3  Log into the vSphere Web Client once the registration is completed.
   Note  First login may take longer, as the vCenter will be downloading and deploying the plugin from the Web server.
      Once the VMware vSphere Web Client loads, you will see the Cisco ACI Fabric in the Navigator pane. This allows you to manage your ACI fabric.
      Note  After you register the plugin, when you launch the web client for the first time, an error message might display asking to reload the web client. Click Reload to refresh the page and the error message will not appear again.