



Importing Existing Brownfield AWS Cloud VPCs Into Cisco Cloud APIC

[New and Changed Information](#) 2

[Benefits of Importing Existing Brownfield AWS Cloud VPCs into Cisco Cloud APIC](#) 2

[Terminology Used In This Document](#) 5

[About Transit Gateway Attachments for Unmanaged \(Brownfield\) VPCs](#) 5

[What Cisco Cloud APIC Does and Does Not Do With Brownfield VPCs](#) 6

[Guidelines and Restrictions](#) 7

[Workflow for Importing Existing Brownfield Cloud VPCs Into Cisco Cloud APIC](#) 8

[Updates in Release 25.0\(4\)](#) 9

[Configuring Access Policies at Different Levels](#) 16

[Copying a Route Table Associated with a Brownfield VPC](#) 23

[Creating an Unmanaged \(Brownfield\) Cloud Context Profile](#) 25

[Adding the Transit Gateway Attachment for an Unmanaged VPC in AWS](#) 32

[Creating an EPG Associated With the Brownfield Cloud Context Profile](#) 33

[Completing the Remaining Configurations for the Brownfield VPC in AWS](#) 41

[Trademarks](#) 44

Revised: July 13, 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
25.0(4)	Updates to access policies	This release provides updates for access policies for Cisco Cloud APIC with AWS, where new access policies are available at different levels. See Updates to Access Policies in Release 25.0(4), on page 10 for more information.
25.0(4)	Route table copying	This release allows for route table copying when importing brownfield VPCs into Cisco Cloud APIC. See About Route Table Copying, on page 14 for more information.
25.0(2)	Support for importing existing brownfield AWS cloud VPCs into Cisco Cloud APIC	This release provides support for importing existing brownfield AWS cloud VPCs into Cisco Cloud APIC.

Benefits of Importing Existing Brownfield AWS Cloud VPCs into Cisco Cloud APIC



Note

- In this document, a brownfield VPC is defined as a VPC that you create without Cisco Cloud APIC intervention. For this initial support in release 25.0(2), a brownfield VPC and an unmanaged VPC mean the same thing.
- This document deals specifically with importing existing brownfield **AWS cloud VPCs** into Cisco Cloud APIC, which is supported beginning with release 25.0(2).

For information on importing existing brownfield **Azure cloud VNets** into Cisco Cloud APIC, which was supported beginning with release 5.2(1), see [Importing Existing Brownfield Azure Cloud VNets Into Cisco Cloud APIC](#).

Prior to release 25.0(2), cloud deployments through Cisco Cloud APIC are considered greenfield deployments, where the configurations for the necessary components (resource groups, VPCs, CIDRs, subnets, and so on) are done through the Cisco Cloud APIC. You would then deploy the services under these resource groups created through the Cisco Cloud APIC to bring up your applications.

Many users who have adopted Amazon Web Services (AWS) Cloud for their data center extensions have hundreds of VPCs and instances already deployed in the cloud. This results in having two different environments, one for the new greenfield configurations through Cisco Cloud APIC and existing brownfield configurations on AWS. This is not ideal if you don't want separate control points for your existing cloud resources once you adopt the Cisco Cloud APIC solution.

Prior to release 25.0(2), existing brownfield environments, where the resource groups and VPCs were created without using Cisco Cloud APIC, were not able to coexist in a Cisco Cloud APIC-managed site. Beginning with release 25.0(2), support is now available

for importing existing brownfield AWS VPCs into Cisco Cloud APIC. This enhancement uses AWS transit gateway to provide communication between greenfield VPCs configured through Cisco Cloud APIC and brownfield VPCs that were configured outside of Cisco Cloud APIC.

The following figures show example AWS topologies, where AWS transit gateway is configured or AWS transit gateway connect is configured. For more information on Cisco Cloud APIC and AWS transit gateway or transit gateway connect, see [Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect](#).

