Shared Services in Cisco Cloud APIC

Revised: February 19, 2022,

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide from the release the guide was first published to the current release. The table does not provide an exhaustive list of all changes made to the guide or the new features of the Cisco Cloud APIC.

Table 1: New and Changed Information

Release	Feature or Change Description
Release 5.0(2)	Added support for inter-tenant shared services.
Release 4.2(1)	Added support for Microsoft Azure cloud sites.
Release 4.1(1)	First release of this document.

Shared Services Use Case Overview

This document describes how to configure shared services between on-premises Cisco APIC and a Cloud APIC site or between two cloud APIC sites. A sample deployment diagrams below illustrate a few deployment scenarios for shared services, where a Web EPG is consuming DNS service offered by a DNS EPG deployed in another site. In this case, two separate VRFs are created: one for the on-premises sites and one for the cloud site.

Figure 1: Shared Services, On-Premises and AWS

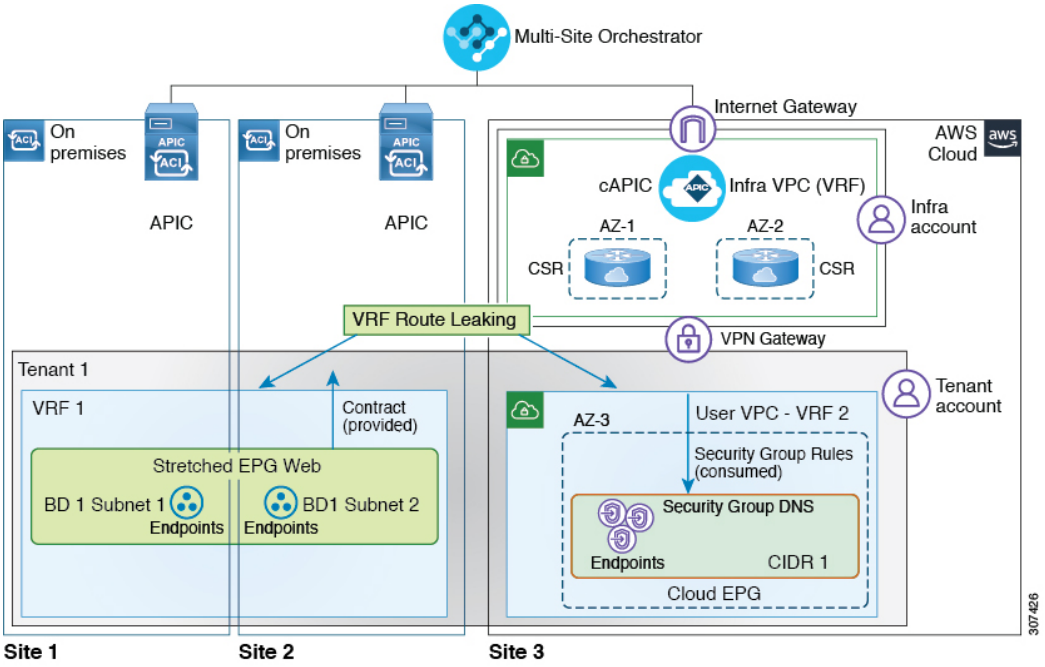


Figure 2: Shared Services, On-Premises and Azure

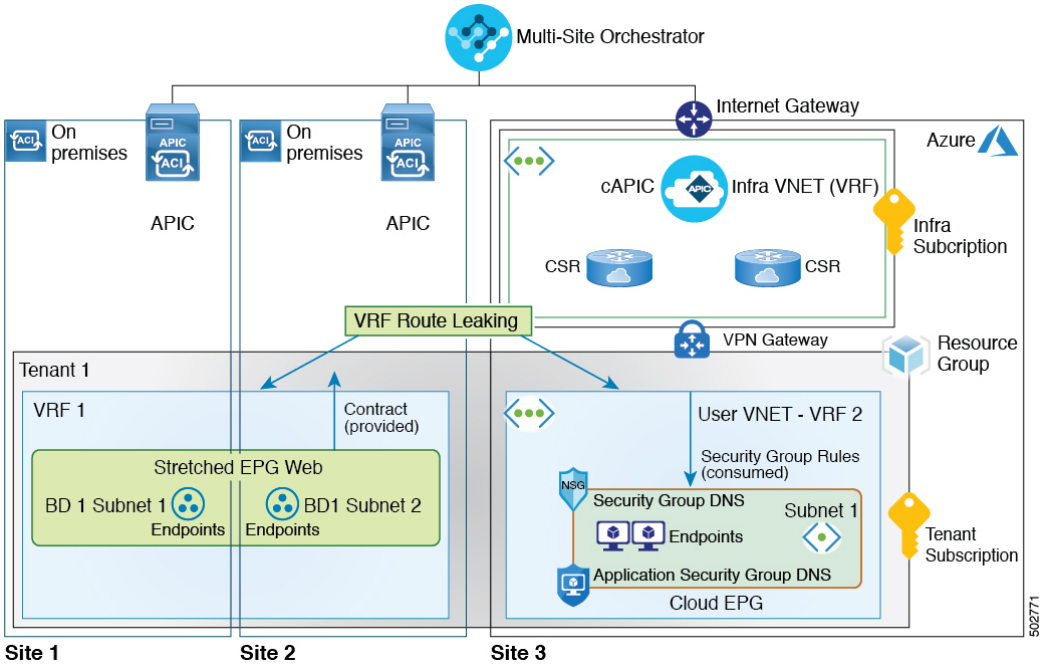
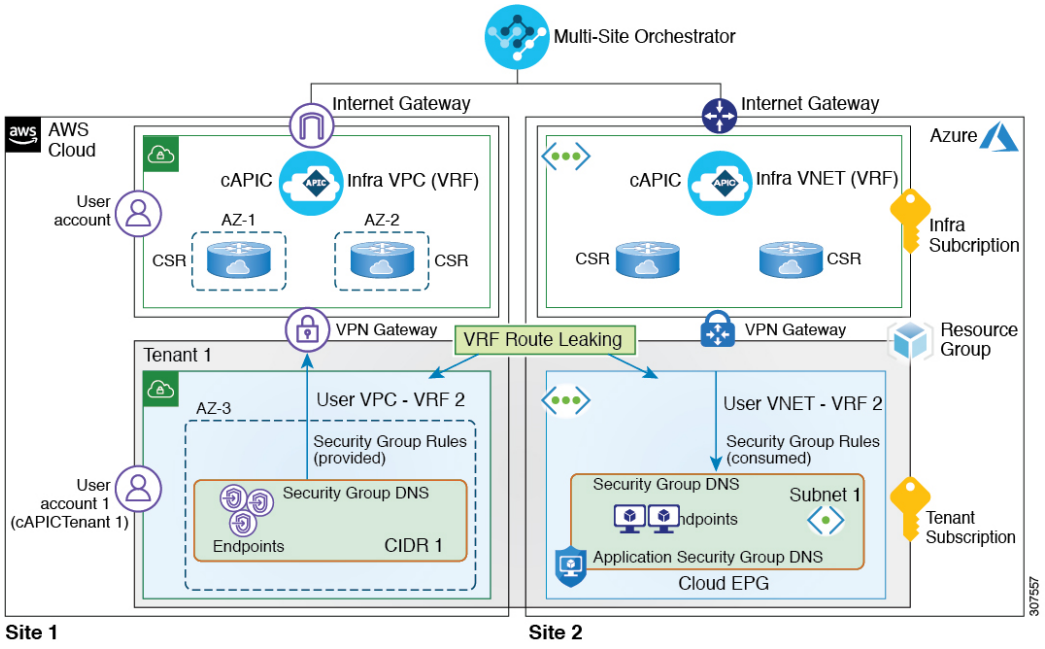


Figure 3: Shared Services, On-Premises and Multi-Cloud



Alternatively, an on-premises VRF can be stretched into the cloud site. However, if you choose to do that, only a single VRF can be stretched between an on-premises site and a cloud site.

You can use the Cisco ACI Multi-Site Orchestrator to deploy either one of the described scenarios by simply establishing a contract between the DNS EPG and the Web EPG. The routing, forwarding, and policy enforcement is managed automatically by the APICs in each site.

Prerequisites

- You must have a Cisco ACI Multi-Site Orchestrator installed and configured and the on-premises site added, as described in Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide

  If you plan to use Cloud APIC in AWS, you must install Cisco ACI Multi-Site Release 2.1(1) or later.

  If you plan to use Cloud APIC in Azure, you must install Cisco ACI Multi-Site Release 2.2(1) or later.

- You must have a Cloud APIC installed, configured, and added to the Multi-Site Orchestrator.

  For AWS, you must install Cloud APIC Release 4.1(1) or later, as described in the Cisco Cloud APIC for AWS Installation Guide.

  For Azure, you must install Cloud APIC Release 4.2(1) or later, as described in the Cisco Cloud APIC for Azure Installation Guide.

- If you plan to use Amazon Web Services, you must have an AWS account set up and configured for the user tenant that will be used in this use case, as described in Setting Up the AWS Account for the User Tenant chapter of the Cisco Cloud APIC for AWS Installation Guide

  There is a one-to-one mapping between AWS accounts and Cisco Cloud APIC tenants, so each tenant must have a unique AWS account associated with it. However, if you already configured an AWS account and a user tenant in your Cisco Cloud APIC, you can choose to use the same tenant for this use-case.

- If you plan to use Microsoft Azure, you must have an Azure subscription set up and configured to use for the user tenant, as described in chapter of the Cisco Cloud APIC for Azure Installation Guide.

  You can create multiple Cloud APIC tenants under the same Azure subscription or you can choose to create a separate subscription for each Cloud APIC tenant. For this use case you can choose to create a new tenant or use an existing one you may have configured previously, for example the subscription configured under the `Infra` tenant used for the Cloud APIC installation.

Guidelines and Limitations

When configuring this use case, the following restrictions apply:

- ACI Multi-Site multi-cloud deployments support a combination of any two cloud sites (AWS, Azure, or both) and two on-premises sites for a total of four sites.
- If you plan to use Amazon Web Services cloud site, you cannot use the same account for multiple Tenants. This includes the `infra` Tenant as well as any user Tenants you may configure.
- Inter-tenant shared services are supported starting with Cloud APIC, Release 5.0(2) and Multi-Site Orchestrator, Release 3.0(2) for cloud tenants only.

  Inter-tenant shared services are not supported between cloud and on-premises tenants.

- For shared services across different VRFs, each on-premises site can have no more than one VRF stretched to one or more cloud sites. Multiple VRFs can be stretched between cloud sites only.
- When creating the shared services contract between the cloud EPG and on-premises EPG across different VRFs within same tenant, the Contract's scope must be set to `tenant`.

- If configuring shared services contract between EPG in VRF1 that is stretched between on-premises and cloud sites and VRF2 which is present only in on-premises site, shadow VRF will be deployed for VRF2 in the cloud site. This deployment of shadow VRF will create AWS VPC or Azure VNET in one of the managed regions with IPv4 CIDR subnet `1.253.0.0/16`.

Gathering the Necessary Information

There are several pieces of information that you will need as you go through the procedures in this document. Gather the information outlined in the following sections, then refer to the information that you enter in this section in later procedures, when necessary.

APIC Bridge Domain Information

You will need to provide bridge domain (BD) information when creating an EPG that contains on-premises endpoints. If you are configuring cloud-only deployments, you can skip this section.

Cisco APIC Bridge Domain Information	Example	Your Entry
Bridge Domain name	bd1	
Subnet information	2.2.2.254/24	
Endpoint information	2.2.2.1/24	

Cloud Tenant Information

When you add a tenant in Multi-Site Orchestrator GUI as described later in this document, you must provide cloud account information for the cloud service where the tenant will be created. You can obtain this information from either your AWS account or Azure account.

Note If you are planning to deploy the tenant to only one type of cloud service, you can skip the irrelevant information in the following tables.

Table 2: AWS Information for Cloud Tenant

Required Information	Your values	Where to locate the information
AWS account ID for the user tenant	_____	The Amazon account for your cloud tenant. Creating a new AWS account and user is described in Setting Up an AWS Account and User, on page 7.

Required Information	Your values	Where to locate the information
AWS Access Key ID and Secret Access Key for the user tenant	AccessKey: _____ Secret Access Key: _____	The following information is required only for `Untrusted` tenants only. If you plan to add a `Trusted` tenant, you can skip this field. You can use the information from the .csv file you downloaded when you created the AWS account and user or follow the following procedures to locate this information in AWS: 1. Log into this new, separate Amazon Web Services account. 2. Go to Identity and Access Management (IAM). https://aws.amazon.com/iam/ 3. In the left pane, select Users. 4. Click the link for your Cisco Cloud APIC user tenant account. 5. On the Summary page, click the Security credentials tab. 6. Click Create access key if you do not already have an Amazon Web Services access key ID. 7. Locate the information from the Access key ID and Secret access key fields.

Table 3: Azure Information for Cloud Tenant

Required Information	Your values	Where to locate the information
Azure account subscription ID for the user tenant	_____	Use the Azure subscription ID. You can obtain the subscription ID by logging into your Azure account and navigating to Home > All Services > Subscriptions. **Note** Keep in mind, you must use the Subscription ID and not Subscription Name as listed in the Azure portal. Alternatively, if you'd like to create a new subscription specifically for the tenant you plan to use for this use case, follow the steps described in Setting Up an Azure Account with a Subscription, on page 8 for this field.
Azure Application ID, Directory ID, and Client Secret	Subscription ID: _____ Application ID: _____ Client Secret: _____	The following information is required only for `Unmanaged` tenants. If you plan to add a managed tenant, you can skip this field. You can locate this information using the following procedure: 1. Log into your Azure account. 2. Navigate to Home > All Services > App registrations > <application-name> and note the `Application (client) ID` and `Directory (tenant) ID`. 3. Then click Certificates & secrets > New client secret and create a Client Secret. **Note** The secret is only viewable immediately after you create it.

Setting Up an AWS Account and User

There is a one-to-one mapping between AWS accounts and Cisco Cloud APIC tenants, so each tenant must have a unique AWS account associated with it. This includes the `infra` tenant as well as any user tenants you may configure.

Note You must have a separate AWS user for each user tenant. However, if you are configuring several different use case scenarios, you can use the same user tenant for all the use cases. You can use the following procedure to create a new user within your AWS account, if necessary.

Procedure

Step 1 Create a new Amazon Web Services account for the Cloud APIC user tenant.

a) Browse to https://aws.amazon.com/.
b) Click Create an AWS Account.
c) Enter the necessary information to create a new AWS account.

Step 2 Log in to your AWS account.

https://signin.aws.amazon.com/

Step 3 Go to the AWS Management Console:

https://console.aws.amazon.com/

Step 4 Create a new user in your AWS account.

This step is required for `Untrusted` tenants only. If you are planning to add this tenant as a `Trusted` tenant, you only need the AWS account ID and can skip this step.

a) Click the Services link at the top of the screen, then click the IAM link.
b) In the left pane, click Users, then click the Add user button.

The Add User page appears.

c) In the User name field, enter a unique name for this user.
d) In the Access type field, check Programmatic access, then click the Next: Permissions button at the bottom of the page.
e) In the Set permissions area, select Attach existing policies directly.

The screen expands to display Filter policies information.

f) Check the box next to Administrator Access, then click the Next: Tags button at the bottom of the page.
g) Leave the information in the Add tags page as-is and click the Next: Review button at the bottom of the page.
h) Click the Create User button at the bottom of the page.

Ignore the warning that states This user has no permissions if that warning appears.

An access key is created for you at this point.

i) Make a note of the Access Key ID and Secret Access Key information for this Amazon Web Services admin account.

Download the .csv file or copy the information from the Access key ID and Secret access key fields to a file.

j) Click the Close button at the bottom of the page.

