Cisco ACI vCenter Plug-in

This chapter contains the following sections:

About Cisco ACI with VMware vSphere Web Client

The Cisco ACI vCenter plug-in 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 plug-in 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 plug-in. Only the elements that are relevant to virtualization administrators are exposed.

Cisco ACI vCenter Plug-in Overview

The Cisco Application Centric Infrastructure (ACI) vCenter plug-in for the VMware vSphere Web Client, adds a new view to the GUI called Cisco ACI Fabric.

The Cisco Application Centric Infrastructure (ACI) vCenter plug-in 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 plug-in 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 plug-in:

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

The Cisco ACI vCenter plug-in 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 plug-in 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.

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

The Cisco ACI vCenter plug-in also allows to consume preconfigured 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 plug-in also has troubleshooting capabilities:

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

Getting Started with Cisco ACI vCenter Plug-in

Cisco ACI vCenter Plug-in Software Requirements

The Cisco ACI vCenter plug-in Software Requirements:

Platform Series	Recommended Release
vCenter	Cisco APIC supports any version of Linux Appliance and Windows Server that VMware supports. See VMware documentation for details.
Application Policy Infrastructure Controller (APIC)	Release 3.2(2) and later

Required APIC Configuration

This sections describes the required APIC configuration.

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

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

Installing the Cisco ACI vCenter Plug-in

This section describes how to install the Cisco Application Centric Infrastructure (ACI) vCenter plug-in. You must have working HTTPS traffic between your VMware vCenter and Cisco Application Policy Infrastructure Controller (APIC). That is because VMware vCenter downloads the plug-in directly from the Cisco APIC.

If you cannot enable HTTPS traffic between your VMware vCenter and Cisco APIC, and you wish to use your own web server to host the Cisco ACI vCenter plug-in zip file, see the Alternative Installation of the Cisco ACI vCenter Plug-in, on page 35.

If you are using VMware 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 Plug-in, on page 35.

To install a plug-in, the vCenter must download the plug-in from a Web server. In the following procedure, the Cisco APIC is used as the Web server, and the VMware vCenter downloads the plug-in directly from the Cisco APIC.

Before 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 Cisco APIC only supports TLSv1.1 and TLSv1.2, therefore the vCenter will not be able to download the plug-in from the Cisco APIC. The plug-in must be put on a separate Web server, that allows TLSv1 or that does not use HTTPS.

Note If you log out of VMware vCenter 6 .7 and then log back in, you may not see the vCenter plug-in icon. If that occurs, clear the cookies and history or log in using another browser.

Before you begin

- Make sure all of the prerequisites are met.

  For more information, see the Cisco ACI vCenter Plug-in Software Requirements, on page 2 and Required APIC Configuration, on page 3 sections.

- Ensure HTTPS traffic is allowed between your vCenter server and APIC.
- If you are installing the Cisco ACI vCenter plug-in for VMware vCenter 6.7, you need PowerCLI version 11.2.0 or later.

Note During installation, you may see the following error on the console:

```
Error: Invalid server certificate. Use
Set-PowerCLIConfiguration to set the value for
the InvalidCertificationAction option to Prompt
if you'd like to connect once or to add a
permanent exception for this server.
```

To avoid seeing this error, enter the following command before installation:**`Set-PowerCLIConfiguration -InvalidCertificateAction Ignore -Confirm:$false`**

Procedure

Step 1 Go to the following URL:

Example:

`https://`*`<APIC>`***`/vcplugin`**

Step 2 Follow the instructions on that web page.

Connecting the Cisco ACI vCenter Plug-in to your Cisco ACI Fabric

This section describes how to connect the Cisco Application Centric Infrastructure (ACI) vCenter plug-in to your Cisco ACI fabric.

Note

- The registration is VMware vCenter-wide and it does not take into account the user that performs it. It is a configuration for the whole VMware 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 Cisco Application Policy Infrastructure Controller (APIC) account used for the registration defines configuration restriction on the Cisco ACI vCenter plug-in.

You can connect the plug-in to your Cisco ACI fabric, using one of the following ways:

Connect the Cisco ACI vCenter plug-in to your Cisco ACI fabric using credentials.	For more information, see Connecting vCenter Plug-in to the Cisco ACI Fabric Using Credentials, on page 5.
Connect the Cisco ACI vCenter plug-in to your Cisco ACI fabric using an existing certificate.	For more information, see Connecting vCenter Plug-in to your ACI Fabric Using an Existing Certificate, on page 5.

Connect the Cisco ACI vCenter plug-in to your Cisco ACI fabric by creating a new certificate.	For more information, see Connecting vCenter Plug-in to your ACI Fabric by Creating a New Certificate, on page 6.

Connecting vCenter Plug-in to the Cisco ACI Fabric Using Credentials

This section describes how to connect the Cisco Application Centric Infrastructure (ACI) vCenter plug-in to your Cisco ACI fabric using credentials.

Before you begin

Ensure the Cisco ACI vCenter plug-in is installed. For more information, see Installing the Cisco ACI vCenter Plug-in, 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 Cisco Application Policy Infrastructure Controller (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 Cisco APIC node was successfully added to the Cisco ACI fabric.

Step 7 In the **ACI Fabric** pane, you will see the new registered Cisco APIC discover the other Cisco APICs.

The Cisco ACI vCenter plug-in always uses a single Cisco APIC for its requests. However, it switches the Cisco APIC if the Cisco APIC currently used is no longer available.

Note Registering the Cisco ACI fabric with the Cisco ACI vCenter plug-in is not supported for remote users.

Connecting vCenter Plug-in to your ACI Fabric Using an Existing Certificate

This section describes how to connect the vCenter plug-in 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 plug-in always uses a single APIC for its requests. If the currently used APIC is no longer available, the Cisco ACI vCenter plug-in switches APICs.

Connecting vCenter Plug-in to your ACI Fabric by Creating a New Certificate

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

Before you begin

- Ensure the plug-in 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 plug-in, 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 plug-in always uses a single APIC for its requests. If the currently used APIC is no longer available, the Cisco ACI vCenter plug-in switches APICs.

Cisco ACI vCenter Plug-in Features and Limitations

This section describes the possible operations provided by the Cisco ACI vCenter plug-in, 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 plug-in allows CRUD operations on the Tenant object. The following attributes are exposed in the plug-in:

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

When a tenant is created by the plug-in, 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 plug-in.

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

Application Profiles

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

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

Endpoint Groups

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

- 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/Cisco AVS where the EPG is deployed. This correspond to the association with a VMM domain in ACI

  By default, all EPGs created with the plug-in are associated with the VMM Domain pointing to the vCenter where the plug-in 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 microsegmentation (only for DVS, not Cisco AVS): This allows you to create a “Base EPG” . All the virtual machines connected to this EPG are candidates to apply microsegmentation rules of a uSeg EPG. Microsegmented 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 Cisco AVS.

An EPG linked to a VMM domain pointing to the vCenter where the plug-in 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 plug-in allows CRUD operations on the mircosegemented EPG objects. The following attributes are exposed in the plug-in:

- Name: The name of the microsegmented EPG.
- Description (Optional): The description of the microsegmented EPG.
- Bridge Domain: The Bridge Domain associated with this microsegmented 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/Cisco AVS where the EPG is deployed. This correspond to the association with a VMM domain in ACI

  By default, all EPGs created with the plug-in are associated with the VMM Domain pointing to the vCenter where the plug-in 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.
- Miro-segmentation attributes: List of rules that decide which VM belongs to this microsegmented EPG. Rules options include: IP, MAC, VM name, OS, Host, VM id, VNic, Domain, Data Center, Custom Attribute.

Note Domain attributes (VMM Domain) only allow you to select VMM domains to the local vCenter. You choose a domain by selecting the corresponding DVS/Cisco AVS.

Custom attributes can only be chosen. They cannot be set by the plug-in. They must be set by the VMware vSphere Client. To create custom labels, see the documentation on the VMware website.

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 plug-in.

The only plug-in 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 plug-in allows CRUD operations on the VRF objects. The following attributes are exposed in the plug-in:

- 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 plug-in allows CRUD operations on the Bridge Domain objects. The following attributes are exposed in the plug-in:

- 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 plug-in. 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 plug-in allows CRUD operations on the Contract objects. The following attributes are exposed in the plug-in:

- 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 plug-in 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 plug-in 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 plug-in (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 plug-in does not allow folder manipulation.
  - Only empty mandatory parameters of the function profile are editable by the plug-in.
- 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 connecter 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 AVS Installation and Upgrade

The Cisco ACI vCenter plug-in enables you to install, uninstall, upgrade, or downgrade Cisco AVS from the vSphere Web Client:

- Once the vCenter plug-in is connected to the ACI fabric, it allows you to see all the Cisco AVS domains present on Cisco APIC, and to install, uninstall, upgrade, or downgrade Cisco AVS for some or all of the hosts in the data center associated with the Cisco AVS domains.
- New versions of Cisco AVS that have been downloaded from Cisco.com can be uploaded to the vCenter using the GUI. These versions can then be installed on the hosts in a given domain.
- You can see all hosts if they are connected to a given Cisco AVS domain. You also can see the hosts' OpFlex Agent status and the current version of Cisco AVS, if installed.

When installing or upgrading Cisco AVS, the vCenter plug-in automatically performs the following steps on a ESXi host:

1. Places the host into maintenance mode.
2. Uploads the appropriate VIB file to the host data store.
3. Installs or reinstalls Cisco AVS software.
4. Deletes the VIB file from the host data store.
5. Takes the host out of maintenance mode.

Note

- The vCenter plug-in only installs or uninstalls Cisco AVS VIBs on the hosts; you need to manually connect or disconnect the host to the Cisco AVS switch.
- If the host is part of an HA/DRS cluster, when the host is placed in maintenance mode, the VMs will be migrated automatically. If the VMs can't be migrated automatically, you need to migrate them or turn off all the VMs on the host for the installation or upgrade to succeed.

For more information see the following sections in the Cisco AVS Installation Guide:

- "Installing Cisco AVS Using the VMware vCenter Plug-in"
- "Upgrading or Downgrading Cisco AVS Using the VMware vCenter Plug-in"
- "Uninstalling Cisco AVS using the VMware vCenter Plug-in"

Role-based Access Control for Cisco ACI vCenter Plug-in

Starting with Cisco APIC Release 3.1(1), the Cisco ACI vCenter plug-in supports enhanced role-based access control (RBAC) based on Cisco APIC user roles and security domains.

The UI of the Cisco ACI vCenter plug-in reflects the read and write privileges of Cisco APIC users. For example, if the user tries to access contract features but does not have read privilege for contracts, a gray screen displays with message saying the user does not have permission. A user who does not have write privileges sees a disabled link or action.

Setting Read and Write Roles

The following table describes how each privilege should be set for read and write roles in order to enable or disable the different features of Cisco ACI vCenter plug-in RBAC.

Note You must create Cisco APIC roles and associate them when assigning a security domain to a user or users. You also must add security domains to any tenant the user will have access to.

Table 1: Cisco ACI vCenter Plug-in RBAC Privileges

Roles	Workflow	Limited Read Role	Write Role
Mandatory settings for all roles		vmm-connectivity and vmm-ep	
Application Profile	List	tenant-network-profile or tenant-epg	
	Create/Delete		tenant-network-profile