Figure 1: Example AWS Topology with AWS Transit Gateway

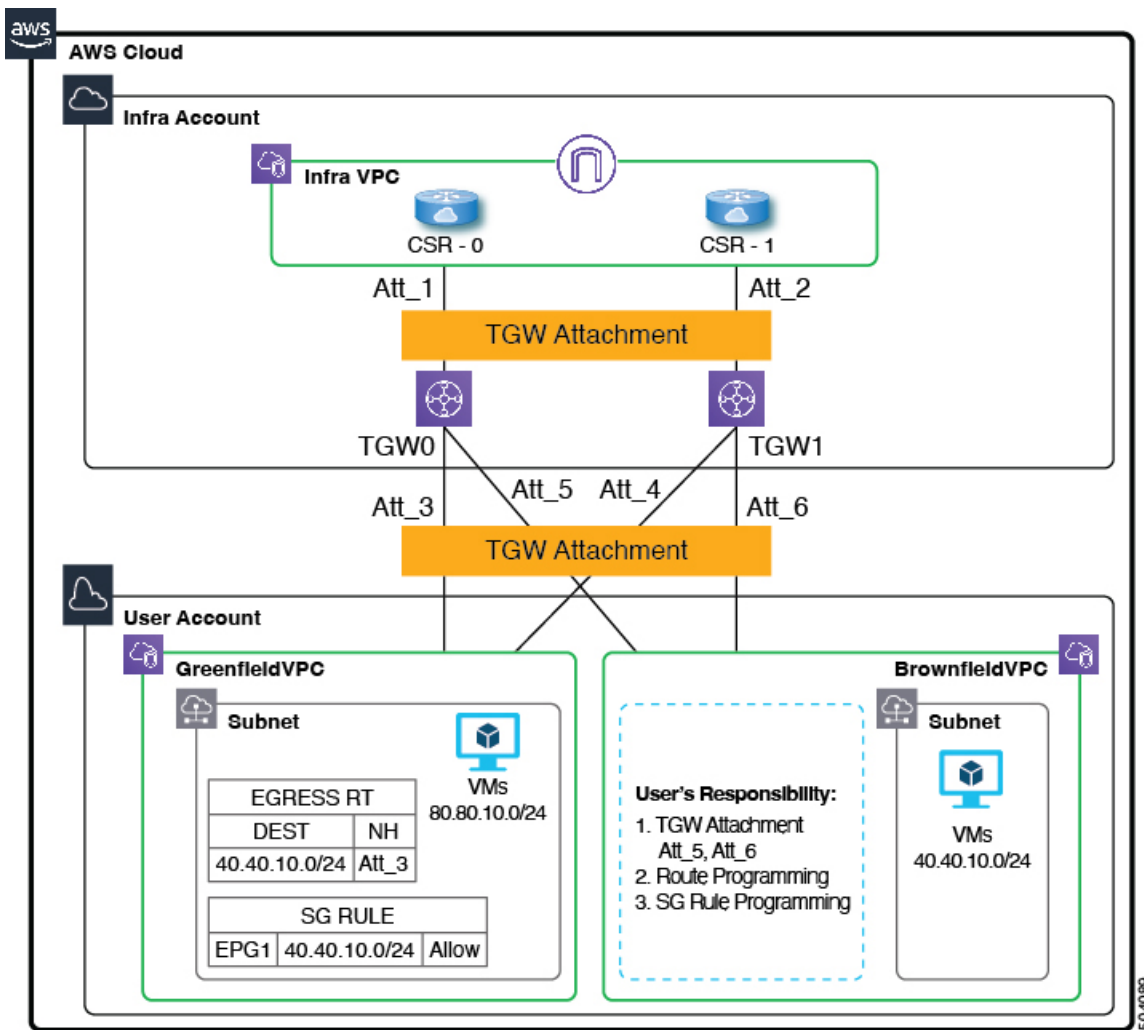
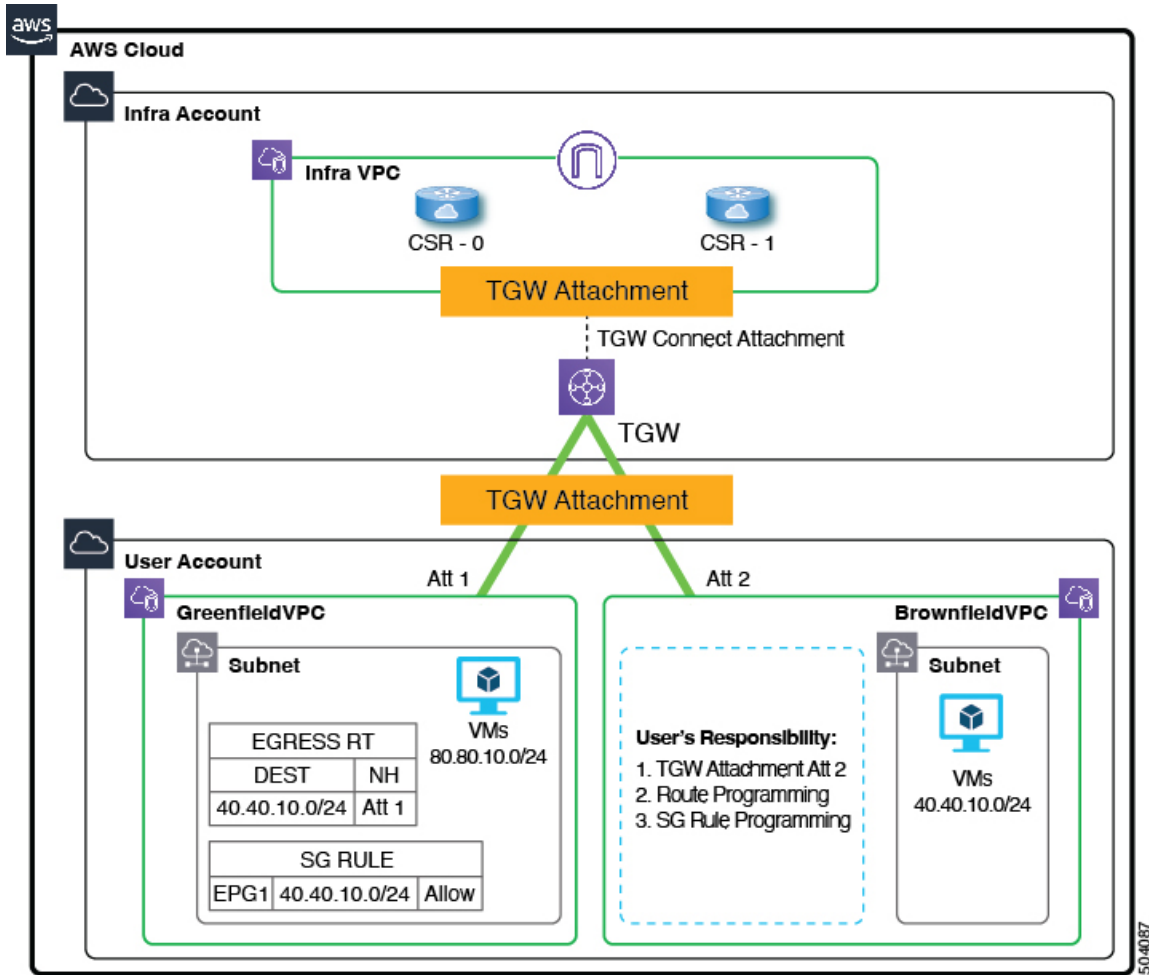


Figure 2: Example AWS Topology with AWS Transit Gateway Connect



In the figures above:

- The infra VPC and the greenfield VPC were created and are managed through Cisco Cloud APIC. In addition, for the greenfield VPC, the transit gateway attachment is created by the Cisco Cloud APIC.
- The brownfield VPC was created by you through AWS and is managed outside of Cisco Cloud APIC.

Note that with this feature, Cisco Cloud APIC does not configure or provision anything in the existing brownfield resource groups. The security group rules, route tables, and routes are not programmed through Cisco Cloud APIC for these brownfield resource groups. Cisco Cloud APIC will not manage security group rules, route tables, and routes for these existing brownfield deployments, so you will continue to manage security group rules, route tables, and routes for those existing brownfield deployments outside of Cisco Cloud APIC.

In addition, if you have existing cloud resources under a brownfield VPC that you do not want to import into Cisco Cloud APIC (such as CIDRs, subnets, route tables, transit gateway or transit gateway VPC attachments), these existing cloud resources will continue to exist in the cloud without any modifications or deletions from Cisco Cloud APIC. With a read-only access policy, aside from running a read inventory, Cisco Cloud APIC will have no privileges on these existing cloud resources.

Terminology Used In This Document

This section introduces some of the key terminology and concepts used in this document:

Greenfield VPC

A VPC in AWS that is created and managed by Cloud APIC based on the cloud context profile.

Brownfield or unmanaged VPC

A VPC in AWS that is created without using a policy through Cloud APIC.

Access policy

Policies that are created on Cloud APIC that denote the respective privilege.

Prior to release 25.0(4), the access policies are:

- Default
- Read-Only
- Unmanaged

Beginning with release 25.0(4), the access policies are:

- Read Only
- Routing Only
- Routing & Security

Note that most of these access policies can be applied at the global, account/tenant, VPC, and subnet levels (Read Only is not supported at the global level). See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

Route table copying

A new feature introduced in release 25.0(4). Describes the ability to copy routes from route tables that are associated with the subnets in a brownfield VPC when you import that brownfield VPC into Cisco Cloud APIC. Cisco Cloud APIC does not modify any existing route tables associated with a brownfield VPC, but rather copies all the routes from that route table into a Cisco Cloud APIC-created route table when you import a brownfield VPC into Cloud APIC.

About Transit Gateway Attachments for Unmanaged (Brownfield) VPCs



Note The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect what Cisco Cloud APIC configures transit gateway attachments with brownfield VPCs. See [How the Brownfield VPC Import Differs in Release 25.0\(4\), on page 16](#) for more information.

Typically, when Cisco Cloud APIC creates a greenfield VPC on the cloud as part of the AWS Transit Gateway configuration, it also configures the transit gateway attachment between the greenfield VPC and the transit gateway.

However, when configuring the AWS Transit Gateway with an unmanaged (brownfield) VPC, Cisco Cloud APIC is not able to configure the transit gateway attachment between the brownfield VPC and the infra transit gateway, so that transit gateway attachment configuration for the brownfield VPC must be done manually by you.

In order to have communication between the greenfield VPC and the brownfield VPC, you must manually configure the transit gateway attachment for the brownfield VPC to the greenfield transit gateway (the TGW created by Cisco Cloud APIC). Without this, the packet flow will not occur between the greenfield VPC and the brownfield VPCs.

For more information, see [Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect](#).

What Cisco Cloud APIC Does and Does Not Do With Brownfield VPCs



Note The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect what Cisco Cloud APIC does and does not do with brownfield VPCs. See [How the Brownfield VPC Import Differs in Release 25.0\(4\), on page 16](#) for more information.

With this enhancement as part of release 25.0(2), Cisco Cloud APIC is able to orchestrate the network connectivity and security required on the greenfield resource group/VPC side to be able to send and receive packets from a brownfield VPC.

When you register a brownfield VPC with Cisco Cloud APIC, the following configurations take place:

- An inventory pull is performed on the brownfield resource group or VPC.
- Based on the contracts with between the brownfield cloud EPGs and the greenfield cloud EPGs, Cisco Cloud APIC will make the necessary configurations only in certain areas:
 - Cisco Cloud APIC programs the security group rules for the greenfield VPC to allow inbound and outbound traffic to and from the brownfield VPCs. Cisco Cloud APIC does not program the security group rules for the brownfield VPC. You must manually program the security group rules for the brownfield VPC separately.
 - Cisco Cloud APIC does not program any route tables or routes for the brownfield VPC. In order for the brownfield VPC to communicate with the greenfield VPC, you must manually make the following configurations:
 - Create the contract between the greenfield and brownfield EPGs
 - Create the transit gateway VPC attachment with the greenfield infra transit gateway
 - Create the route table for the brownfield VPC and subnet.
 - Add the routes where the destinations are the greenfield CIDRs and the next hop is the transit gateway VPC attachment
- Cisco Cloud APIC creates a VRF corresponding to the brownfield VPC on all of the CSRs with the access control lists and routes corresponding to the CIDRs in the brownfield VPC. Cisco Cloud APIC also configures route leaking in the CSR based on the configured contracts.
- Cisco Cloud APIC shares the greenfield infra transit gateway to the AWS account that was used to create the brownfield VPC. At this point, you must manually create the transit gateway VPC attachment before the import of the brownfield VPCs into Cisco Cloud APIC can continue.

Cloud EPGs associated with brownfield cloud context profiles through the VRF should have subnet-based endpoint selectors (tag-based EPGs will not be applicable on brownfield cloud context profiles).

Cisco Cloud APIC does not create any cloud resources with regards to the brownfield VPC, such as configuring route programming, or creating security group rules or transit gateway VPC attachments.

In addition, the following Cisco Cloud APIC components are affected or are not affected when you register a brownfield VPC with Cisco Cloud APIC:

- No changes take place with CSR programming for the brownfield VRF. From the CSR perspective, the brownfield VRF will behave like any other VRF. On the CSR, the brownfield VRF will be programmed along with the CIDRs imported as part of the brownfield cloud context profile. The CSR doesn't know if a given VRF is associated with a greenfield or a brownfield cloud context profile.
- Access control lists will be programmed on the GigabitEthernet2 interface to allow traffic coming in from and going to these unmanaged (brownfield) VPC CIDRs. Based on the contracts, route leaking will occur between the EPGs associated with the VRFs.

Guidelines and Restrictions



Note The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect the guidelines and restrictions for importing brownfield VPCs. See [How the Brownfield VPC Import Differs in Release 25.0\(4\), on page 16](#) for more information.

Following are the guidelines and restrictions when importing existing brownfield cloud configurations into Cloud APIC.

- The following guidelines and restrictions apply specifically for unmanaged (brownfield) cloud context profiles:
 - A given VPC ID of an brownfield VPC cannot be mapped to two different unmanaged cloud context profiles on a Cisco Cloud APIC. A given VPC ID can only be used once to create only one unmanaged cloud context profile on a Cisco Cloud APIC.
 - An brownfield VPC mapped to a cloud context profile should reside in the same AWS account as the tenant that is associated with this cloud context profile. