Configuring VNet Peering for Cloud APIC for Azure

Revised: February 19, 2022,

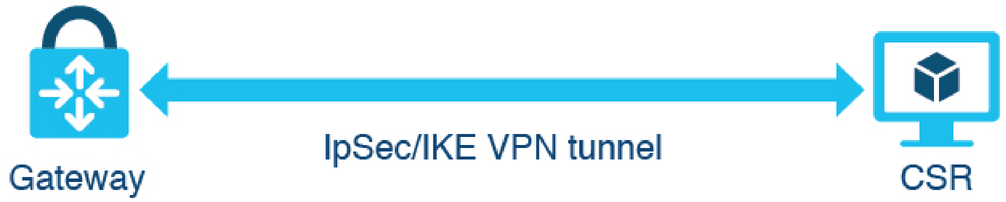
New and Changed Information

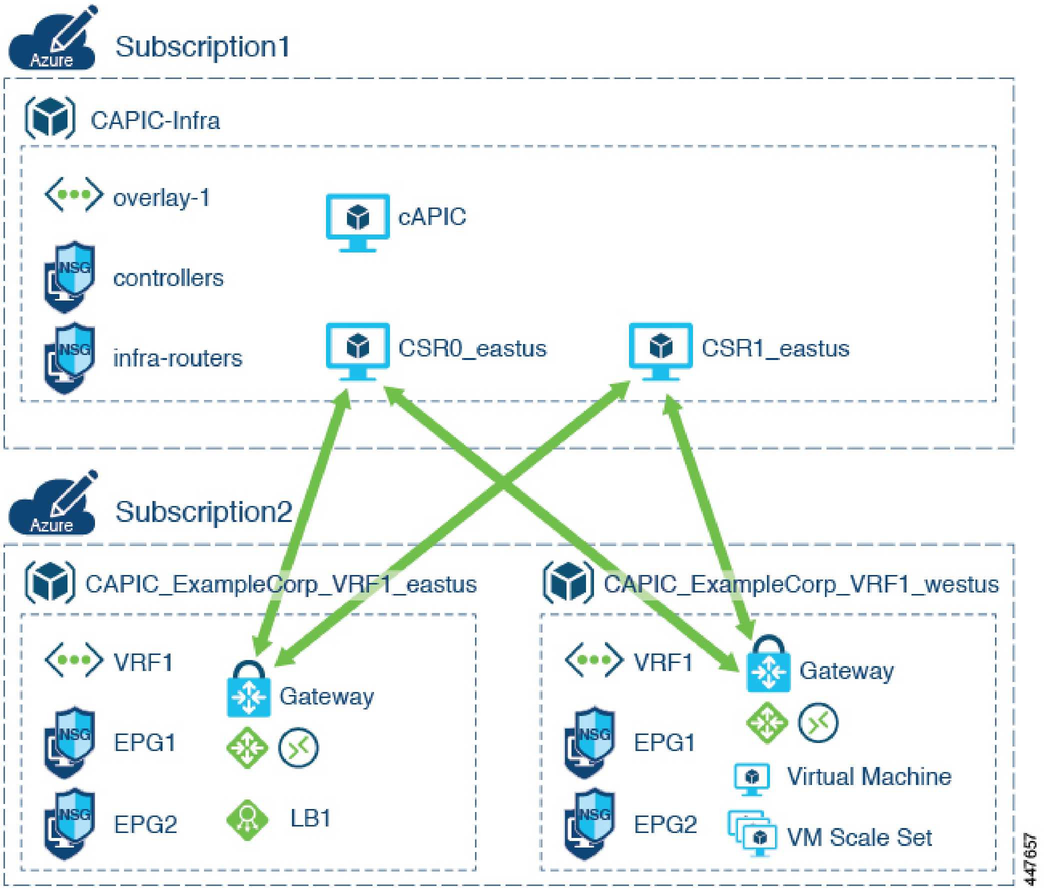
The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Cisco APIC Release Version	Feature	Description
5.2(1)	Support is available for VNet peering across Azure ADs, so spoke VNets can be deployed in different subscriptions in different Azure ADs.	• In releases prior to release 5.2(1), you must deploy the infra (hub) and spoke VNets in the same Azure AD, but you can deploy the infra and spoke VNets in different subscriptions within the same Azure AD. • Beginning with release 5.2(1), support is now available for VNet peering across Azure ADs, so spoke VNets can be deployed in different subscriptions in different Azure ADs. See Support for VNet Peering Across Azure Active Directories, on page 9 for more information.
5.1(2)	Azure VNet peering at the global level is enabled by default and cannot be disabled.	• For releases prior to release 5.1(2), you can manually enable Virtual Network Peering at the global level in the Connectivity for Internal Network area. • For release 5.1(2) and later, VNet peering at the global level is enabled by default and cannot be disabled.
5.0(2)	Support for Azure VNET peering in Cisco Cloud APIC	This release provides support for Azure VNET peering in Cisco Cloud APIC.

Data Forwarding Between VNets

Prior to Release 5.0(2), the solution for inter-VNet communication in a Cisco Cloud APIC uses a hub-spoke overlay topology with IPsec tunnels between a pair of Cisco CSR routers in the infra VNet and a Virtual Network Gateways (VNG) in the user VNet. BGP runs over the IPsec tunnels as the routing protocol between the CSR routers and the VNG.





This implementation has several limitations:

- Azure VPN gateway is an expensive and heavy Azure resource
- Every user VNet must deploy an Azure VPN gateway in order to forward the traffic to a CSR
- Each VPN tunnel offers limited bandwidth (1.25 Gbps), which limits the total throughput
- Creating a virtual network gateway (VPN gateway) can take up to 45 minutes to complete

Beginning in Release 5.0(2), Cisco Cloud APIC supports using Azure VNet peering for inter-VNet connectivity. Azure VNet peering is a service that functions as an internal router to automate connectivity between virtual networks (VNets). The VNets can be in different Azure regions in a cloud site.

VNet peering provides a low-latency, high-bandwidth connection useful in scenarios such as cross-region data replication and database failover. Since traffic is private and remains on the Microsoft backbone, if you have strict data policies, VNet peering becomes preferable because the public internet isn't involved. Since there's no gateway in the path, there are no extra hops, ensuring low-latency connections.

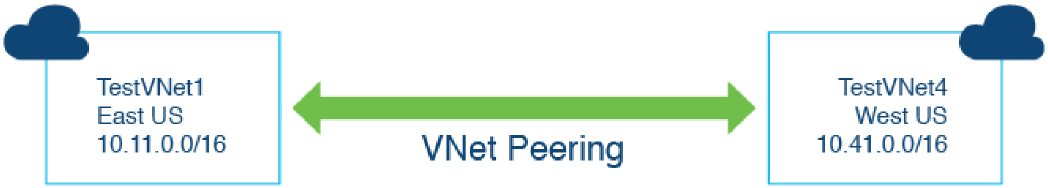
Azure VNet peering, similar to a Cisco CSR, is owned by the infra tenant. However, it’s shared with multiple user accounts.

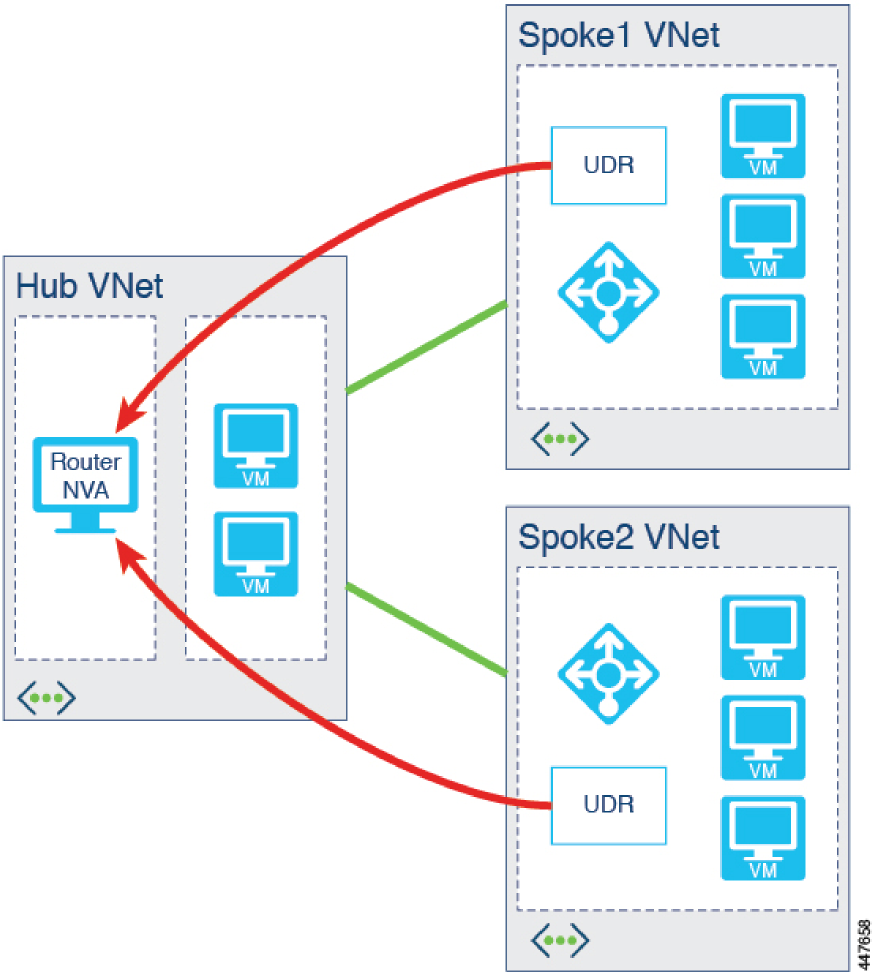
Cisco APIC Release 5.0(2) is backward-compatible with previous methods of configuring communication between VNets.

About VNet Peering

Virtual network (VNet) peering enables seamless connection between two Azure Virtual Networks and is Microsoft's recommended way of forwarding data between two VNets. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only. Peerings are bidirectional.

Peering connections are non-transitive. For example, assume three VNets (A, B, and C), where A is bidirectionally peered with B, and B is with C. This does not mean A and C are peered with each other.





Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.

The benefits of using virtual network peering include:

- A low-latency, high-bandwidth connection between resources in different virtual networks.
- The ability for resources in one virtual network to communicate with resources in a different virtual network.
- No downtime to resources in either virtual network when creating the peering, or after the peering is created.
- Much higher traffic throughput compared to IPSec tunnels.

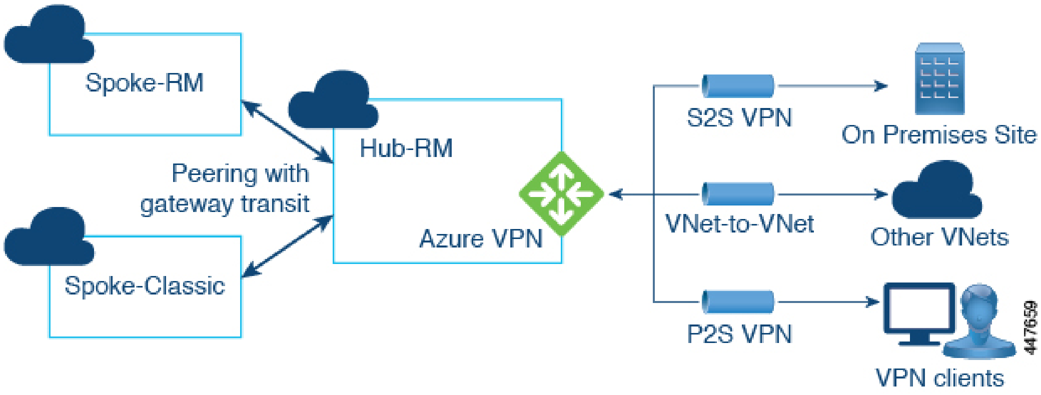
For more information on VNet peering, see the article ***Virtual network peering*** in the Documentation section in the Azure website.

Cisco Cloud APIC Implementation of VNet Peering

Cisco Cloud APIC uses several components to implement VNet peering.

Hub and Spoke Topology

Cisco Cloud APIC uses a hub and spoke topology for VNet peering rather than a full-mesh topology because a hub-spoke topology is easier to manage. In the hub-spoke topology, all the user VNets peer with a central hub VNet, forming a full hub and spoke topology.



A CSR acts as the network virtual appliance (NVA) in the hub and routes the packets from one VNet to another VNet, and also forms the VXLAN tunnels toward the on-premises site. This kind of connection provides full bandwidth between Azure VNets as supported by your datacenter.

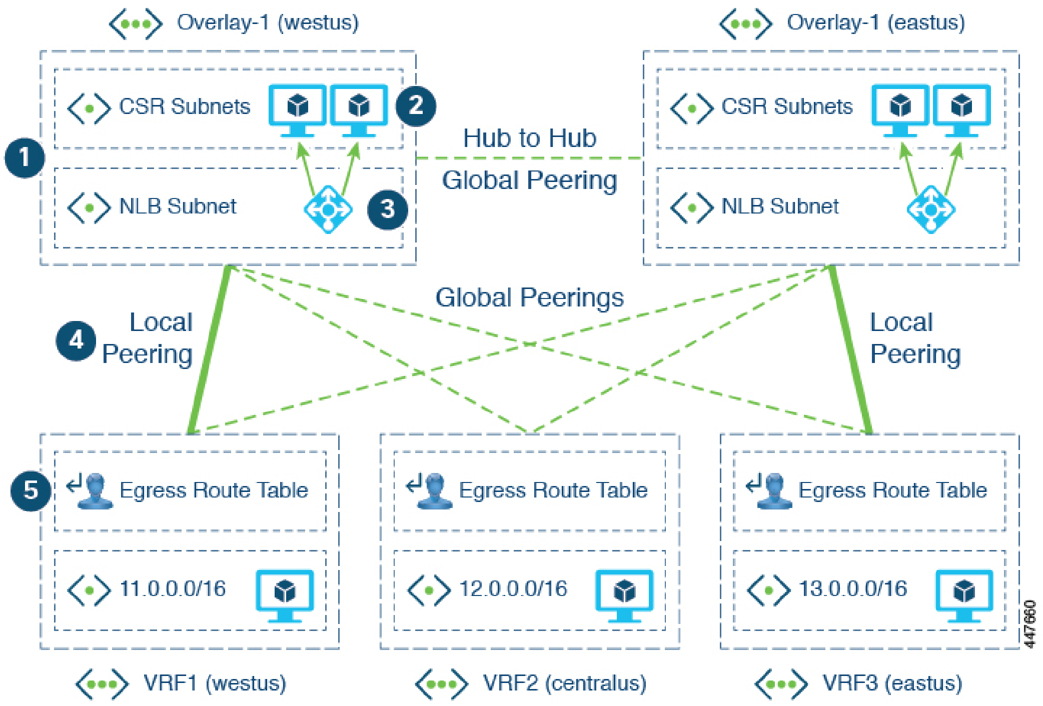
User-Defined Routes

As mentioned previously, peering connections with Azure VNet peering are non-transitive. Since spokes are not peered with each other, Cisco Cloud APIC uses user-defined routes (UDRs) on each user VNet to forward traffic to other VNets.

UDRs are used to override Azure's default system routes, or to add additional routes. UDRs for the spoke are added to a subnet's route table, with the next-hop pointing to the NLB of the NVA (CSR) in the hub.

Cloud APIC Implementation

The following figure shows how Cloud APIC typically implements VNet peering.



Where:

1. Infra VNets act as the hub, and tenant VNets act as the spokes. Bi-directional peering is used between each hub-spoke pair.

2. CSRs in the hub VNet act as the NVAs for spoke-to-spoke routing.

3. An Azure network load balancer (NLB) is placed in front of the CSRs to perform load-balancing and failover.

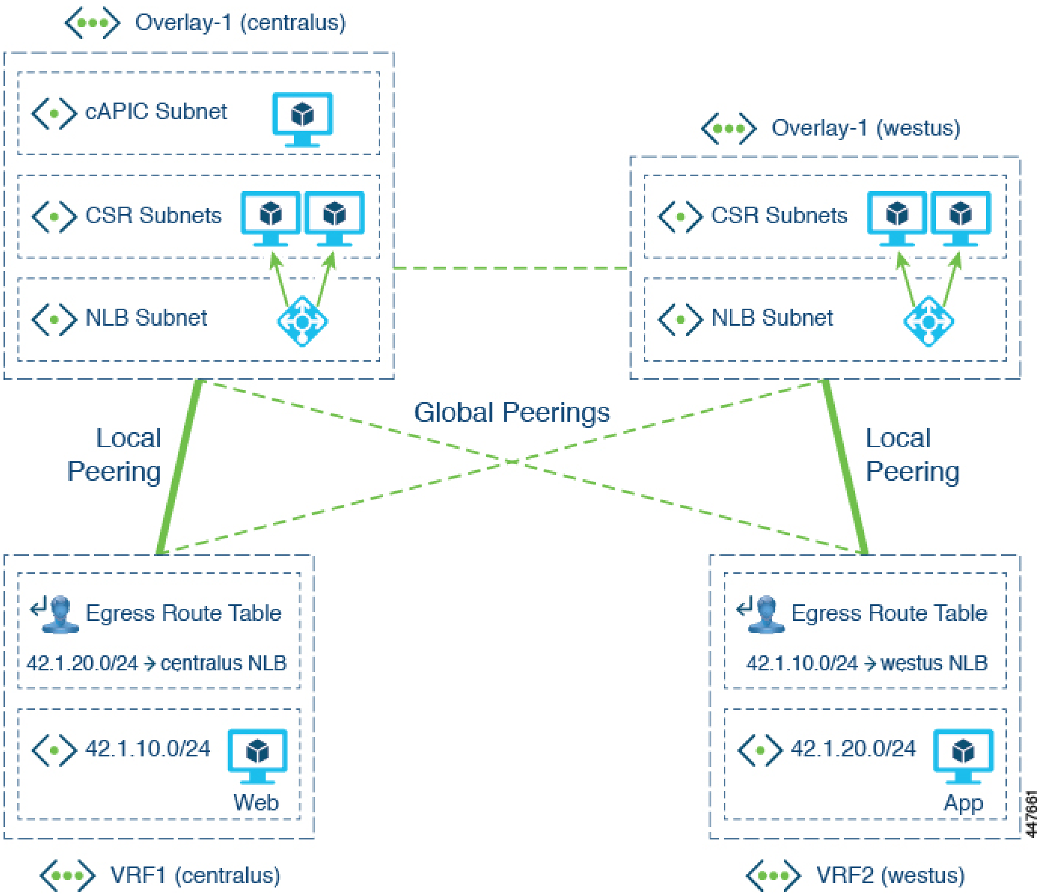
4. In a multi-region cloud site on Azure, each region can have its own hub VNet (infra VNet with a pair of CSRs and a NLB), or can share the hub VNet in other regions. All spoke VNets are peered with all hub VNets, across regions. The types of peerings are:

   - Local peering: Peering with hub in the same Azure region

   - Global peering: Peering with hubs in different Azure regions

5. The UDR in the spoke VNets redirect traffic to the CSR NLB for traffic destined to other spokes or sites.

For example:



In this example:

- Spoke-1: VRF1 (42.1.10.0/24)
- Spoke-2: VRF2 (42.1.20.0/24)

A UDR is needed in each spoke's route table, with one UDR per CIDR in the destination VRF. The next-hop for the UDR is the IP address of the NLB, where the routes with the local NLB are preferred over those with remote NLBs.

In the Cloud APIC implementation of VNet peering:

- For the hub-to-hub peerings:
  - All of the hub VNets are peered with each other
  - There is bi-directional peering between each pair of hub-hub VNets
- For the hub-to-spoke peerings:
  - The infra VNets act as the hubs
  - The tenant VNets act as the spokes
  - There is bi-directional peering between each pair of hub-spoke VNets
- For the global vs local peerings:

- A tenant VNet (spoke) is peered with all of the infra VNets (hubs)
- Local peering: Peering with a hub in the same region
- Global peering: Peering with a hub in a different region

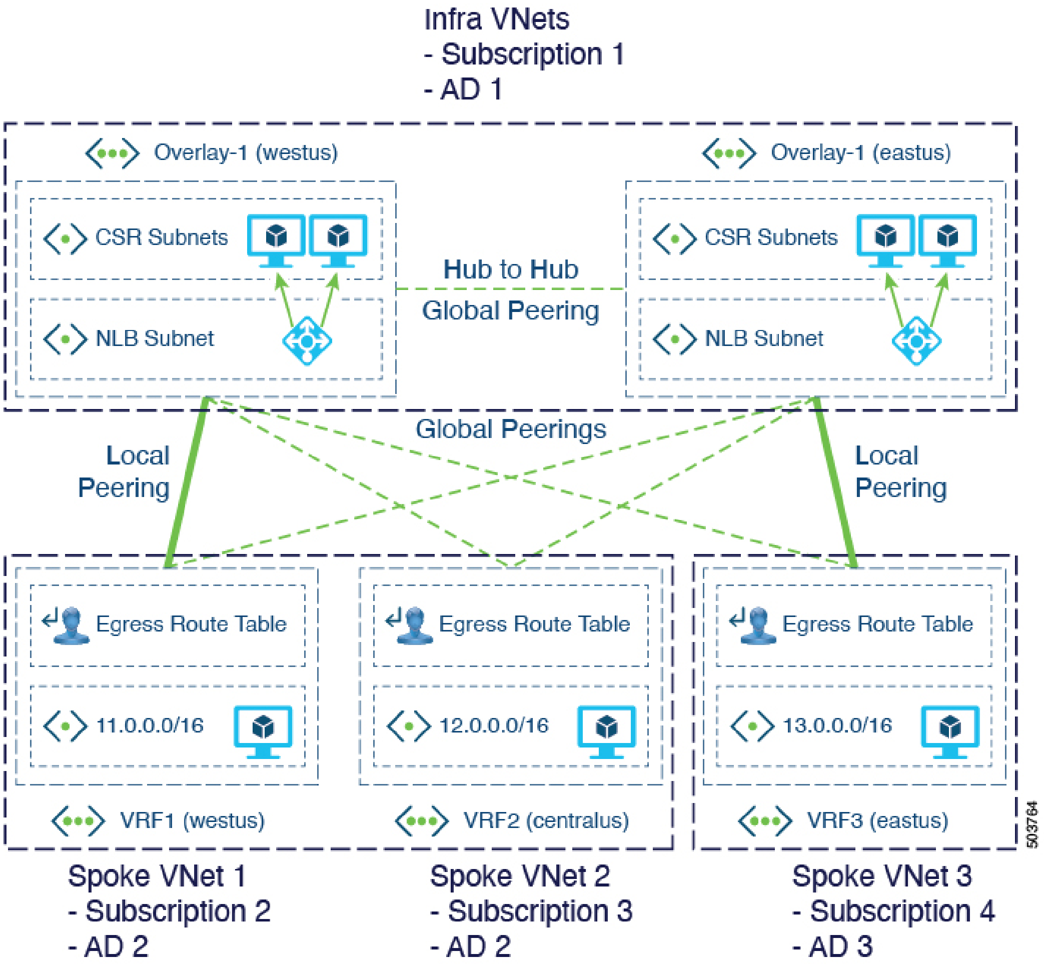
Support for VNet Peering Across Azure Active Directories

With the VNet peering solution available for releases prior to release 5.2(1), there is a limitation in that VNet peering cannot be established between two VNets that belong to different subscriptions corresponding to different Azure Active Directories. Azure Active Directory (Azure AD) is Microsoft's enterprise cloud-based identity and access management (IAM) solution. An Azure subscription has a trust relationship with Azure AD. A subscription trusts Azure AD to authenticate users, services, and devices.

Multiple subscriptions can trust the same Azure AD, but each subscription can only trust a single Azure AD. One or more Azure subscriptions can establish a trust relationship with an instance of Azure AD in order to authenticate and authorize security principals and devices against Azure services. When a subscription expires, the trusted instance of the Azure AD service remains, but the security principals lose access to Azure resources.

- In releases prior to release 5.2(1), you must deploy the infra (hub) and spoke VNets in the same Azure AD, but you can deploy the infra and spoke VNets in different subscriptions within the same Azure AD.
- Beginning with release 5.2(1), support is now available for VNet peering across Azure ADs, so spoke VNets can be deployed in different subscriptions in different Azure ADs.

The following figure shows an example configuration where VNet peering is enabled across Azure ADs.



In the example configuration in this figure, each dotted brown box represents a distinct Azure AD boundary, where:

- Both of the infra VNets belong to Subscription 1, and Subscription 1 belongs to Azure AD 1
- The spoke VNets belong to these subscriptions and ADs:
  - Spoke VNet 1: Belongs to Subscription 2, and Subscription 2 belongs to Azure AD 2
  - Spoke VNet 2: Belongs to Subscription 3, and Subscription 3 also belongs to Azure AD 2
  - Spoke VNet 3: Belongs to Subscription 4, and Subscription 4 belongs to Azure AD 3
- Local peerings and global peerings behave as they did prior to release 5.2(1), as described in Cisco Cloud APIC Implementation of VNet Peering, on page 6

If you want to configure VNet peering across Azure ADs, you must make the following configurations:

- Both the infra tenant and the user tenants must use only the service principal option. VNet peering across Azure ADs can only be achieved by using the service principal mode of authorization on Azure. For more information, see Configuring Infra and User Tenants With Service Principal Mode of Authorization, on page 12.

Note The managed identity option is still supported for infra and user tenants if you do not configure VNet peering across Azure ADs.

- You must make the necessary Contributor role configurations:
  - You must configure the Contributor role on the infra subscription for the service principal associated with the infra tenant.
  - You must configure the Contributor role on the tenant subscription for the service principal associated with the user tenant.
- You must also make the necessary Network Contributor role configurations:
  - You must configure the Network Contributor role on the tenant subscription for the service principal associated with the infra tenant.
  - You must configure the Network Contributor role on the infra subscription for the service principal associated with the user tenant.

Following is an example scenario to illustration these configurations. Assume that we have VNet A1, which belongs to the following:

- Subscription S1
- Azure active directory 1 (AD 1)
- Infra tenant

And assume we have VNet B1, which belongs to the following:

- Subscription S2
- Azure active directory 2 (AD 2)
- User tenant

To peer these two VNets, you would need to use service principal for both the infra tenant and the user tenant. For example:

- The infra tenant uses subscription S1 with access credentials/service principal SP-infra
- The user tenant uses subscription S2 with access credentials/service principal SP-user

Both of these service principals should have Contributor roles on their respective subscriptions to allow the Cisco Cloud APIC to make the calls to create the VNets and establish the VNet peering, where you would make the following configurations:

- Assign SP-infra Contributor role on Subscription S1.
- Assign SP-user Contributor role on Subscription S2.

However, in order to point the peering toward opposite VNets and make the VNet peering connection successful, you also need to make the following configurations:

- Assign SP-infra Network Contributor role on Subscription S2 for establishing the hub to spoke peering link.
- Assign SP-user Network Contributor role on Subscription S1 for establishing the spoke to hub peering link.

To make these configurations, you would export SP-infra in AD 1 into AD 2. Similarly, you would also export SP-user in AD 2 into AD 1.

The following link provides an example on exporting service principals across ADs using PowerShell:

How to export Service Principal to different AD

Considerations When Upgrading to Release 5.2(1)

For releases prior to release 5.2(1), the Cisco Cloud APIC virtual machine will have a Contributor role assigned for the subscription for the infra tenant. If you upgrade from a previous release to release 5.2(1) and you want to configure VNet peering across Azure ADs, you will have to make the following manual changes through the Cisco Cloud APIC GUI:

- Change the Access Type mode to Service Principal for the infra tenant
- Provide the service principal details for the infra tenant

See Configuring Infra and User Tenants With Service Principal Mode of Authorization, on page 12 for more information.

After you have made those changes, you can remove the Contributor role for the Cisco Cloud APIC virtual machine on the necessary subscriptions in the Azure portal.

Guidelines and Limitations for Azure VNet Peering Across Azure Active Directories

Note The following guidelines and limitations apply specifically for the VNet peering across Azure ADs enhancement available in release 5.2(1). For general guidelines and limitations for Azure VNet peering with Cisco Cloud APIC, see Guidelines and Limitations for Azure VNet Peering, on page 27.

With the VNet peering across Azure ADs enhancement available in release 5.2(1), the following guidelines and restrictions apply:

- The following are allowed when configuring VNet peering across Azure ADs:
  - Infra VNets and spoke VNets can be in different Azure ADs
  - Spokes can be spread across different subscriptions across different Azure ADs
- The following are not allowed when configuring VNet peering across Azure ADs:
  - Infra VNets in a given site cannot be deployed or split across different subscriptions. All infra VNets in a site must belong in the same subscription, which means that all infra VNets in a site must also belong in the same Azure AD.
- The managed identity option is not supported for infra and user tenants when using VNet peering across Azure ADs (service principal must be used instead in this situation).

Configuring Infra and User Tenants With Service Principal Mode of Authorization

These procedures describe how to configure the infra and user tenants with a service principal mode of authorization.

As part of this process, you will create a new App registration of the type multitenant in the active directory, and you will provide the following pieces of information:

- Subscription ID
- Application (client) ID
- Client secret

- Directory (tentant) ID

At the end of this process, you will run an az command that is provided to you by the service provider.

The procedures for configuring a tenant with a service principal mode of authorization is identical, whether that tenant is an infra tenant or a user tenant, with the exception of the point where you will set the service principal mode of authorization for the infra tenant or user tenant in the Cisco Cloud APIC GUI, where:

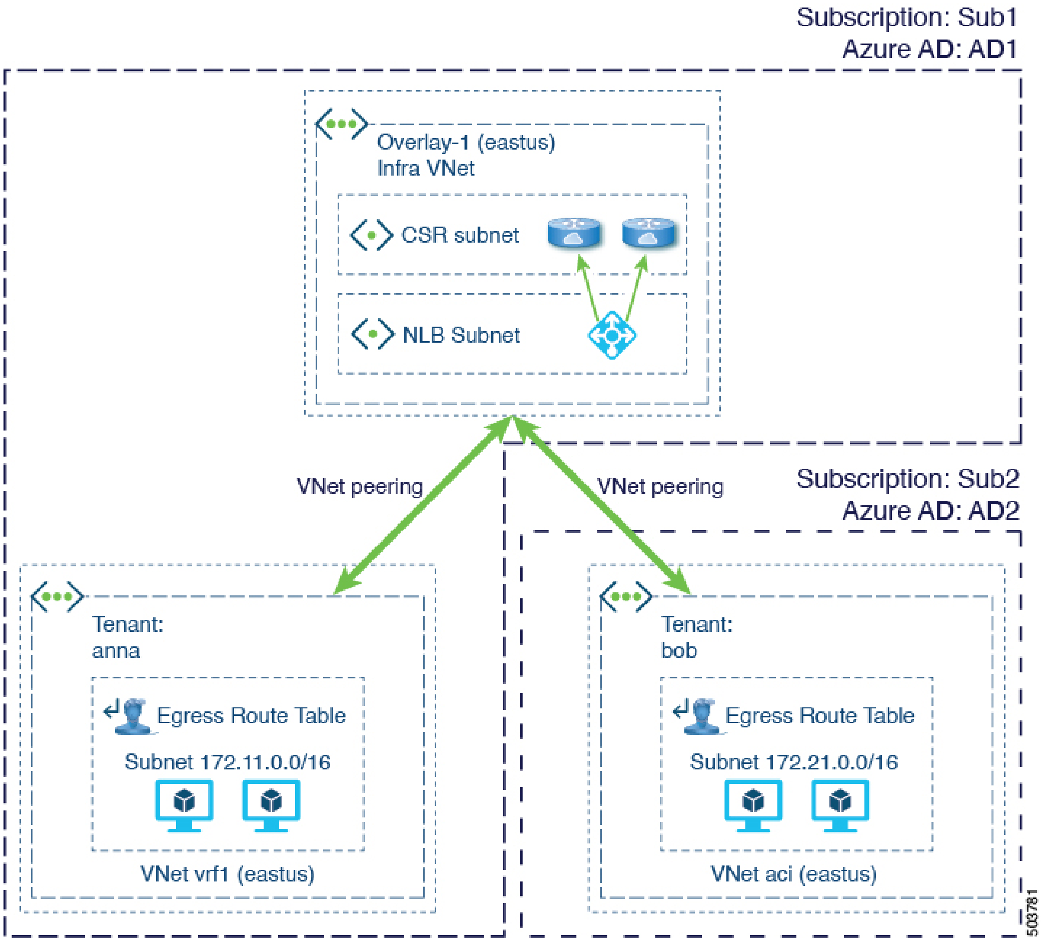
- For the infra tenant, you will be editing an existing infra tenant to set the service principal mode of authorization for that tenant
- For the user tenant, you can create a new user tenant or edit an existing user tenant to set the service principal mode of authorization for that tenant

These procedures are therefore provided in the following fashion:

1. Follow the procedures provided in this section to first configure the infra tenant a service principal mode of authorization in Azure.
2. Once you have completed these procedures to configure the infra tenant, return to the beginning and follow all of these procedures a second time, this time to configure the user tenant with a service principal mode of authorization in Azure.

   Keep in mind that you will have to make additional tenant-specific configurations to configure the Network Contributor role for both the infra and user tenant subscriptions.

These procedures will use the following topology example.



Procedure

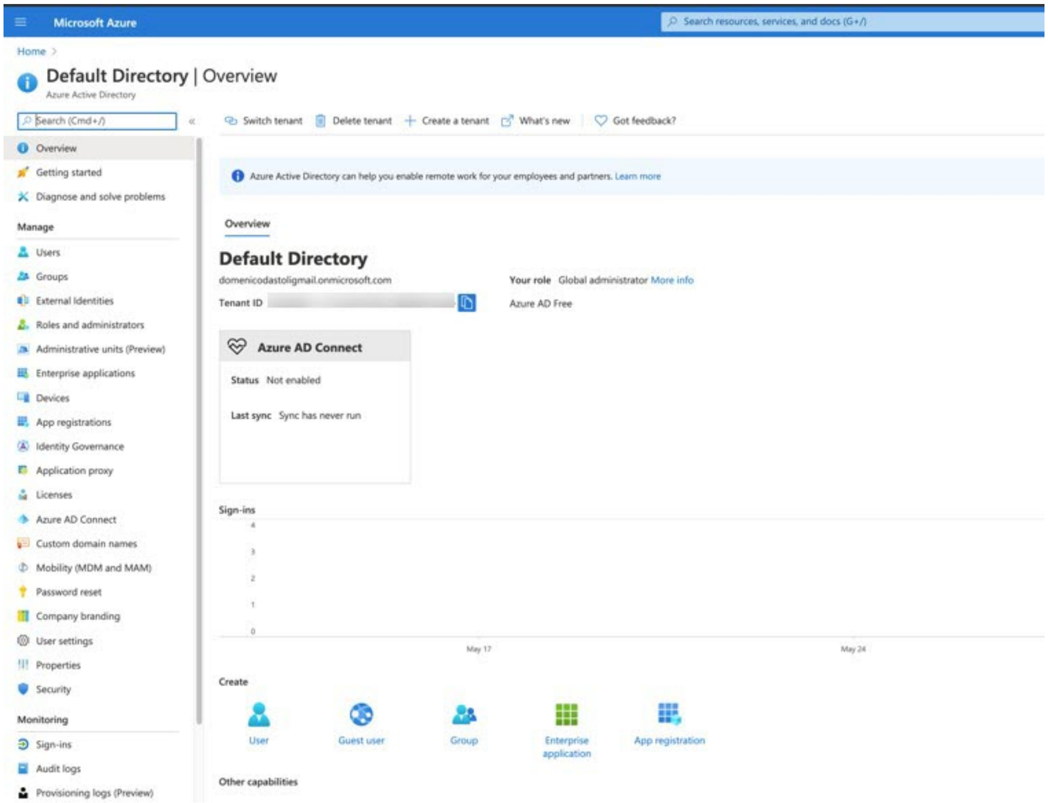
Step 1 Log into the appropriate Azure account for the Cloud APIC infra or user tenant and go to the Azure management portal, if you are not there already:

https://portal.azure.com/#home

- If you are configuring the infra tenant with a service principal mode of authorization, log into your Azure account for the Cloud APIC infra tenant.
- If you are configuring the user tenant with a service principal mode of authorization, log into your Azure account for the Cloud APIC user tenant.

Step 2 In the left navigation bar, click Azure Active Directory.

The overview page for the Azure active directory for your tenant appears.



Azure Active Directory can help you enable remote work for your employees and partners. Learn more

Default Directory

domenicodastoligmail.onmicrosoft.com

Tenant ID [redacted]

Your role Global administrator More info

Azure AD Free

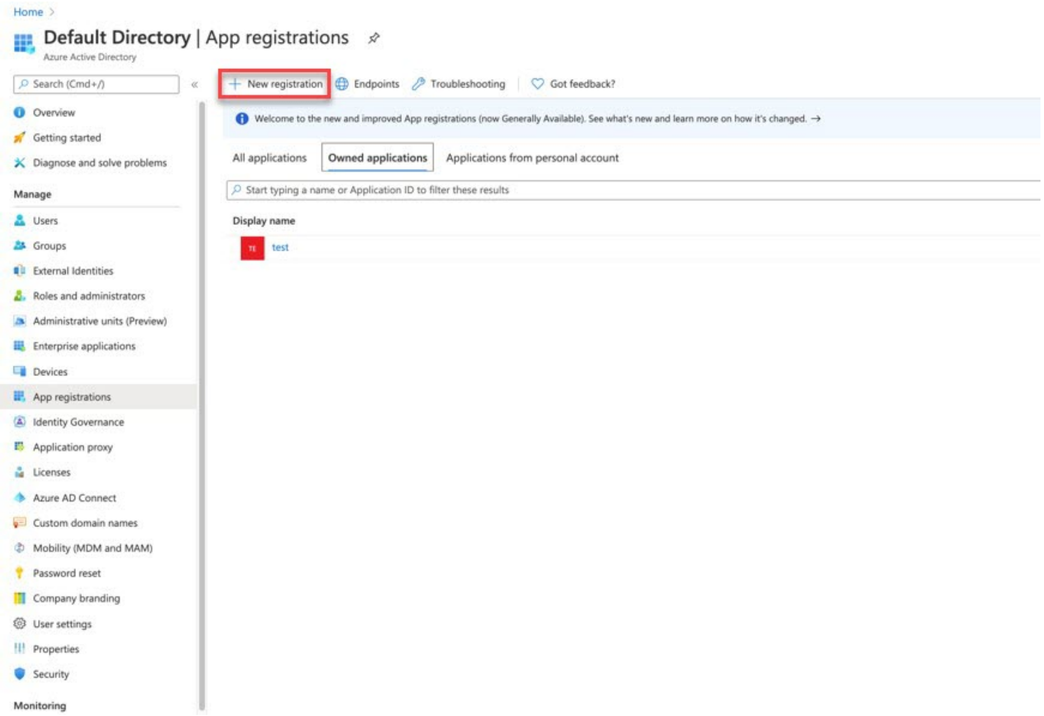
Azure AD Connect

Status Not enabled

Last sync Sync has never run

Step 3 In the left navigation bar, click App registrations.