Roles	Workflow	Limited Read Role	Write Role
EPG	List	tenant-epg, tenant-connectivity-l2, and tenant-connectivity-l3	
	Create/Delete	tenant-connectivity-l2 and tenant-connectivity-l3	tenant-epg
VRF	List	tenant-connectivity-l2 and tenant-connectivity-l3	
	Create/Delete		tenant-connectivity-l2 and tenant-connectivity-l3
Bridge Domain	List BD	tenant-connectivity-l2 and tenant-connectivity-l3	
	Create/Delete BD		tenant-connectivity-l2 and tenant-connectivity-l3
	List BD Subnet	tenant-connectivity-l2 and tenant-connectivity-l3	
	Create/Delete BD Subnet		tenant-connectivity-l2 and tenant-connectivity-l3
Contract	List Contract	tenant-security and tenant-epg	
	Create/Delete Contract		tenant-security and tenant-epg
	List Filter	tenant-security and tenant-epg	
	Create/Delete Filter	tenant-epg	tenant-security
L4L7	List	tenant-security, tenant-epg, and nw-svc-policy	
	Create/Delete	tenant-epg	tenant-security and nw-svc-policy
Troubleshooting	List Session	admin*	
	Create/Delete Session		admin*
L2 Out	List L2Outs	tenant-ext-connectivity-l2	
	Contract creation	tenant-ext-connectivity-l2	tenant-security

Roles	Workflow	Limited Read Role	Write Role
L3 Out	List L3Outs	tenant-ext-connectivity-l3	
	Contract creation	tenant-ext-connectivity-l3	tenant-security

Note In the preceding table, you must add roles marked with an asterisk (*) with the security domain "all."

For more information about Cisco APIC user roles and security domains, see the section "User Access: Roles, Privileges, and Security Domains" in Cisco ACI Fundamentals.

Recommended RBAC Configuration for Cisco ACI vCenter Plug-in

We recommended that you define two user roles with privileges to be created on APIC for aaaUser:

- vcplugin_read—defines the read permissions of aaaUser.
- vcplugin_write—defines the write permissions of aaaUser.

You can register the Cisco ACI fabric only as a local user on Cisco APIC. If the default log-in domain is local, you can log in as admin or any local username and password.

However, if the default login domain is not local, you can still register the fabric by specifying the local domain in the username:

```
apic#local domain\username
```

The local domain name must exist on Cisco APIC before you enter the local domain and username.

Note Any RBAC configuration requires that you assign the security domain or domains of aaaUser to the VMM domain between Cisco APIC and VMware vCenter.

Note The Cisco ACI vCenter plug-in adapts to any combination of user roles that follow the permissions described in the RBAC privileges table in Role-based Access Control for Cisco ACI vCenter Plug-in, on page 13 in this guide.

Upgrading VMware vCenter when Using the Cisco ACI vCenter Plug-in

If you are upgrading VMware vCenter from version 6.0 to version 6.5, and you are using the Cisco ACI vCenter plug-in, you need to take an additional step before you proceed with the upgrade.

Note It is a best practice to uninstall the vCenter plug-in before you upgrade the VMware vCenter and then reinstall it after the upgrade.

Procedure

Delete the folder `C:\ProgramData\cisco_aci_plugin\` on the vCenter.

If you do not delete the folder, and you try to register a fabric again after the upgrade, you see the following error message: "Error while saving setting in C:\ProgramData\cisco_aci_plugin*user_domain*.properties" where the user is the user currently logged in to the vSphere Web Client, and the domain is the domain to which it belongs.

Although you can still register a fabric, you do not have rights to override settings that were created in the old VMware vCenter. You need to enter any changes in Cisco APIC configuration again after restarting VMware vCenter.

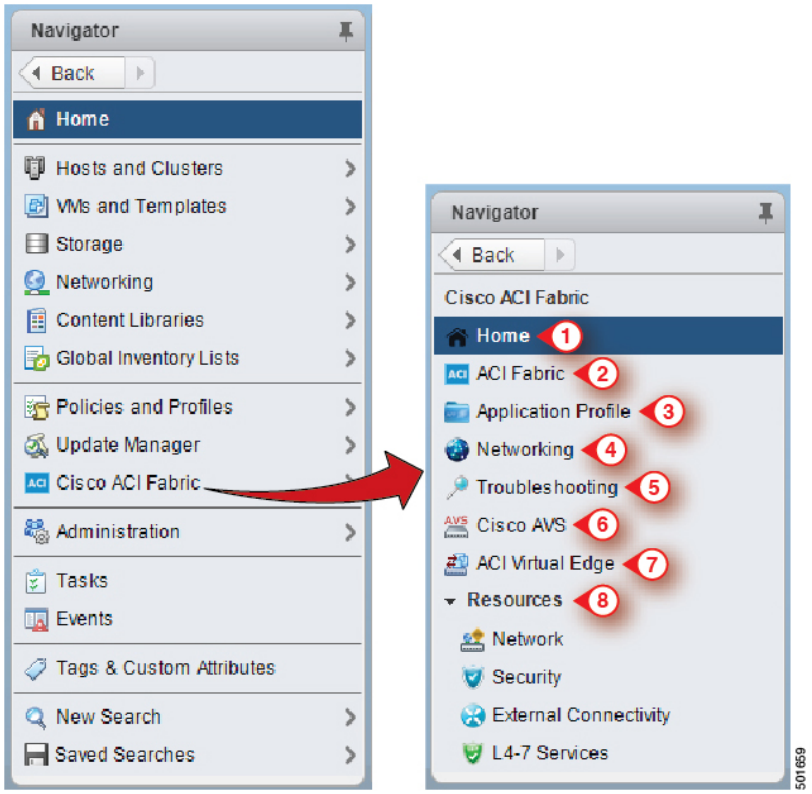
Cisco ACI vCenter Plug-in GUI

Cisco ACI vCenter Plug-in GUI Architecture Overview

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

Main Menu

Figure 1: Main Menu



1	**Home**—Displays the Cisco ACI vCenter plug-in home page and has a **Getting Started** and an **About** tab. The **Getting Started** tab that allows you to perform basic tasks such as **Create a new Tenant**, **Create a new Application Profile**, **Create a new Endpoint Group** and click the Cisco Application Centric Infrastructure (ACI) link to explore the ACI website. The **About** tab displays the current version of the Cisco ACI vCenter plug-in.
2	**ACI Fabric**—Used to register an ACI Fabric in the plug-in and manage the tenants of the fabrics.
3	**Application Profile**—Used to manage application profiles by a drag and drop interface of EPG, uSeg EPG, L2/L3Out and Contract. Provides visibility on an application health, Stats and Faults.
4	**Networking**—Drag and Drop interface to manage VRFs and Bridge Domains.
5	**Troubleshooting**—View contracts defined between to entity, Start endpoint to endpoint troubleshooting sessions, browse the virtual machines (VMs) and view their connections to the endpoint groups (EPGs).
6	**Cisco AVS**—Install, upgrade, or uninstall Cisco AVS. See the Cisco Application Virtual Switch Installation Guide for information.

7	**Cisco ACI Virtual Edge**—Install or uninstall Cisco ACI Virtual Edge, or migrate from Cisco AVS or VMware VDS to ACI Virtual Edge. See the Cisco ACI Virtual Edge Installation Guide for information.
8	**Resources**—Allows you to browse in a hierarchical view of all objects managed by the plug-in.

Note While navigating through **Application Profile**, **Networking** and **Resources** sections, a selection bar at the top of each screen allows you to select an active tenant. Content displayed for each section is specific to the tenant selected in that bar.

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 Cisco APIC 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 **Navigator** pane, choose **Home**. In the **Work** pane displays the following tabs:

- **Getting Started** tab

  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 Cisco APIC states of the fabric.

Note When the plug-in detects the Cisco 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 Cisco APIC. Click **Reload** to refresh the Cisco APIC state. This forces it to try to reconnect to each Cisco APIC, even to the unavailable ones. This updates their status, if they are available again.

- **Tenants** tab

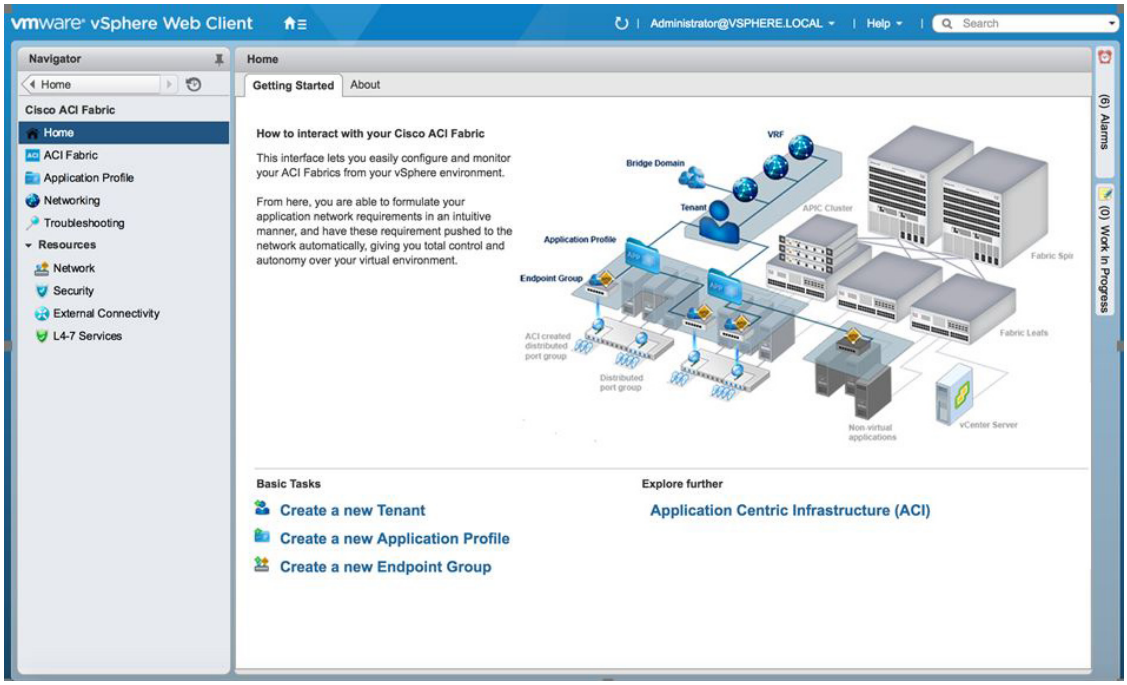
  The **Tenants** pane enables you to do the following things:

  - 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 matches 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 Cisco 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 Cisco 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-provisoned 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 plug-in, 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 Plug-in to the Cisco ACI Fabric Using Credentials, on page 5.

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 **ACI Fabric**.

Step 4 In the **ACI Fabric** pane, choose the **Tenants** tab.

Step 5 In the **Tenants** pane, click **Create a new Tenant**.

Step 6 In the **New Tenant** dialog box, perform the following actions:

a) In the **Enter a name for the Tenant** field, enter the tenant name.

b) (Optional) In the **Enter a description for the Tenant** field, enter the description for the tenant.

c) Click **OK**.

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 23.

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 **Resources** > **Network**.

Step 4 In the **Network** pane, under the **Endpoint Groups** tab, perform the following actions:

a) From the **Tenant** drop-down list, choose the tenant name.
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 23.

- Ensure that an application profile has been created.

  For more information, see Creating a New Application Profile, on page 24.

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 24.

- (DVS only, not Cisco 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 24.

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 24.
- 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:

a. Drag and drop the **Contract** on the EPG that needs to consume the contract.

b. 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:

a. Drag and drop the **Contract** on the contract that the EPG needs to provide.

b. 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 24.

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 an 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 24.

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 a 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**.
g) (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 sections 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 in to 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 (tenant1).

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 elements to get details, corresponding to the category selected in the left pane.

Step 13 In the **Navigation** pane, click **Traceroute** to start a traceroute between the two endpoints.

Start an Exisiting 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 traceroute between the two endpoints.

Uninstalling the Cisco ACI vCenter Plug-in

This section describes how to uninstall the VMware vCenter Plug-in.

Before you begin

- You must have a PowerCLI console available.
- You must have the `ACIPlugin-Uninstall.ps1` script available.

  You can find the script inside the plug-in archive, or you can download it from: `https://APIC_IP/vcplugin/ACIPlugin-Uninstall.ps1`.

Procedure

Step 1 Open a PowerCLI console.

Step 2 Run the `ACIPlugin-Uninstall.ps1` script.

Step 3 When prompted, in the **vCenter IP / FQDN** field, enter the vCenter where the plug-in needs to be uninstalled.

Step 4 In the dialog box that appears, enter the root privilege credentials of the vCenter.
you should see the following message in the console if the uninstallation was successful:

```
[x] Uninstalled ACI vCenter Plugin
```

Upgrading the Cisco ACI vCenter Plug-in

This section describes how to upgrade the Cisco ACI vCenter Plug-in.

Procedure

To upgrade the Cisco ACI vCenter Plug-in, you must follow the installation procedure.

For more information, see Installing the Cisco ACI vCenter Plug-in, on page 3.

Troubleshooting the Cisco ACI vCenter Plug-in Installation

This section describes how to troubleshoot the Cisco ACI vCenter plug-in installation.

If the Cisco ACI vCenter plug-in 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 your 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"com%2ecisco%2eaciPlugin"%5d

  You should see the Cisco ACI vCenter plug-in 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:

```
[2016-05-31T19:32:56.780Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004 com.vmware.vise.vim.extension.VcExtensionManager
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
[2016-05-31T19:32:56.872Z] [INFO ] m-catalog-manager-pool-11128 70002693 100019 200004

com.vmware.vise.vim.cm.CmCatalogManager
No new locales or service infos to download.
[2016-05-31T19:32:57.678Z] [INFO ] -extensionmanager-pool-11139 70002693 100019 200004

com.vmware.vise.vim.extension.VcExtensionManager
Done downloading plugin package from https://172.23.137.72/vcenter-plugin-2.0.343.6.zip

[2016-05-31T19:32:58.438Z] [INFO ] -extensionmanager-pool-11139 70002693 100019 200004

com.vmware.vise.vim.extension.VcExtensionManager
Done expanding plugin package to /etc/vmware/vsphere-client/vc-packages/vsphere-client-
serenity/com.cisco.aciPlugin-2.0.343.6
[2016-05-31T19:32:58.440Z] [INFO ] -extensionmanager-pool-11139 70002693 100019 200004

com.vmware.vise.extensionfw.ExtensionManager
Undeploying plugin package 'com.cisco.aciPlugin:2.0.343.5’.
```

Reference Information

Alternative Installation of the Cisco ACI vCenter Plug-in

This section describes how to install the Cisco ACI vCenter plug-in. 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 plug-in zip file, follow this procedure.

Before you begin

- Make sure that all the prerequisites are met.

  For more information, see Cisco ACI vCenter Plug-in 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 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.

c) If the Web server is not HTTPS, restart the vSphere Web Client service using the '**/etc/init.d/vsphere-client restart**' command.

Step 2 Run the script using the PowerCLI console or Python:

Option	Description
To use 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 plug-in needs to be installed.

Option	Description

	• In the **Plugin .zip file URL** field, enter the URL where the vCenter will be able to download the plug-in.
	Note Ensure you have not renamed the .zip file.
	• If you are using HTTP, leave the SHA1 thumbprint field empty. If you are using HTTPS, enter the SHA1 thumbprint of the Web server used, using one of the following formats:
	• Separated by colons:
	`xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx`
	• Separated by spaces:
	`xx xx xx xx xx xx xx xx xx xx xx`
	Note Some browsers on Windows might display the certificate thumbprint as a single non-delimited string (for example, xxxxxxxxxxxxxxxxx), which the installation script does not process correctly. Make sure that the SHA1 thumbprint of the Web server uses one of the correct formats. Otherwise, the Cisco ACI vCenter plug-in appears to fail.
	c. In the dialog box, enter the root privilege credentials of the vCenter.

To use Python	**Note** You must use Python 2.7.9 or higher and have the pyvmomi package installed in the Python environment.
	Run the Python script: **`python deployPlugin.py`**
	When prompted, enter the following information:
	• In the **vCenter IP** field, enter the vCenter where the plug-in 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 plug-in.
	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:
	`D7:9F:07:61:10:B3:92:93:E3:49:AC:89:84:5B:03:80:C1:9E:2F:8B`
	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 plug-in 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 plug-in, 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.