Setting Up an Azure Account with a Subscription

You can choose to deploy multiple tenants within the same subscription or create a separate subscription for each tenant.

If you want to use an existing subscription, for example the one where you deployed your Cloud APIC, skip this section. Otherwise, you can create a separate subscription specifically for the tenant in this use case.

Procedure

Step 1 Log in to your Azure account.

https://azure.microsoft.com

Step 2 In the left side bar, click All services.

Step 3 In the All services filter bar at the top, search for "subscriptions" and click Subscriptions.

Step 4 Create a subscription.

Provide all the required information to create a subscription.

Step 5 Create a new application.

This step is required for `Unmanaged` tenants only. If you are planning to add this tenant as a `Managed` tenant, you only need the subscription ID and can skip this step.

a) In the left side bar, click All services.
b) In the All services filter bar at the top, search for "registrations" and click App registrations.
c) In the main window, click +New registration.
d) In the Register an application screen, provide the information for your application.
e) Make a note of the Application (client) ID and Directory (tenant) ID fields values.
f) Click the Certificates & secrets, then click +New client secret.

Provide the secret's description and duration.

Once the secret is created, note the value.

Note The secret's value is only viewable immediately after you create it.

Cloud Site CIDR Information

Each VRF you define creates a VPC in Amazon Web Services or a VNET in Azure. CIDR is a cloud context profile configuration linked to the VRF and is broken up into one or more subnets used by your cloud endpoints. You will need to provide the CIDR and subnet information when you configure VRF.

Keep in mind that while you can define one or more subnets within a CIDR in AWS, you would need to define at least 2 subnets in Azure. This is because when you create subnets in Azure, one subnet is always used as a gateway subnet, so you would need an additional subnet for the endpoints.

In AWS, subnets are linked to availability zones (AZ) and you will need one subnet per availability zone.

Cloud Site CIDR Information	Example	Your Entry
CIDR prefix (AWS VPC or Azure VNET) and netmask	3.3.0.0/16	
Subnet information	Endpoints subnet: 3.3.2.0/24 (Azure only) Gateway subnet: 3.3.1.0/24	
Endpoint information	3.3.2.1/24	

Creating a Tenant

Use the following procedure to create a Tenant and associate it with your on-premises and cloud sites.

Before you begin

- You must have AWS account or Azure cloud services subscription active and available.
- If you are creating a brand new tenant for use with AWS, there is a one-to-one mapping between AWS user accounts and APIC tenants, so you must have a separate AWS user account created and ready to be used by the tenant. For more information, see Setting Up an AWS Account and User, on page 7.

Procedure

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 In the left navigation menu, click Tenants.

Step 3 In the main pane, click Add Tenant.

Step 4 In the Add Tenant window, provide a name for the tenant.

You may also choose to provide a description of the tenant.

Step 5 In the Associated Sites area, select the on-premises site where you want to add the tenant.

When associating with an on-premises site, simply check the checkbox next to the site.

(Optional) If you want to assign the tenant to a specific security domain, you can choose it from the dropdown menu.

Step 6 If you want to add this tenant to an AWS site, check the checkbox next to it.

When associating an AWS cloud site with a tenant, you must also provide the AWS user account information.

a) After you check an AWS site, select the security domain from the dropdown list if necessary.
b) Then click Associate Account next to it.
c) In the AWS Account ID field, provide the ID of the AWS user account you have created for this tenant.

This is the AWS account that you logged into when setting up the AWS account for Trusted Tenant using the CFT.

d) In the Access Type field, choose the type of AWS user account you have created.

- Select Trusted, if you set up the AWS account for Trusted Tenant using CFT.
- Select Untrusted, if you set up the AWS account for an Untrusted User Tenant using the AWS access key ID and secret access key. In this case you must also provide the following:
  - Cloud Access Key ID: Enter the AWS access key ID information for the user tenant in this field.
  - Cloud Secret Access Key: Enter the AWS secret access key information for the user tenant in this field.

Step 7 If you want to add this tenant to an Azure site, check the checkbox next to it.

When associating an Azure cloud site with a tenant, you must also provide the Azure subscription information.

a) After you check an Azure site, select the security domain from the dropdown list if necessary.

Note Security domain must be specified if you plan to share a subscription that is already used by another tenant. In that case, both tenants must be assigned to the same security domain.

b) Then click Associate Account next to it.

c) Choose tenant mode.

You can choose one of the following two modes when adding a tenant:

- Choose Mode: Select Shared, if you want to use an existing subscription that is shared with an existing tenant.

  Unlike AWS user accounts, where there is always a one-to-one mapping between AWS accounts and Cloud APIC tenants, Azure allows you to create multiple tenants using the same subscription.

  If you choose Select Shared, you can then select a subscription from the dropdown list and your new tenant will be associated with the same Azure subscription. Note that you must have a security domain configured for the tenants that share the subscription for it to show up in the dropdown list.

- Choose Mode: Create Own, if you want to associate the tenant with a new Azure subscription.

  Then in the Azure Subscription ID field, provide the ID of the Azure subscription.

  You can obtain the subscription ID by logging into your Azure account and navigating to Home > Subscriptions. Keep in mind, you must use the Subscription ID and not Subscription Name as listed in the Azure portal.

d) In the Access Type field, choose the access type between the Cloud APIC VM and the tenant.

- Select Managed Identity, to allow the Cloud APIC VM to manage the cloud resources.
- Select Unmanaged Identity, to manage the cloud resources via a specific application. In this case you must also provide the application's credentials to the Cloud APIC:
  - Application ID: Enter the application ID for the Azure application. This ID is listed in Home > App registrations > <application-name> > Application (client) ID field in the Azure portal.
  - Client Secret: Enter the application secret. You can create a secret under Home > App registrations > <application-name> > Certificates & secrets > New client secret.
  - Azure Active Directory ID: Enter the application directory ID for the Azure application. This ID is listed in Home > App registrations > <application-name>, in the Directory (tenant) ID field.

Step 8 In the Associated Users area, select which users have access to the tenant

Step 9 (Optional) Enable consistency checker.

You may choose to enable scheduled consistency checker for this tenant. Additional information about consistency check is available in the Cisco ACI Multi-Site Configuration Guide.

Note Consistency checker is available only for on-premises fabrics.

Step 10 Click Save to add the tenant.

Step 11 Verify that the tenant was successfully pushed to the on-premises APIC site:

a) Log into your on-premises APIC site.
b) On the menu bar, choose Tenants > All Tenants.
c) In the main pane, verify that the tenant you created in the previous step is displayed in the on-premises APIC site.

Step 12 Verify that the tenant was successfully pushed to the Cloud APIC site:

a) Log into your Cloud APIC site.
b) On the main Cloud APIC page, under Application Management, click Tenants.
c) Verify that the tenant that you just created through the ACI Multi-Site Orchestrator in the previous step is displayed in the Cloud APIC site.

You may need to click the Refresh button at the top right corner of the screen before your new tenant is displayed.

Creating a Schema and Templates

Use the following procedure to create a new schema for the Cloud APIC site. For this use-case example, we will configure a single schema and two templates, with one template for each site.

You are in the ACI Multi-Site Orchestrator for this entire procedure.

Procedure

Step 1 In the Main menu, click Schemas.

Step 2 On the Schema screen, click the Add Schema button.

Step 3 On the Untitled Schema screen, replace the text `Untitled Schema` at the top of the page with a name for the schema that you intend to create (for example, `schema-shared-services`).

Step 4 Configure the first template.

a) In the left pane, mouse over Template 1 and click the notepad icon. Then change the template's name, for example `template1-onprem`, `template1-aws`, or `template2-azure`.
b) In the middle pane, click the area To build your schema please click here to select a tenant.
c) In the right pane, access the Select A Tenant dialog box and choose the tenant that you created in Creating a Tenant, on page 9 from the drop-down menu.

Step 5 Configure the second template.

a) In the left pane, click the + sign next to Templates to add another template.
b) Mouse over the new template and click the notepad icon. Then change the template's name, for example `template2-onprem`, `template2-aws`, or `template2-azure`..
c) In the middle pane, click the area To build your schema please click here to select a tenant.
d) In the right pane, access the Select A Tenant dialog box and choose the tenant that you created in Creating a Tenant, on page 9 from the drop-down menu.

Associating Templates with Sites

Use the following procedure to associate the templates with the appropriate sites.

Procedure

Step 1 In the left pane, click the + icon next to Sites.

Step 2 In the Add Sites window, check the checkbox next to your on-premises site and your cloud site.

Step 3 From the Assign to Template dropdown next to each site, select the appropriate templates.

This use-case example uses two separate templates, so you would add the cloud template to the cloud site and the on-premises template to the on-premises site.

However, if you also choose to stretch your on-premises VRF into the cloud, you can add the on-premises template to both sites.

Step 4 Click SAVE

Creating VRFs for Shared Services

When configuring shared services, you must create two separate VRFs.

Procedure

Step 1 Configure the on-premises or stretched VRF.

a) In the left pane, select the on-premises template you created.
b) In the middle pane, scroll down until you see the VRF area, then click + in the dotted box.
c) In the right pane, enter the VRF name in the DISPLAY NAME field (for example, `on-premises-vrf`).

If you plan to stretch this VRF between on-premises and cloud sites, you can name it `stretched-vrf` instead.

d) Click SAVE.

Step 2 Configure the cloud VRF.

a) In the left pane, select the cloud template you created.
b) In the middle pane, scroll down until you see the VRF area, then click + in the dotted box.
c) In the right pane, enter the VRF name in the DISPLAY NAME field (for example, `cloud-vrf`).
d) Click SAVE.

Configuring Cloud Region and CIDR

After you add a cloud site to your schema, you can associate a CIDR with the cloud VRF.

Procedure

Step 1 In the left pane, select the template under the cloud site that you have added.

Because you configure the CIDR information at the site-local level, you must select the template under the Sites category on the left, not from the general Templates category.

Step 2 In the middle pane, scroll down to the VRF area, then click the VRF you created.

Step 3 In the right pane, under the Site Local Properties click Regions + to add a region. Then select the region from the dropdown menu.

Step 4 In the right pane, under the Site Local Properties click + CIDR).

Step 5 Click Save.

Step 6 Enter the CIDR information for the VRF.

If it's the first CIDR you are adding for the region, select Primary. Otherwise, select Secondary.

Step 7 Click +Subnet to add a subnet to the CIDR.

Note The subnets you configure for your cloud site must be different from the subnets you configure for the on-premises bridge domain.

If you are configuring this for an AWS cloud, you can provide one or more subnets. In addition, if you have configured more than one availability zone for your AWS site, you must add one subnet per availability zone.