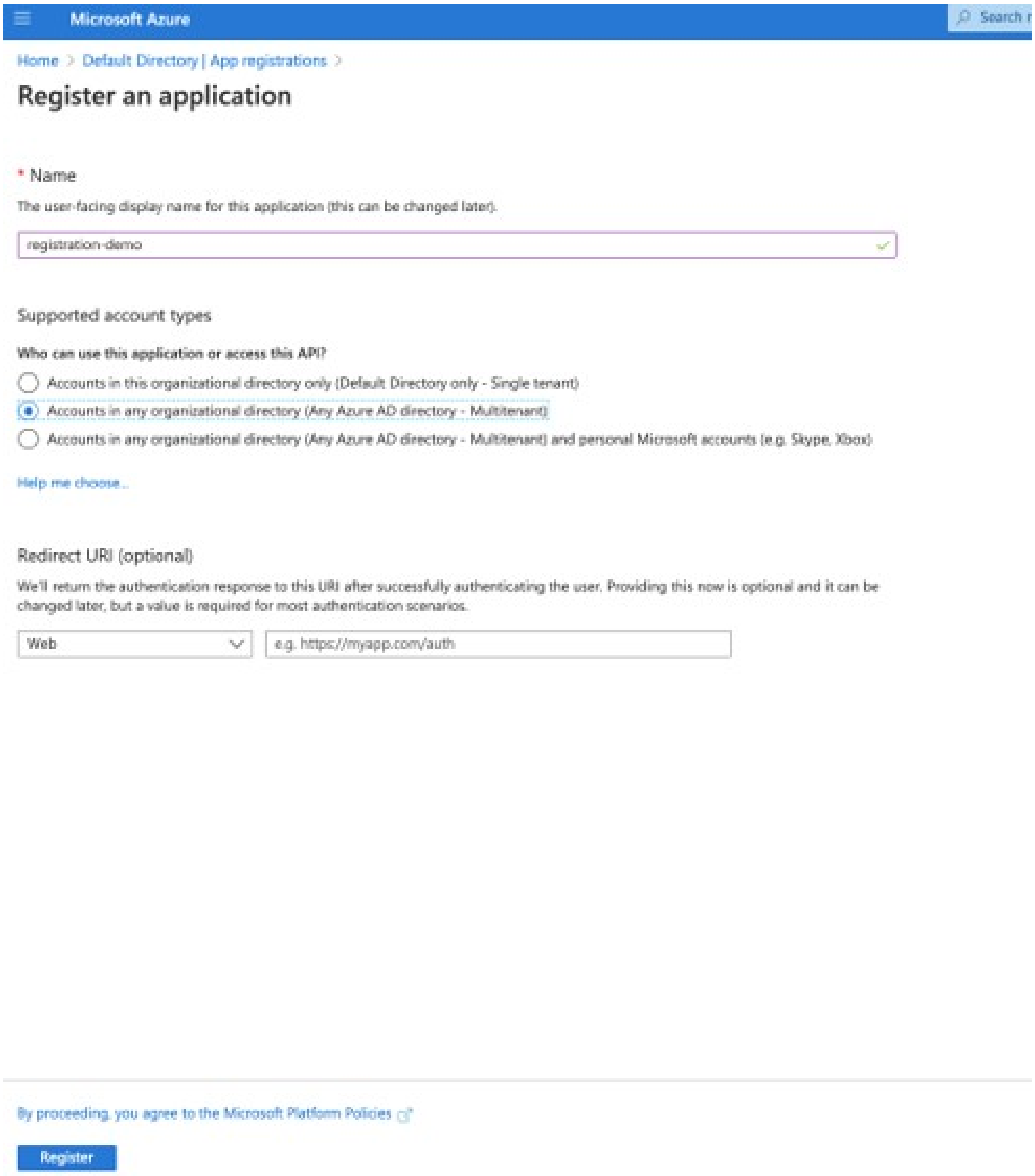
The App registrations window appears.



Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Step 4 In the App registrations window, click the New registration at the top of the window.

The Register an application window appears.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

registration-demo

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (Default Directory only - Single tenant)

● Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Step 5 In the Register an application window, enter the following information and make these selections:

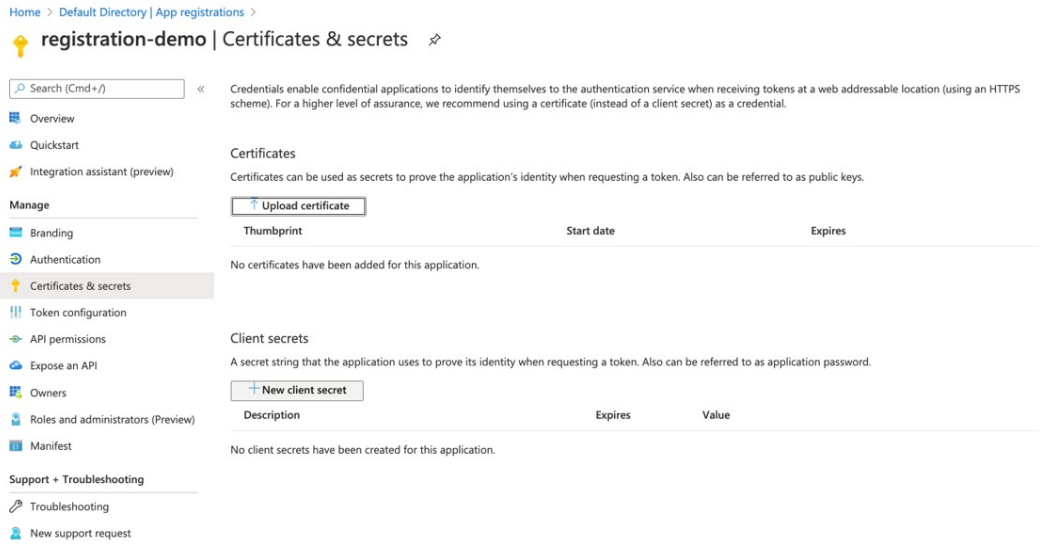
a) In the Name field, enter a name for the application.

b) In the Who can use this application or access this API field, click the button next to the middle selection, Accounts in any organizational directory (Any Azure AD directory - Multitenant).

c) Enter the necessary information in the Redirect URI field.

Step 6 Click Register.

The Certificates & secrets window appears.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

No certificates have been added for this application.

Client secrets

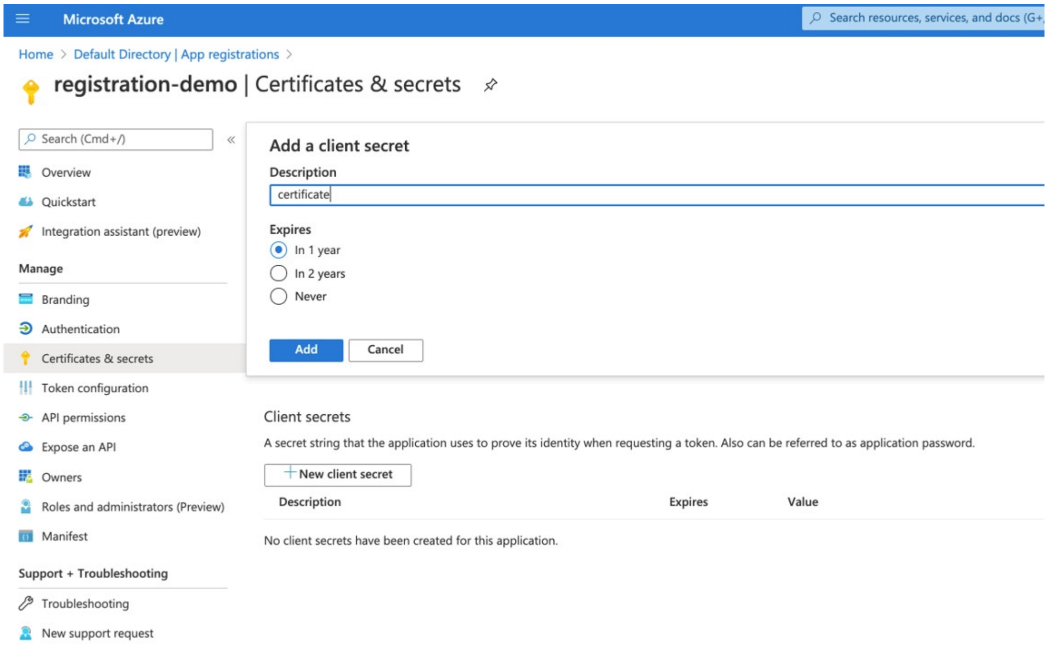
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

Step 7 In the Client secrets area, click New client secret.

Step 8 Enter a description and expiration period for this client secret, then click Add.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | App registrations >
registration-demo | Certificates & secrets
Search (Cmd+/)
Overview
Quickstart
Integration assistant (preview)
Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Preview)
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Add
Cancel
New client secret

Add a client secret

Description

certificate

Expires

● In 1 year

○ In 2 years

○ Never

Client secrets

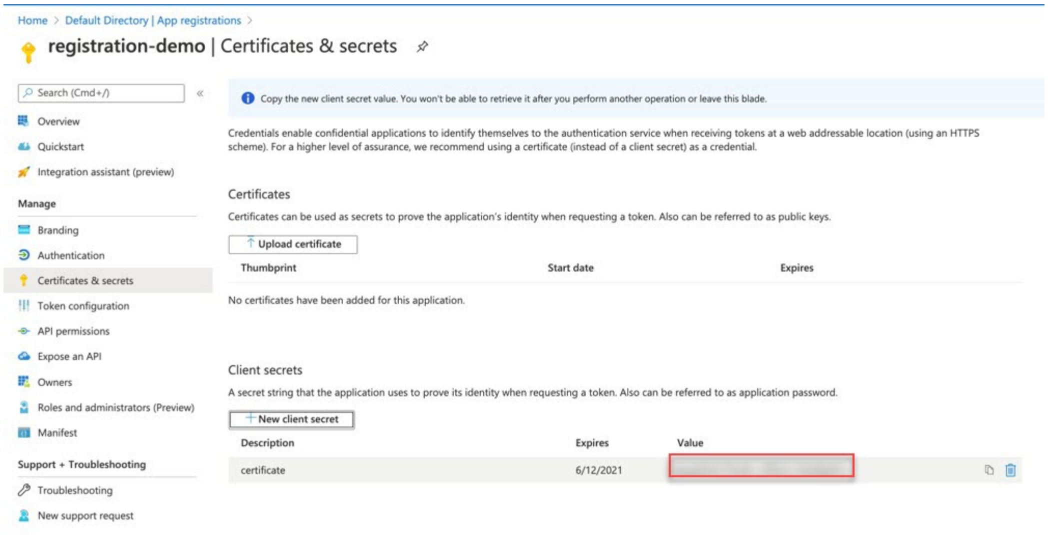
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

This generates the necessary information that you will need for the Application Secret field later on in these procedures.

Step 9 Open a text file and copy-and-paste the information in the Value column for the new client secret that you just created.



registration-demo | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

No certificates have been added for this application.

Client secrets

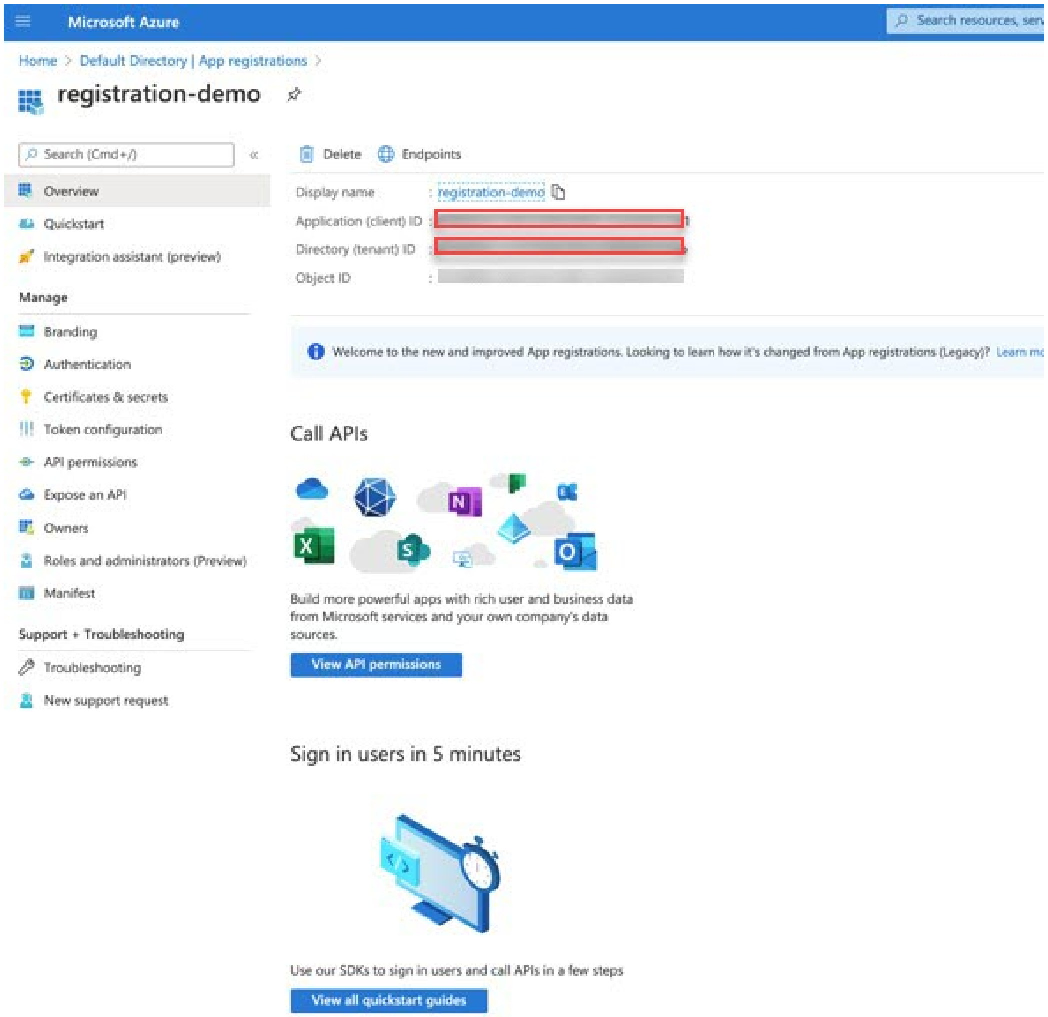
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
certificate	6/12/2021	[redacted]

Step 10 In the left navigation bar, click Overview.

Step 11 Locate the following fields, then copy-and-paste the values from those fields into the same text file:

- Application [client] ID
- Directory [tenant] ID



Display name : registration-demo

Application (client) ID : [redacted]

Directory (tenant) ID : [redacted]

Object ID : [redacted]

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn mo

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps

Step 12 Save the text file and note its location.

You will refer to this information when you configure the tenant later on in these procedures.

Step 13 Log into your Cisco Cloud APIC.

Step 14 In the left nav panel, click Application Management > Tenants.

A list of configured tenants appears.

Step 15 Determine if you are setting the service principal mode of authorization for the infra tenant or for a user tenant:

- If you are setting the service principal mode of authorization for the infra tenant, you will be editing an existing infra tenant:

  a. Click the infra link in the list of tenants.

     A panel showing details for this infra tenant slides in from the right side of the window.

  b. Click the details icon (↗).

Another window appears that provides more detailed information for the infra tenant.

c. Click Actions > Edit

d. Go to Step 16, on page 20.

- If you are setting the service principal mode of authorization for a user tenant, you can edit an existing user tenant or you can create a new user tenant.
  - To edit an existing user tenant, follow the instructions provided above for editing an infra tenant, except select the user tenant that you want to edit from the list of tenants in the first step.
  - To create a new user tenant, in the main Tenants window, click Actions > Create Tenant.

Step 16 Enter the necessary information in the Name and Security Domain fields.

Step 17 In the Azure Subscription area, make the following selections:

- Mode: Choose Create Own.
- Azure Subscription ID: Enter the subscription ID for the subscription for your Azure account.
- Access Type: Choose Service Principal.
- Application ID: Enter the application ID that you copied in Step 11, on page 18.
- Client Secret: Enter the client secret that you copied in Step 9, on page 18.
- Active Directory ID: Enter the Azure active directory ID that you copied in Step 11, on page 18.

Step 18 Click Save when finished.

Step 19 Export the application to the other subscription.

For more information, see:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/share-images-across-tenants

The service principal needs to be exported to the other subscription. For example, assume you have two tenants/apps, anna and bob. The service principal would need to be exported to the other subscription in these ways:

- First tenant/app: anna
  - Contributor role of Sub1 (AD1)
  - Network contributor role of Sub2 (AD2)
- Second tenant/app: bob
  - Contributor role of Sub2 (AD2)
  - Network contributor role of Sub1 (AD1)

a) Export the service principal app anna to Sub2 by opening a web browser and entering the necessary information for this URL, where you use the following values:

- Tenant ID for Sub2
- Application ID for the anna app

For example:

```
https://login.microsoftonline.com/<tenant_ID_for_Sub2>/oauth2/authorize?client_id=
<application_ID_for_app_anna>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```

In the Permissions requested page that comes up, click Accept.

b) Export the service principal app bob to Sub1 by opening a web browser and entering the necessary information for this URL, where you use the following values:

- Tenant ID for Sub1
- Application ID for the bob app

For example:

```
https://login.microsoftonline.com/<tenant_ID_for_Sub1>/oauth2/authorize?client_id
=<application_ID_for_app_bob>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```

In the Permissions requested page that comes up, click Accept.

Step 20 Configure the Contributor and Network Contributor roles for the tenant subscription.

As described in Support for VNet Peering Across Azure Active Directories, on page 9, you have to configure the roles for Contributor and Network Contributor roles for the infra and user tenants.

- You must make the necessary Contributor role configurations:
  - You must configure the Contributor role on the infra subscription for the service principal associated with the infra tenant.
  - You must configure the Contributor role on the tenant subscription for the service principal associated with the user tenant.
- If you want to configure VNet peering across Azure ADs, you must also make the necessary Network Contributor role configurations:
  - You must configure the Network Contributor role on the tenant subscription for the service principal associated with the infra tenant.
  - You must configure the Network Contributor role on the infra subscription for the service principal associated with the user tenant.

For example, assume the following:

- The infra tenant uses subscription Sub1 with access credentials/service principal SP-infra
- The user tenant uses subscription Sub2 with access credentials/service principal SP-user

Both of these service principals should have Contributor roles on their respective subscriptions to allow the Cisco Cloud APIC to make the calls to create the VNets and establish the VNet peering, where you would make the following configurations:

- Assign SP-infra Contributor role on Subscription Sub1.
- Assign SP-user Contributor role on Subscription Sub2.

However, in order to point the peering toward opposite VNets and make the VNet peering connection successful, you also need to make the following configurations:

- Assign SP-infra Network Contributor role on Subscription Sub2 for establishing the hub to spoke peering link.
- Assign SP-user Network Contributor role on Subscription Sub1 for establishing the spoke to hub peering link.

You can configure the Contributor and Network Contributor roles for the tenant subscription through the GUI or the CLI.

- To configure the Contributor and Network Contributor roles for the tenant subscription using the GUI, see Configuring the Contributor and Network Contributor Roles for the Tenant Subscription Using the GUI, on page 22.
- To configure the Contributor and Network Contributor roles for the tenant subscription using the CLI, see Configuring the Contributor and Network Contributor Roles Using the CLI, on page 25.

Configuring the Contributor and Network Contributor Roles for the Tenant Subscription Using the GUI

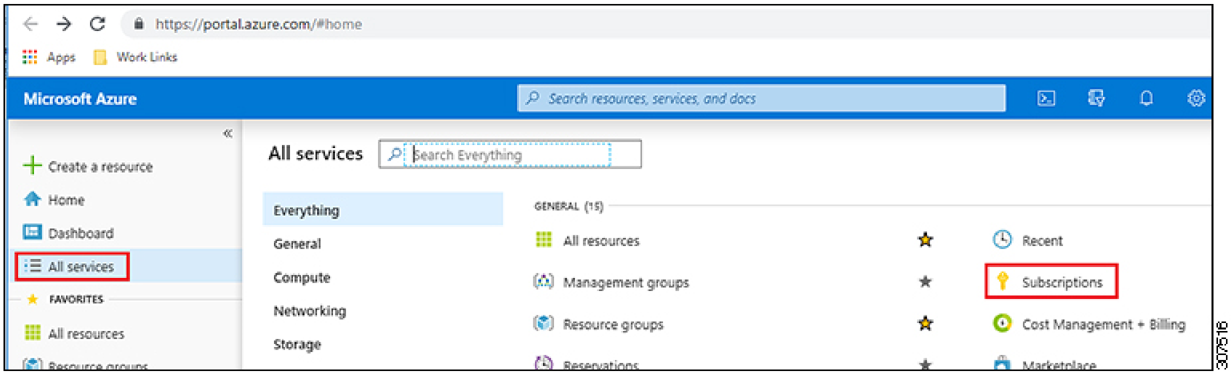
These procedures describe how to configure the Contributor and Network Contributor roles for the tenant subscription using the GUI. For instructions on how to configure the Contributor and Network Contributor roles for the tenant subscription using the CLI, see Configuring the Contributor and Network Contributor Roles Using the CLI, on page 25.

Before you begin

Complete the procedures provided in Configuring Infra and User Tenants With Service Principal Mode of Authorization, on page 12 before proceeding with the procedures in this topic.

Procedure

Step 1 From the main Azure management portal page, click the All services link in the left nav bar, then click the Subscriptions link.



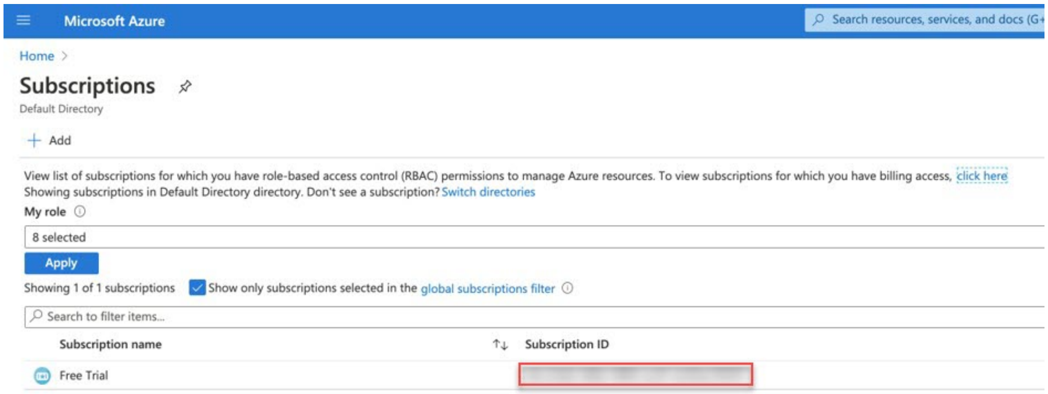
Step 2 In the Subscriptions page in the Azure management portal, click the appropriate subscription account.

- To configure the Contributor role:
  - You must configure the Contributor role on the infra subscription for the service principal associated with the infra tenant.
  - You must configure the Contributor role on the tenant subscription for the service principal associated with the user tenant.

- To configure the Network Contributor role:
  - You must configure the Network Contributor role on the tenant subscription for the service principal associated with the infra tenant.
  - You must configure the Network Contributor role on the infra subscription for the service principal associated with the user tenant.

The overview information for that subscription is displayed.

Step 3 Copy-and-paste the subscription ID for the subscription for your Azure account into the text file.



View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here

Showing subscriptions in Default Directory directory. Don't see a subscription? Switch directories

My role: 8 selected

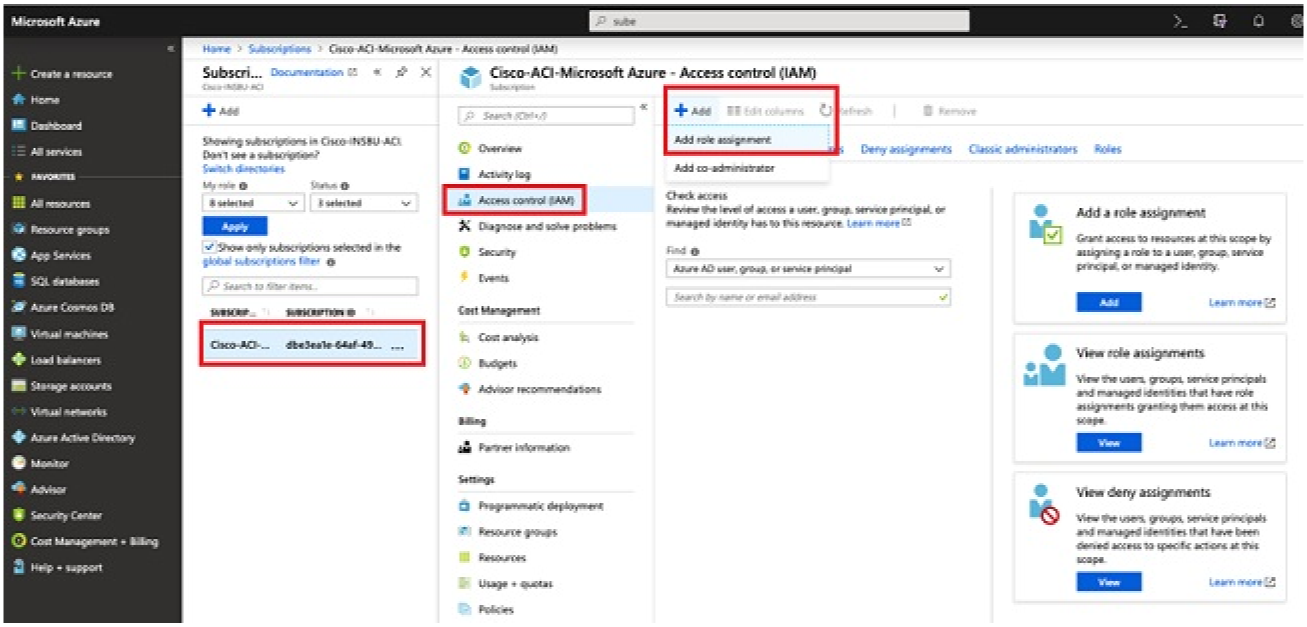
Showing 1 of 1 subscriptions ☑ Show only subscriptions selected in the global subscriptions filter

Subscription name	Subscription ID
Free Trial	[redacted]

Step 4 From the overview page for that subscription, locate the Access control (IAM) link in the left nav bar and click that link.

The Access Control page for that subscription is displayed.

Step 5 Click + Add, then select Add role assignment from the drop-down menu.



Showing subscriptions in Cisco-INSBU-ACI. Don't see a subscription?

☑ Show only subscriptions selected in the global subscriptions filter

Review the level of access a user, group, service principal, or managed identity has to this resource.

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

Step 6 Add a Contributor role assignment.

To configure the Contributor role:

- You must configure the Contributor role on the infra subscription for the service principal associated with the infra tenant.
- You must configure the Contributor role on the tenant subscription for the service principal associated with the user tenant.

a. In the Add role assignment page, make the following selections:

   - In the Role field, select Contributor from the drop-down menu.
   - In the Assign access to field, select Azure AD user, group, or service principal.
   - In the Select field, select the credentials that are associated with the Azure application.

b. Click Save at the bottom of the screen.

Step 7 Add a Network Contributor role assignment.

To configure the Network Contributor role:

- You must configure the Network Contributor role on the tenant subscription for the service principal associated with the infra tenant.
- You must configure the Network Contributor role on the infra subscription for the service principal associated with the user tenant.

a. In the Add role assignment page, make the following selections:

   - In the Role field, select Network Contributor from the drop-down menu.
   - In the Assign access to field, select Azure AD user, group, or service principal.

- In the Select field, select the credentials that are associated with the Azure application.

b. Click Save at the bottom of the screen.

What to do next

When you have configured all of the necessary infra and user tenants with a service principal mode of authorization and you have configured the Contributor and Network Contributor roles for the tenant subscription, enable VNet peering as you normally would. See Configuring Azure VNet Peering Using the GUI, on page 28 for those instructions.

Configuring the Contributor and Network Contributor Roles Using the CLI

These procedures describe how to configure the Contributor and Network Contributor roles for the tenant subscription using the CLI. For instructions on how to configure the Contributor and Network Contributor roles for the tenant subscription using the GUI, see Configuring the Contributor and Network Contributor Roles for the Tenant Subscription Using the GUI, on page 22.

Before you begin

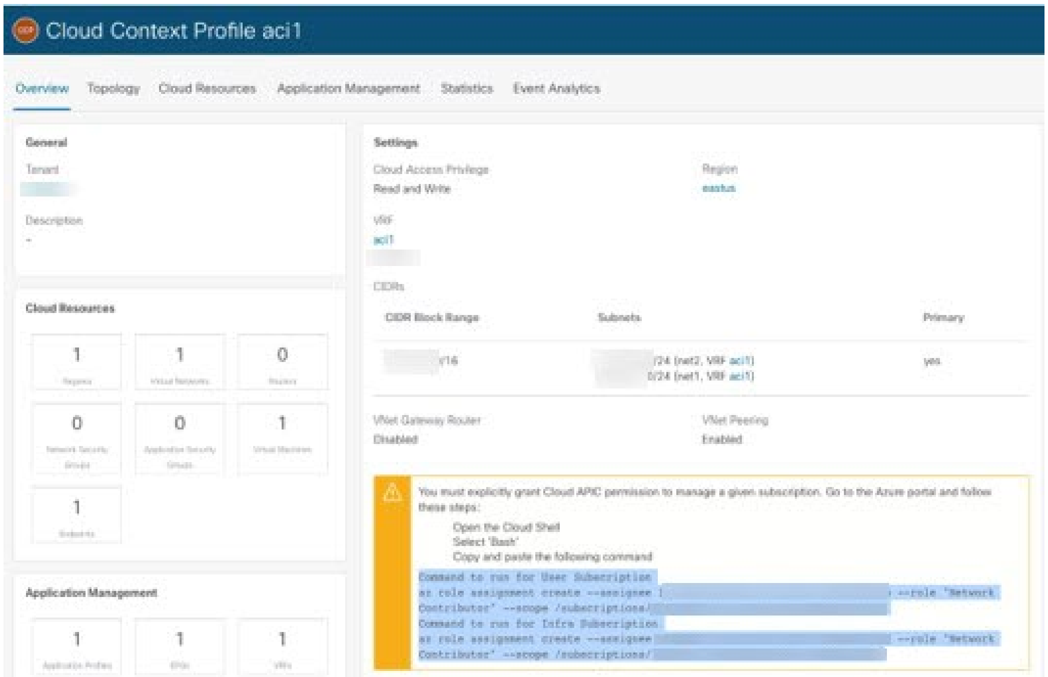
Complete the procedures provided in Configuring Infra and User Tenants With Service Principal Mode of Authorization, on page 12 before proceeding with the procedures in this topic.

Procedure

Step 1 In the Cisco Cloud APIC GUI, navigate to Application Management > Cloud Context Profile, then select the appropriate cloud context profile.

Note that you should be in the user tenant, not the infra tenant, for these steps.

Step 2 Copy the az command provided in this window.



Cloud Context Profile aci1

General

Tenant

[redacted]

Description

-

Cloud Resources

1 Regions	1 Virtual Networks	0 Routers
0 Network Security Groups	0 Application Security Groups	1 Virtual Machines
1 Endpoints		

Application Management

1 Application Profiles	1 EPGs	1 VRFs

Settings

Cloud Access Privilege

Read and Write

Region

eastus

VRF

aci1

[redacted]

CIDRs

CIDR Block Range	Subnets	Primary
[redacted]/16	[redacted]/24 (net2, VRF aci1) [redacted]0/24 (net1, VRF aci1)	yes

VNet Gateway Router

Disabled

VNet Peering

Enabled

You must explicitly grant Cloud APIC permission to manage a given subscription. Go to the Azure portal and follow these steps:

Open the Cloud Shell
Select 'Bash'
Copy and paste the following command

```
Command to run for User Subscription
az role assignment create --assignee [redacted] --role 'Network
Contributor' --scope /subscriptions/[redacted]
Command to run for Infra Subscription
az role assignment create --assignee [redacted] --role 'Network
Contributor' --scope /subscriptions/[redacted]
```

Step 3 Return to the Azure management portal and click Registrations in the left navigation bar.

Step 4 Open the Cloud Shell.

Step 5 Select Bash.

Step 6 Assign the Network Contributor roles.

a) Assign the Network Contributor role of Sub2 to the anna app.

Paste the az command that you copied in Step 2, on page 25 in the following manner:

```
az role assignment create --assignee <application_ID_for_app_anna> --role "Network Contributor"
--scope /subscriptions/<subscription_ID_of_Sub2>
```

b) Assign the Network Contributor role of Sub1 to the bob app.

Paste the az command that you copied in Step 2, on page 25 in the following manner:

```
az role assignment create --assignee <application_ID_for_app_bob> --role "Network Contributor"
--scope /subscriptions/<subscription_ID_of_Sub1>
```

Step 7 Assign the Contributor roles.

a) Assign the Contributor role of Sub1 to the anna app:

```
az role assignment create --assignee <application_ID_for_app_anna> --role "Contributor" --scope
/subscriptions/<subscription_ID_of_Sub1>
```

b) Assign the Contributor role of Sub2 to the bob app.

```
az role assignment create --assignee <application_ID_for_app_bob> --role "Contributor" --scope
/subscriptions/<subscription_ID_of_Sub2>
```

What to do next

When you have configured all of the necessary infra and user tenants with a service principal mode of authorization and you have configured the Contributor and Network Contributor roles for the tenant subscription, enable VNet peering as you normally would. See Configuring Azure VNet Peering Using the GUI, on page 28 for those instructions.

Guidelines and Limitations for Azure VNet Peering

Note Following are general guidelines and limitations for Azure VNet peering with Cisco Cloud APIC. For guidelines and limitations specifically for the VNet peering across Azure ADs enhancement available in release 5.2(1), see Guidelines and Limitations for Azure VNet Peering Across Azure Active Directories, on page 12.

Following are the guidelines and limitations for Azure VNet peering.

- You can't add, remove, or update a CIDR on the VNet if it has peering connections with other VNets. In this situation, you must remove the VNet peerings, then make the necessary change to the CIDR (add, remove, or update the CIDR), then reestablish the VNet peerings again.
- Resources in one virtual network can't communicate with the front-end IP address of a Basic Internal Load Balancer (ILB) in a globally-peered virtual network.
- Some services that use a Basic load balancer don't work over global virtual network peering. For more information, see

  Constraints for peered virtual networks.
- There is no support for traffic between two user VNets where one of the VNets has only VNet peering configured and the other VNet has only VPN gateway configured.
- If you are running on release 5.1(1) or earlier and you have the following configuration for your system:
  - VNet peering enabled
  - Multiple cloud sites, each managing multiple regions
  - Two CSRs deployed in each region

  And you reboot both CSRs, you might experience a 3-minute traffic loss between the VMs across those cloud sites. Traffic should begin to flow again between the VMs across the cloud sites after several minutes.

Prerequisites for Configuring Azure VNet Peering

Complete the following tasks before configuring Azure VNet peering:

- Install Cisco Cloud APIC.

  Follow the instructions in the Cisco Cloud APIC for Azure Installation Guide, Release 5.0(x).
- Verify that you have set up your sites correctly (on-premises or in the cloud).

  Follow instructions in the appropriate Cisco Application Policy Infrastructure Controller (APIC) or Cisco Cloud APIC documentation.

- If you’re connecting an on-premises site to a cloud site, configure and deploy your on-premises Cisco Application Centric Infrastructure (ACI) fabric and Cisco ACI Multi-Site. Also ensure that you have a MultiSite license.

Configuring Azure VNet Peering Using the GUI

To configure Azure VNet peering, you set up the cloud site and then configure the necessary information in the cloud context profile.

You use Cisco Cloud APIC to set up the cloud site. You can use Cisco Cloud APIC to configure the cloud context profile; however, if you are using Azure VNet peering in a multisite environment, we recommend that you do so in Cisco Application Centric Infrastructure (ACI) Multi-Site Orchestrator.

Set Up the Cloud Site to Use Azure VNet Peering

Complete this task to set up the Azure cloud site to support VNet peering. This procedure assumes that you have not yet set up the cloud site.

The procedure for setting up the cloud site to use Azure VNet peering is very similar to a typical Cloud APIC first-time setup procedure, with the exception of enabling the Azure VNet peering feature using the VNet Peering option, as described in Step 4, on page 28.

Before you begin

- Understand the guidelines and limitations provided in Guidelines and Limitations for Azure VNet Peering, on page 27.
- Complete the tasks in the section Prerequisites for Configuring Azure VNet Peering, on page 27.

Procedure

Step 1 Log in to Cisco Cloud APIC.

Step 2 In the Welcome to Cloud APIC dialog box, click Review First Time Setup.

Step 3 In the Let's Configure the Basics dialog box, in the Region Management area, click Begin.

The Setup—Region Management window appears.

Step 4 Enable Virtual Network Peering at the global level in the Connectivity for Internal Network area, if necessary.

Enabling VNet peering in the Connectivity for Internal Network area enables VNet peering at the global level, which deploys NLBs in all the regions with a CSR.

- For release 5.1(2) and later, VNet peering at the global level is enabled by default and cannot be disabled.
- For releases prior to release 5.1(2), choose Virtual Network Peering to enable the Azure VNet peering feature at the global level.

  Note that the VPN Connectivity via CSR option is used to enable the traditional VPN connectivity through the overlay IPsec tunnels between CSRs and Azure VPN Gateway routers, instead of using VNet peering.

Step 5 If you want connectivity to the on-premises site or another cloud site—in addition to connectivity within this cloud site—check the Inter-Site Connectivity check box.

Step 6 Locate the Cloud APIC home region and check the box in the Cloud Routers column for the Cloud APIC home region, if it is not checked already.

The region that you selected when you were configuring your cloud site is the home region and should be selected already in this page. This is the region where the Cloud APIC is deployed (the region that will be managed by Cloud APIC), and will be indicated with the text `Cloud APIC Deployed` in the Region column.

Step 7 In the Regions to Manage area, choose one or more regions that you want to manage.

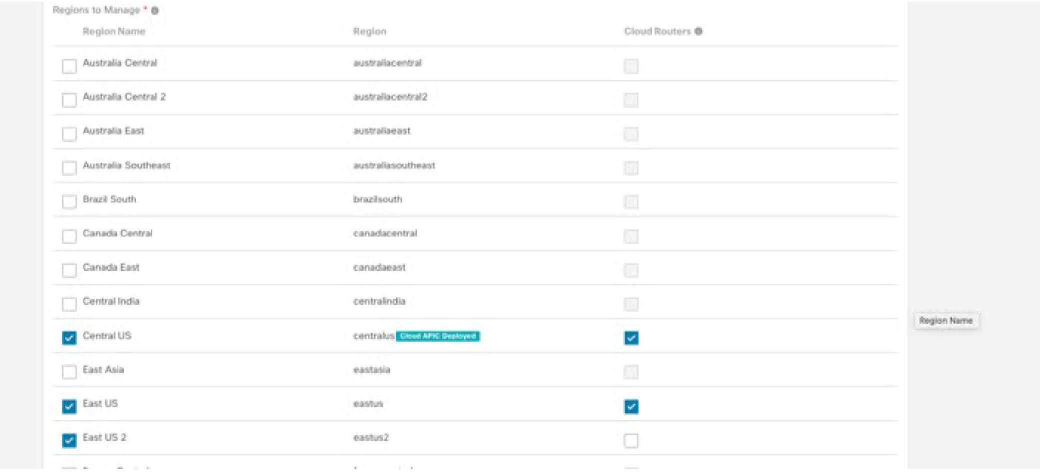
In the current release, a cloud site can consist up to 4 regions, including the home region where the Cloud APIC is deployed.

A Cloud APIC can manage multiple cloud regions as a single cloud site. In the current release, a cloud site can consist up to 4 regions, including the home region where the Cloud APIC is deployed. If a Cloud APIC manages two regions, those two regions are considered a single site.

The following options are available on the row for any region that you select:

- Cloud Routers: Select this option if you want to deploy CSRs in this region. You must have at least one region with CSRs deployed to have inter-VNET or inter-site communications. However, if you choose multiple regions in this page, you do not have to have CSRs in every region that you choose.
- Inter-Site Connectivity: Select this option if you want this region to connect to other sites (for example, if you want this region to connect to an on-premises site, or to connect cloud site-to-cloud site, through Cisco ACI Multi-Site). Infra VNETs or VPCs are deployed on all regions selected for inter-site connectivity. Note that when you select inter-site connectivity for a region, the cloud routers option is also selected automatically for this region because you must have two cloud routers deployed for inter-site connectivity hubs.

For example, consider the following configuration:



Regions to Manage *

Region Name	Region	Cloud Routers
□ Australia Central	australiacentral	□
□ Australia Central 2	australiacentral2	□
□ Australia East	australiaeast	□
□ Australia Southeast	australiasoutheast	□
□ Brazil South	brazilsouth	□
□ Canada Central	canadacentral	□
□ Canada East	canadaeast	□
□ Central India	centralindia	□
☑ Central US	centralus Cloud APIC Deployed	☑
□ East Asia	eastasia	□
☑ East US	eastus	☑
☑ East US 2	eastus2	□

In this example configuration:

- The regions Central US and East US have checkmarks in the Cloud Routers column. They will have CSRs and an Azure NLB deployed in their infra VNets that will serve as the hub VNets for VNet peering.
- The region East US2 will not have a CSR deployed (does not have a checkmark in the Cloud Routers column). This managed region with no CSR will be able to have spoke VNets, but will use the hub VNets in the other regions.

Step 8 Click Next.

Another panel of the Setup—Region Management dialog box appears.

The General area shows the subnets for the cloud routers, which you provided when you installed Cisco Cloud APIC.

Step 9 In the Fabric Autonomous System Number field, enter the BGP autonomous system number (ASN) that is unique to this site.

Note the following Microsoft Azure ASN restrictions:

- Do not use 64518 as the autonomous system number in this field.
- Do not use 32-bit ASNs. Azure VPN Gateways support 16-Bit ASNs at this time.
- The following ASNs are reserved by Azure for both internal and external peerings:
  - Public ASNs: 8074, 8075, 12076
  - Private ASNs: 65515, 65517, 65518, 65519, 65520

  You cannot specify these ASNs for your on-premises VPN devices when connecting to Azure VPN gateways.
- The following ASNs are reserved by IANA and cannot be configured on your Azure VPN Gateway: 23456, 64496-64511, 65535-65551 and 429496729

Step 10 In the Subnet for Cloud Router field, enter the subnet for the cloud router.

The first subnet pool for the first two regions is automatically populated. If you selected more than two regions, you will need to add another subnet for the cloud routers for the additional regions. Addresses from this subnet pool will be used for inter-region connectivity for any additional regions that are added that need to be managed by the Cloud APIC after the first two regions. This must be a valid IPv4 subnet with mask /24.

Step 11 Click Add Subnet for Cloud Router and enter information for additional subnets, if necessary.

- For releases prior to Release 5.0(2), enter information on additional subnets based on the number of CSRs that are being deployed.
- For Release 5.0(2) and later, enter information on additional subnets based on the number of regions that your Cloud APIC is managing.

All CIDRs for the infra tenant will be pre-allocated in peering mode. The system needs three /25 subnets for each managed region with CSRs.

Click the checkbox to accept the values for every subnet that you add.

Step 12 Configure the remaining fields as you normally would.

a) Under the Cloud Router Template area, in the Number of Routers Per Region field, choose the number of Cisco Cloud Services Routers (CSRs) that will be used in each region.

   The default is two. The current release supports up to four CSRs per region.

b) In the Username, enter the username for the Cisco Cloud Services Router.

   Note Do not use `admin` as a username for the Cisco Cloud Services Router when deploying it to an Azure cloud site.

c) In the Password field, enter the password for the Cisco Cloud Services Router.

d) In the Throughput of the routers field, choose the throughput of the Cisco Cloud Services Router.

   In some cases, changing the value in this field changes the size of the CSR instance that is deployed. Choosing a higher value for the throughput could result in a larger VM being deployed.

Note If you wish to change this value at some point in the future, you must delete the CSR, then repeat the processes in this chapter again and select the new value that you would like in the same Throughput of the routers field.

In addition, the licensing of the CSR is based on this setting. You will need the equivalent or higher license in your Smart account for it to be compliant.

Note Cloud routers should be undeployed from all regions before changing the router throughput or login credentials.

e) In the License Token field, enter the license token for the Cisco Cloud Services Router.

This is the Product Instance Registration token from your Cisco Smart Software Licensing account. To get this license token, go to http://software.cisco.com, then navigate to Smart Software Licensing > Inventory > Virtual Account to find the Product Instance Registration token.

f) Click the appropriate button, depending on whether you are configuring inter-site connectivity or not.

- If you are not configuring inter-site connectivity (if you did not select Inter-Site Connectivity when you were selecting regions to manage in the Region Management page), click Save and Continue. You have completed setting up the cloud site in this case.

- If you are configuring inter-site connectivity (if you selected Inter-Site Connectivity when you were selecting regions to manage in the Region Management page), click Next at the bottom of the page. The Inter-Site Connectivity page appears.

g) Enter the following information in the Inter-Site Connectivity page:

- IPSec Tunnels to Inter-Site Routers: This field is necessary only for on-premises connectivity to cloud sites. There is no need to enter information in this field if you don't have an on-premises site.

  In this area, click the + button next to the Add Public IP of IPsec Tunnel Peer field.

  - Enter the peer IP address for the IPsec tunnel termination to the on-premises device.

  - Click the check mark to add this peer IP address.

- OSPF Area for Inter-Site Connectivity: Enter the underlay OSPF area ID that will be used with on-premises ISN peering (for example, `0.0.0.1`)

- Under the External Subnets for Inter-Site Connectivity heading, click the + button next to the +Add External Subnet field.

  - Enter the subnet tunnel endpoint pool (the cloud TEP) that will be used in Azure. It must be a valid IPv4 subnet with a mask between /16 and /22 (for example, `30.29.0.0/16`). This subnet will be used to address the IPsec tunnel interfaces and loopbacks of the Cloud Routers used for on-premises connectivity, and cannot overlap with other on-premises TEP pools.

  - Click the check mark after you have entered in the appropriate subnet pools.

h) When you have entered all the necessary information on this page, click Save and Continue at the bottom of the page.

You have completed setting up the cloud site in this case.

What to do next

1. Perform the tasks in the chapter "Configuring the Cisco Cloud APIC Using the GUI," in the Cisco Cloud APIC for Azure User Guide 5.0(x).

   The tasks include configuring a tenant, an application profile, a VRF, one or more endpoint groups (EPGs), and one or more contracts and filters.

2. Create a cloud context profile for Azure VNET peering.

   See Create a Cloud Context Profile, on page 32 for those procedures.

Create a Cloud Context Profile

This section explains how to create a cloud context profile using the Cisco Cloud APIC GUI for Azure VNET peering.

The procedure for creating a cloud context profile for Azure VNet peering is very similar to a typical cloud context profile configuration procedure, with the additional VNet peering-specific step of enabling the Azure VNet peering feature in the VNet Peering field.

Before you begin

Set up the cloud site to use Azure VNET peering.

Procedure

Step 1 Log in to the Cloud APIC, if you are not logged in already.

Step 2 In the left navigation bar, navigate to Application Management > Cloud Context Profiles.

The existing cloud context profiles are displayed.

Step 3 Click Actions and choose Create Cloud Context Profile.

The Create Cloud Context Profile dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following Cloud Context Profile Dialog Box Fields table then continue.

Table 1: Create Cloud Context Profile Dialog Box Fields

Properties	Description
Name	Enter the name of the cloud context profile.
Tenant	To choose a tenant: a. Click Select Tenant. The Select Tenant dialog box appears. b. From the Select Tenant dialog, click to choose a tenant in the left column then click Select. You return to the Create Cloud Context Profile dialog box.
Description	Enter a description of the cloud context profile.
Settings	

Properties	Description
Region	To choose a region: a. Click Select Region. The Select Region dialog box appears. b. From the Select Region dialog, click to choose a region in the left column then click Select. You return to the Create Cloud Context Profile dialog box.
VRF	To choose a VRF: a. Click Select VRF. The Select VRF dialog box appears. b. From the Select VRF dialog box, click to choose a VRF in the left column then click Select. You return to the Create Cloud Context Profile dialog box.
CIDRs	Add additional CIDRs, if necessary. To add a CIDR: a. Click Add CIDR. The Add CIDR dialog box appears. b. Enter the address in the Address field. c. Click Add Subnet and enter the subnet address in the Address field. d. Click to check (enabled) or uncheck (disabled) the Primary check box. e. When finished, click Add.
VNet Gateway Router	Click to check (enable) or uncheck (disable) in the VNet Gateway Router check box.
VNet Peering	Click to check (enable) or uncheck (disable) the Azure VNet peering feature.

Step 5 Click Save when finished.

Step 6 Configure the Network Contributor role for both the infra and user tenant subscriptions.

For example, assume the following:

- The infra tenant is using subscription S1 with access credentials/service principal C1
- The user tenant is using subscription S2 with access credentials/service principal C2

In this situation, you will have to configure the following for peering to work between the user tenant and the infra VNets:

- You will have to give C1 Network Contributor role permissions to S2 for the hub to spoke peering link
- You will have to give C2 Network Contributor role permissions to S1 for the spoke to hub peering link

a) In the yellow window that appears, copy the az command provided.

    - If you have to configure the Network Contributor role for the user tenant, copy the text in the area Command to run for User Subscription.

    - If you have to configure the Network Contributor role for the infra tenant, copy the text in the area Command to run for Infra Subscription.

b) Return to the Azure management portal and click Registrations in the left navigation bar.
c) Open the Cloud Shell.
d) Select Bash.
e) Paste the az command that you copied in 6.a, on page 33.

Step 7 Follow these steps to disable Azure VNet peering, if necessary.

If you decide that you would like to disable Azure VNet peering after you have configured it, follow these steps to disable the VNet peering feature:

- To disable Azure VNet peering at a global level:

  a. First disable Azure VNet peering at the local level, through the cloud context profile:

     1. Navigate to the Create Cloud Context Profile page:

        Application Management > Cloud Context Profiles

     2. Click the link under the Name column for the cloud context profile where you want to disable VNet peeriing.

        A panel showing details for this cloud context profile slides in from the right side of the window.

     3. Click the Details icon ( ).

        Another window appears that provides more detailed information for this cloud context profile.

     4. Click the pencil icon in the upper right corner of the window.

        The Edit Cloud Context Profile window appears.

     5. Uncheck (disable) the Hub Network Peering field.

     6. Click Save.

  b. Then disable Azure VNet peering at the global level:

     1. In the Cloud APIC GUI, click the Intent icon ( ) and select cAPIC Setup. In the Region Management area, click Edit Configuration.

     2. In the Regions to Manage screen, change the Connectivity for Internal Network setting from Virtual Network Peering to VPN Connectivity via CSR.

- To disable Azure VNet peering at a local level, for a particular Cloud Context Profile:

  a. Navigate to the Create Cloud Context Profile page:

     Application Management > Cloud Context Profiles

  b. Click the link under the Name column for the cloud context profile where you want to disable VNet peeriing.

     A panel showing details for this cloud context profile slides in from the right side of the window.

  c. Click the Details icon ( ).

Another window appears that provides more detailed information for this cloud context profile.

d. Click the pencil icon in the upper right corner of the window.

The Edit Cloud Context Profile window appears.

e. Uncheck (disable) the Hub Network Peering field.

f. Click Save.

Configuring Azure VNet Peering Using the REST API

Complete this task to set up the Azure cloud site to support VNet peering. This procedure assumes that you have not yet set up the cloud site.

Before you begin

- Understand the guidelines and limitations provided in Guidelines and Limitations for Azure VNet Peering, on page 27.
- Complete the tasks in the section Prerequisites for Configuring Azure VNet Peering, on page 27.

Procedure

Step 1 Configure the cloud template for the infra tenant using a post such as the following, where the information used to configure Azure VNet peering is highlighted in bold.

```
<polUni>
    <fvTenant name="infra">
        <cloudApicSubnetPool subnet="10.10.1.0/24" />
        <cloudApicSubnetPool subnet="10.10.2.0/24" />
            <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2"
numRoutersPerRegion="2" status="" vrfName="overlay-1" status="">
               <cloudtemplateProfile name="default" routerPassword="Ins3965!" routerUsername="cisco"
 routerThroughput="1G"/>
                <cloudtemplateExtSubnetPool status="" subnetpool="11.11.0.0/16"/>
                <cloudtemplateExtNetwork name="default" status="">
                    <cloudRegionName provider="azure" region="eastus" status=""/>
                    <cloudRegionName provider="azure" region="westus" status=""/>
                    <cloudtemplateVpnNetwork name="default">
                        <cloudtemplateIpSecTunnel peeraddr="22.22.219.104"/>
                        <cloudtemplateOspf area="0.0.0.1"/>
                    </cloudtemplateVpnNetwork>
                </cloudtemplateExtNetwork>
                <cloudtemplateIntNetwork name="default">
                    <cloudRegionName provider="azure" region="eastus" status=""/>
                    <cloudRegionName provider="azure" region="westus" status=""/>
                </cloudtemplateIntNetwork>
                <cloudtemplateHubNetwork name="default" status="">
                    <cloudtemplateHubNetworkName name="default" asn="64514"/>
                </cloudtemplateHubNetwork>
            </cloudtemplateInfraNetwork>
    </fvTenant>
</polUni>
```

Step 2 Configure the cloud context profile for the user tenant using a post such as the following, where the information used to configure Azure VNet peering is highlighted in bold.

Note The default value of "type" for `cloudRsCtxProfileToGatewayRouterP` is "spoke", so it does not have to be specified when posting a user tenant.

```
<cloudCtxProfile name="c1" status="">
    <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
    <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-westus"/>
    <cloudRsToCtx tnFvCtxName="VRF1"/>
    <cloudCidr name="cidr1" addr="11.0.0.0/16" primary="yes" status="">
        <cloudSubnet ip="11.0.0.0/24" status="">
           <cloudRsZoneAttach status="" tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>

        </cloudSubnet>
    </cloudCidr>
</cloudCtxProfile>
```

Verifying the Azure VNet Peering Deployment

After you configure Azure VNet peering, you should verify that it is deployed correctly.

Before you begin

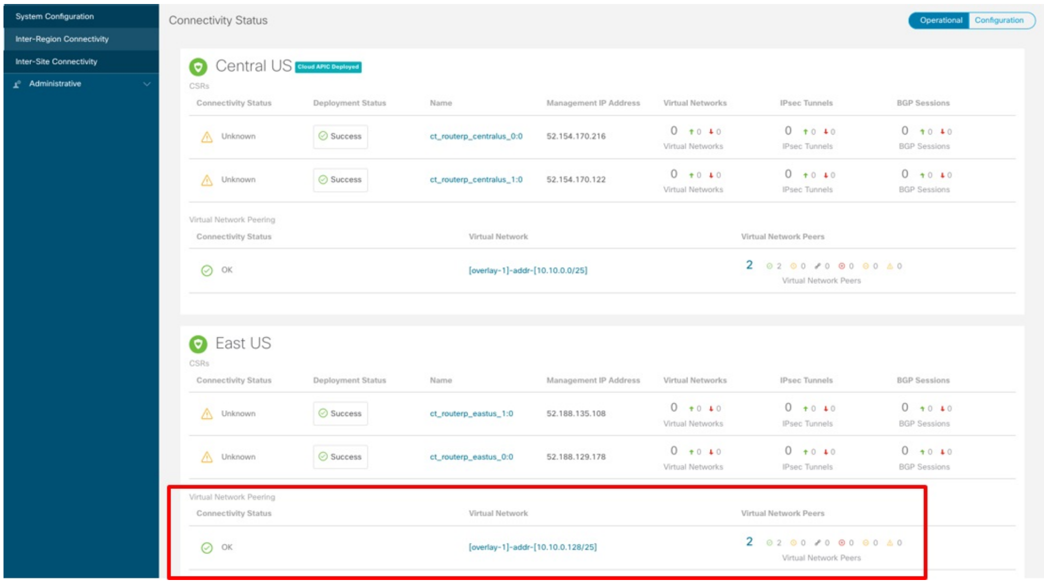
You must have set up the cloud site and configured the cloud context profile.

Procedure

Step 1 Log into Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC).

Step 2 In the left navigation pane, choose Infrastructure > Inter-Region Connectivity.

Step 3 Verify that the information shown in the Virtual Network Peering area is correct.



Connectivity Status

Central US Cloud APIC Deployed

CSRs

Connectivity Status	Deployment Status	Name	Management IP Address	Virtual Networks	IPsec Tunnels	BGP Sessions
⚠ Unknown	✓ Success	ct_routerp_centralus_0:0	52.154.170.216	0 ↑0 ↓0 Virtual Networks	0 ↑0 ↓0 IPsec Tunnels	0 ↑0 ↓0 BGP Sessions
⚠ Unknown	✓ Success	ct_routerp_centralus_1:0	52.154.170.122	0 ↑0 ↓0 Virtual Networks	0 ↑0 ↓0 IPsec Tunnels	0 ↑0 ↓0 BGP Sessions

Virtual Network Peering

Connectivity Status	Virtual Network	Virtual Network Peers
✓ OK	[overlay-1]-addr-[10.10.0.0/25]	2 ✓ 2 ○ 0 ✎ 0 ⊗ 0 ○ 0 ⚠ 0 Virtual Network Peers

East US

CSRs

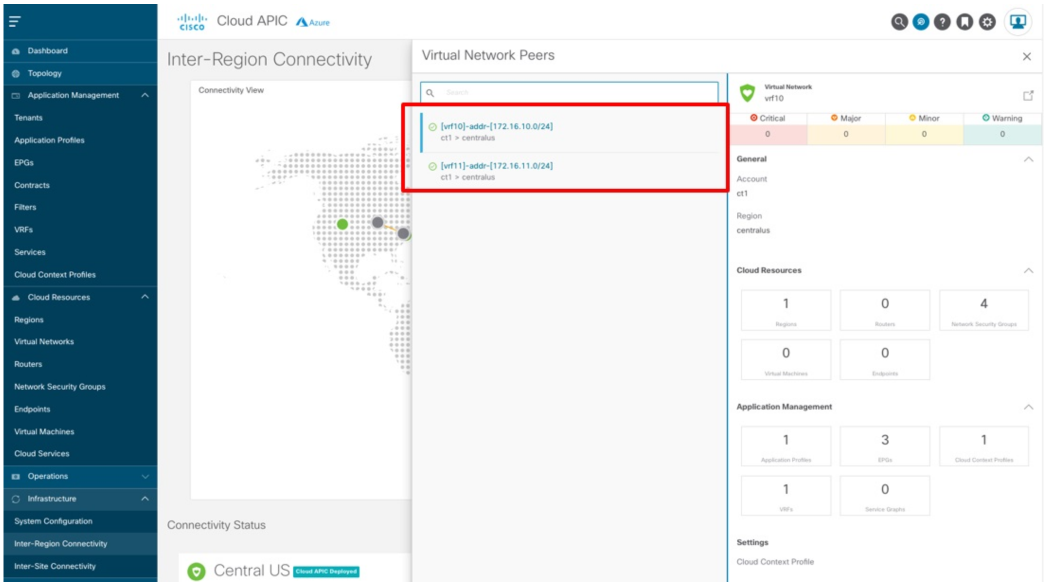
Connectivity Status	Deployment Status	Name	Management IP Address	Virtual Networks	IPsec Tunnels	BGP Sessions
⚠ Unknown	✓ Success	ct_routerp_eastus_1:0	52.188.135.108	0 ↑0 ↓0 Virtual Networks	0 ↑0 ↓0 IPsec Tunnels	0 ↑0 ↓0 BGP Sessions
⚠ Unknown	✓ Success	ct_routerp_eastus_0:0	52.188.129.178	0 ↑0 ↓0 Virtual Networks	0 ↑0 ↓0 IPsec Tunnels	0 ↑0 ↓0 BGP Sessions

Virtual Network Peering

Connectivity Status	Virtual Network	Virtual Network Peers
✓ OK	[overlay-1]-addr-[10.10.0.128/25]	2 ✓ 2 ○ 0 ✎ 0 ⊗ 0 ○ 0 ⚠ 0 Virtual Network Peers

Step 4 Click on the count (the blue number 2 in the example above) to display more detailed information.

This will display peerings from the hub VNet to the tenant VNets.



Inter-Region Connectivity

Virtual Network Peers

[vrf10]-addr-[172.16.10.0/24]
ct1 > centralus

[vrf11]-addr-[172.16.11.0/24]
ct1 > centralus

Virtual Network
vrf10

Critical	Major	Minor	Warning
0	0	0	0

General

Account
ct1

Region
centralus

Cloud Resources

1 Regions	0 Routers	4 Network Security Groups
0 Virtual Machines	0 Endpoints	

Application Management

1 Application Profiles	3 EPGs	1 Cloud Context Profiles
1 VRFs	0 Service Graphs	

Settings

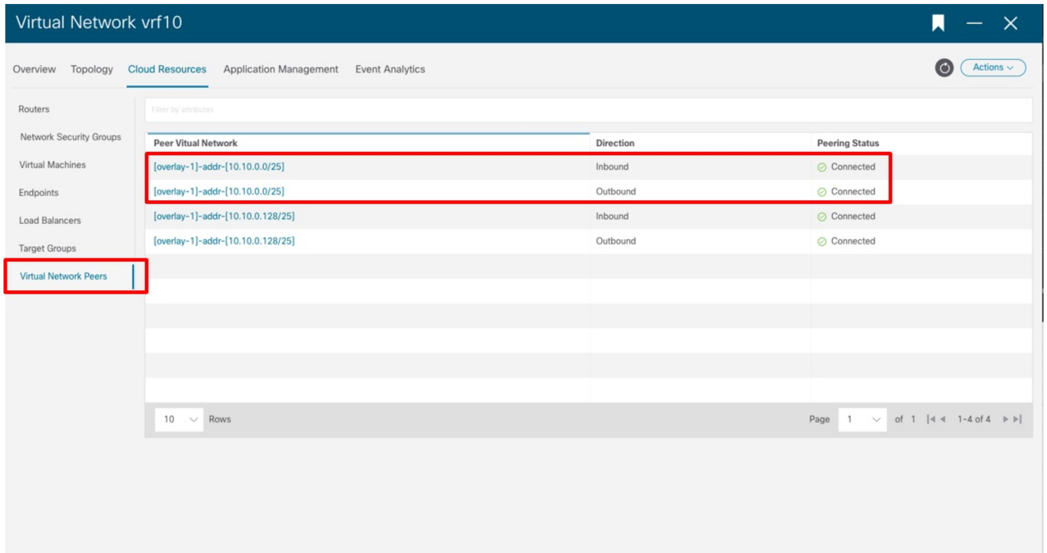
Cloud Context Profile

Connectivity Status

Central US Cloud APIC Deployed

Step 5 In the left navigation pane, choose Cloud Resources > Virtual Network Peers, then click the Cloud Resources tab.

The information displayed in this window shows the bi-directional peerings.

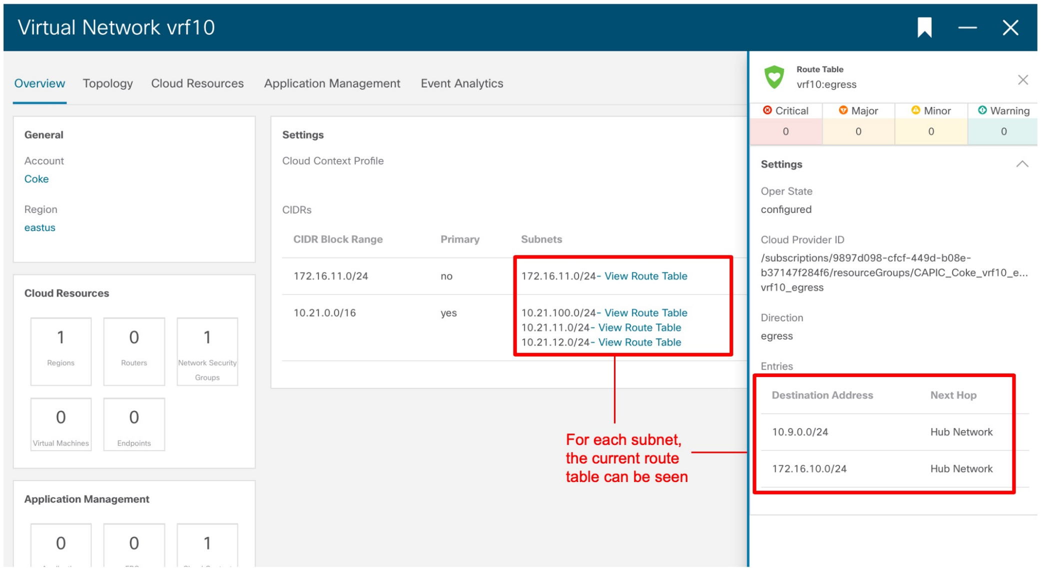


Peer Vitual Network	Direction	Peering Status
[overlay-1]-addr-[10.10.0.0/25]	Inbound	✓ Connected
[overlay-1]-addr-[10.10.0.0/25]	Outbound	✓ Connected
[overlay-1]-addr-[10.10.0.128/25]	Inbound	✓ Connected
[overlay-1]-addr-[10.10.0.128/25]	Outbound	✓ Connected

Step 6 To check routes, in the same page, click the Overview tab.

UDRs (routes) for peering are driven by contracts defined between EPGs. Check the configuration for contracts if routes are not present.

For each subnet shown in the main window, you can also see the current route table, as shown in the following figure.



Account
Coke

Region
eastus

Cloud Context Profile

CIDRs

CIDR Block Range	Primary	Subnets
172.16.11.0/24	no	172.16.11.0/24- View Route Table
10.21.0.0/16	yes	10.21.100.0/24- View Route Table 10.21.11.0/24- View Route Table 10.21.12.0/24- View Route Table

For each subnet, the current route table can be seen

Oper State
configured

Cloud Provider ID
/subscriptions/9897d098-cfcf-449d-b08e-b37147f284f6/resourceGroups/CAPIC_Coke_vrf10_e...vrf10_egress

Direction
egress

Entries

Destination Address	Next Hop
10.9.0.0/24	Hub Network
172.16.10.0/24	Hub Network

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, 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.

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.