If you are configuring this for an Azure cloud, you must provide at least two different subnets. In this case, you will also have to designate one of the subnets to be used as the gateway subnet while the other subnets can be used for the cloud endpoints.

Step 8 Click SAVE.

Creating a BD and Associating It with On-Premises VRF

After you create an on-premises VRF, you create the bridge domain (BD) and associate it with the VRF.

Procedure

Step 1 In the left side bar, make sure you have selected the correct template.

For example, if you created a separate template for on-premises objects, create the BD in that template.

Step 2 In the middle pane, scroll down until you see the Bridge Domain area, then click + in the dotted box to add the on-premises BD.

Step 3 In the right pane, enter a name for the bridge domain in the Display Name field (for example, `bd-onprem`).

Step 4 In the right pane, in the Virtual Routing & Forwarding field select the VRF you created, for example `vrf-onprem`.

Step 5 In the right pane, scroll down to Subnets and click +Subnet to add a classification subnet.

In the Add Subnet dialog:

a) Enter the gateway IP address and the netmask.

Specify the subnet information that you have prepared in APIC Bridge Domain Information, on page 5.

b) Set the Scope to `Advertised Externally`.

The scope must be set to advertise externally to exchange the prefix information between the on-premises and cloud sites.

c) Check the Shared Between VRFs checkbox.

You must enable this option because you are configuring shared services between different VRFs.

d) Click SAVE to add the subnet.

Step 6 Click SAVE.

Creating a Filter for Shared Services Contract

This section describes how to create a filter for the contract that will be used between the cloud EPG and the on-premises EPG.

Procedure

Step 1 Select the template where you want to add the filter.

While we are configuring two separate templates, the filter and the contract can be added to either template.

Step 2 In the middle pane, scroll down to the Filter area, then click + to create a filter.

Step 3 In the right pane, enter the filter name in the Display Name field (for example, `ICMP`).

Step 4 In the right pane, click + Entry.

Step 5 In the Add Entry window, provide the details

a) In the Name field, provide the name for the filter entry.

b) In the Ethertype field, select the type, for example `ip`.

c) In the IP Protocol field, select the protocol, for example `icmp`.

d) Leave the Destination Port Range From field unspecified.

e) Leave the Destination Port Range To field unspecified.

f) Click SAVE to save the filter.

Creating a Contract for Shared Services

This section describes how to create a contract that will be used between the cloud EPG and the on-premises EPG for shared services use-case.

Procedure

Step 1 Select the template where you want to add the contract.

While we are configuring two separate templates, the filter and the contract can be added to either template.

Step 2 In the middle pane, scroll down to the Contract area, then click + to create a contract.

Step 3 In the middle pane, locate the Contract area, then click + to create a contract.

Step 4 In the right pane, enter the contract name in the Display Name field (for example, `contract-shared-services`).

Step 5 In the right pane, scroll down to the Filter Chain area and click + Filter to add a filter to the contract.

Step 6 From the Scope dropdown menu, change the scope of the Contract to `tenant`.

Step 7 In the Add Filter Chain window that opens, select the filter you added in previous section from the Name dropdown menu.

Creating Application Profile and Cloud EPG

This section describes how to create an Application Profile and a cloud EPG.

Procedure

Step 1 In the left side bar, select the correct template.

If you created a separate template for cloud objects (for example, `template-cloud`), create the EPG in that template.

Step 2 In the middle pane, locate the Application profile area, then click + Application Profile.

Step 3 In the right pane, enter the Application Profile name in the Display Name field (for example, `app1`).

Step 4 In the middle pane, click + Add EPG.

Step 5 In the right pane, enter an EPG name in the Display Name field (for example, `epg-cloud`).

Step 6 In the right pane, scroll down to the Cloud Properties section.

Step 7 From the Virtual Routing & Forwarding dropdown, select the cloud VRF you created.

Step 8 Configure the endpoint selector for the EPG as described in the next section.

Adding Cloud Endpoint Selector

On the Cloud APIC, a cloud EPG is a collection of endpoints that share the same security policy. Cloud EPGs can have endpoints in one or more subnets and are tied to a CIDR.

You define the endpoints for a cloud EPG using an object called endpoint selector. The endpoint selector is essentially a set of rules run against the cloud instances assigned to either AWS VPC or Azure VNET managed by the Cloud APIC. Any endpoint selector rules that match endpoint instances will assign that endpoint to the Cloud EPG.

Unlike the traditional on-premises ACI fabrics where endpoints can only belong to a single EPG at any one time, it is possible to configure endpoint selectors to match multiple Cloud EPGs. This in turn would cause the same instance to belong to multiple Cloud EPGs. However, we recommend configuring endpoint selectors in such a way that each endpoint matches only a single EPG.

Configuring actual endpoints is described in the following two sections:

- Configuring endpoints in an AWS cloud site, see Endpoints in AWS Cloud, on page 19
- Configuring endpoints in an Azure cloud site, see Endpoints in Azure Cloud, on page 20

Procedure

Step 1 In the Multi-Site Orchestrator, select the EPG.

Step 2 In the right pane, in the Site Local Properties area, click + Selector under the Selectors heading to configure the endpoint selector.

If you plan to stretch this EPG, you can also choose to add the endpoint selector at the template level instead.

Step 3 In the Add New End Point Selector form, enter a name in the End Point Selector Name field, based on the classification that you use for this endpoint selector.

For example, for an endpoint selector with the IP Subnet classification, you might use a name such as `IP-Subnet-EPSelector`.

Step 4 Click + Expression, then use the three fields to configure the endpoint selector based on how you want to classify the endpoints in the cloud:

The Type field determines the expression that you want to use for the endpoint selector:

- Choose IP Address if you want to use an individual IP address or a subnet for the endpoint selector.

  Note If the endpoints are Azure scale sets and the selector is IP based, the selector must exactly match the subnet where the scale set is placed. For example, if you configured `10.1.0.0/16` CIDR, `10.1.0.0/24` subnet, and the scale set is in this subnet, then the IP selection must match `10.1.0.0/24` exactly and not a wider mask such as `10.1.0.1/32`.

- Choose Region if you want to use the cloud region for the endpoint selector, then choose the specific region that you want use.

  When you select `Region` for the endpoint selector, every instance within the tenant that is brought up in that region will be assigned to this cloud EPG.

- Choose Zone if you want to use the Amazon Web Services availability zone for the endpoint selector, then choose the specific zone that you want use.

  When you select `Zone` for the endpoint selector, every instance within the tenant that is brought up in that zone will be assigned to this cloud EPG.

  Note This selector type is supported only for AWS cloud sites.

- Choose Custom tags or labels if you want to create a custom tag or label for the endpoint selector. Start typing to enter the custom tag or label, then click Create on the new field to create a new custom tab or label.

The Operator field determines the relation between the type and its value:

- Equals: Used when you have a single value in the Value field.
- Not Equals: Used when you have a single value in the Value field.
- In: Used when you have multiple comma-separated values in the Value field.
- Not In: Used when you have multiple comma-separated values in the Value field.
- Has Key: Used if the expression contains only a key.
- Does Not Have Key: Used if the expression contains only a key.

The Value field determines the collection of endpoints that you want to use for the endpoint selector, based on the choices that you made for the two previous fields. This can be a single IP address, a subnet, AWS region or zone, or a custom tag value.

For this use case, you will be assigning endpoints based on IP subnets, so you will configure the endpoint selector using the following example values:

- Type: `IP Address`
- Operator: `Equals`
- Value: `3.3.1.0/24`

Step 5 Click the checkmark next to the new endpoint selector.

Step 6 Click Save in the Add New End Point Selector form.

Creating Application Profile and On-Premises EPG

This section describes how to create an Application Profile and a cloud EPG.

Procedure

Step 1 In the left side bar, select the correct template.

If you created a separate template for on-premises objects (for example, `template-onprem`), create the EPG in that template.

Step 2 In the middle pane, locate the Application Profile area, then click + Application Profile.

Step 3 In the right pane, enter the application profile name in the Display Name field (for example, `app1`).

Step 4 In the middle pane, click + Add EPG.

Step 5 In the right pane, enter an EPG name in the Display Name field (for example, `epg-onprem`).

Step 6 In the right pane, scroll down to the On-Prem Properties section.

Step 7 From the Bridge Domain dropdown menu, select the bridge domain you have created.

Step 8 Configure a subnet for the EPG.

You must configure the subnet at the EPG level.

a) Select the EPG.
b) In the SUBNETS area, click +Subnet.
c) Enter the gateway IP address and the netmask.
d) Set the Scope to `Advertised Externally`.

The scope must be set to advertise externally to exchange the prefix information between the on-premises and cloud sites.

e) Check the Shared Between VRFs checkbox.

You must enable this option because you are configuring shared services between different VRFs.

f) Click SAVE to add the subnet.

On-Premises Endpoints

Multi-Site Orchestrator allows you to provision assignment of endpoints to physical (static port configuration) or virtual (VMM) domains. This section provides an example of how to assign endpoints to an EPG based on a VMM domain (VMware). It is assumed that you have the VMM domain already set up and configured in you on-premises site.

Procedure

Step 1 In the left sidebar, under Templates, select the template that contains your EPG.

If you created a separate templates for on-premises, cloud, or stretched objects, make sure to select the template that contains your on-premises EPG, for example `template-onprem`.

Step 2 In the middle pane, click the EPG.

Step 3 In the right pane, under the Site Local Properties heading, in the Domains area, click + Domain.

Step 4 Enter the necessary information in the Add Domain form:

- In the Domain Association Type field, choose a type.

  For example, you might select VMM for the domain association type.

- In the Domain Profile field, choose the profile for the on-premises domain that you want to use, using domain profile selections that are based on the domain association type that you entered in the previous step.

  For example, you might select a domain profile that was created based on VMware vDS, with a name such as `OnPrem-vDS`.

- In the Deployment Immediacy field, choose On Demand.
- In the Resolution Immediacy field, choose On Demand.

Click Save.

Adding Contract Between Cloud and On-Premises EPGs

This section describes how to add the shared services contract between the cloud and on-premises EPGs you have created.

Procedure

Step 1 Add the contract to the on-premises EPG.

a) In the middle pane, select the on-premises EPG you created.
b) In the right pane, scroll down to the Common Properties area and click +Contract.
c) In the Add Contract window that opens, select the contract you created and its type, then click SAVE.

Step 2 Add the contract to the cloud EPG.

a) In the middle pane, select the cloud EPG you created.

b) In the right pane, scroll down to the Common Properties area and click +Contract.
c) In the Add Contract window that opens, select the contract you created and its type, then click SAVE.

Deploying to Sites

Once you have completed all of the other configuration tasks, deploy the templates you have configured to the sites.

Procedure

Step 1 Click on the Deploy to Sites button at the top right corner of the screen to deploy the templates to the sites.

Confirmation window will appear.

Step 2 Confirm the deployment.

The confirmation window lists the changes that will be made for each site. After you confirm the deployment, you should see a message saying `Successfully Deployed`.

Endpoints in AWS Cloud

This task describes how to create an AWS cloud endpoint (VM) with appropriate endpoint selector information that you defined when creating the cloud EPG in the Multi-Site Orchestrator.

Procedure

Step 1 Log in to the Amazon Web Services account.

Step 2 In the AWS Management Console, click All services.

Step 3 From All services, select Computer > EC2.

Step 4 Click Launch Instance to create a new instance (VM).

Step 5 Then select the type of instance you want to create and provide the required information.

Based on the endpoint selector you have chosen for the cloud EPG you created, specify one or more of the following parameters for the EC2 instance:

- If you plan on assigning endpoints based on an IP subnet, use the CIDR and subnet information you have specified in the endpoint selector.
- If you plan on assigning endpoints based on an Amazon Web Services region or zone, configure an appropriate Availability Zone for each instance.

  For example, you would use `us-west-1` for AWS region or `us-west-1a` for an availability zone.
- If you are assigning endpoints based on a custom tag or label, select the Tags tab and click Add/Edit Tags to create a new tag.

  Then enter the same value you chose in the Value field of the endpointer selector.

Endpoints in Azure Cloud

This task describes how to create an Azure cloud endpoint (VM) with appropriate endpoint selector information that you defined when creating the cloud EPG in the Multi-Site Orchestrator.

Procedure

Step 1 Log in to the Azure account.

Step 2 Navigate to Home > All services > Virtual Machines.

Step 3 Click +Add to create a new virtual machine.

Step 4 In the Create a virtual machine screen, provide the appropriate information based on the endpoint selector you created.

Provide all the required information, such as virtual machine name, size, administrator account, etc.

In the Subscription dropdown, select the subscription where you created your tenant.

If you are assigning endpoints based on an IP subnet, choose the subnet created by the Multi-Site Orchestrator.

If you plan on assigning endpoints based on a custom tag or label, choose a VM, then click the Tags tab on the left. Use an existing tag in this area, or click Add/Edit Tags to create a new one. You will use the entry in the Value field for this tag for the custom tag or label for the endpoint selector.

Verifying Shared Services Configuration

Use the following procedure to verify that shared service was properly configured between the cloud EPG and the on-premises EPG.

Procedure

Step 1 In the on-premises APIC GUI: Verify that the configurations were deployed successfully in the on-premises APIC site:

a) Choose the tenant that you created in Creating a Tenant, on page 9.
b) Expand Application Profiles > ***<profile-name>*** > Application EPGs.
c) Verify that you see the application EPG that you created earlier under the Application EPGs area.
d) Expand Networking > Bridge Domains > ***<bd-name>*** > Subnets.
e) Verify that you see the subnet that you defined earlier under your bridge domain.

Step 2 In the Cloud APIC GUI: Verify that the configurations were deployed successfully on your Cloud APIC:

a) Navigate to Application Management > Application Profiles and verify that the application profile has been created.
b) Navigate to Application Management > EPGs and verify that the EPG has been created.

Step 3 In the Cloud APIC GUI: Verify that the end points were deployed successfully for your EPG on your Cloud APIC:

a) Navigate to Application Management > EPGs and verify that the EPG has been created.
b) In the Name column, locate the EPG that you created earlier, then locate the entry under the Endpoints column for this EPG.

The number shown in this column should match the number of endpoints that you have for this EPG. You might have to click the Refresh button at the top right corner of the screen (the circle with an arrow) to refresh the screen before the number is displayed properly in this column.

c) Click the number in this Endpoints column to bring up more information on the endpoints for this EPG.
d) Verify that the information that you used in the endpoint selector is being used for this endpoint.

Step 4 Verify that the cloud EPG has the correct contract configured.

a) Navigate to Application Management > EPGs and click on the cloud EPG you created.
b) In the Application Management tab, verify that the contract you configured is associated with the EPG.

Step 5 In the AWS management console: Verify that the CIDR configurations that you entered were pushed successfully to AWS:

a) Go to Services > VPC.
b) In the Resources by Region area, click VPCs.
c) Verify that the CIDR is listed under the IPv4 CIDR column.
d) If you used IP subnet for the endpoint selector, click Subnets in the left pane, then verify that the subnets are shown under the IPv4 CIDR column.

Step 6 In the AWS management console: Verify that EC2 instance brought up is classified in the correct security group (EPG):

a) Select the instance from AWS, the click the Description tab.
b) Locate the Security Groups field in the Description area and verify that you can see the application profile and EPG classification.

Step 7 In the Azure portal: Verify that the CIDR configurations that you entered were pushed successfully to Azure:

a) Go to All services > Virtual Networks.
b) Select the virtual network (VNET).
c) Verify that the CIDR is listed in the Address space field.
d) If you used IP subnet for the endpoint selector, click Subnets in the left pane, then verify that the subnets are shown in the Address range column.

Step 8 In the Azure portal: Verify that VMs were brought up successfully and classified in the correct network security group:

a) Go to All services > Virtual Machines.
b) Select the virtual machine.
c) In the left pane, select Settings > Networking.
d) In the description, verify that the correct network security group is listed.

Trademarks

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.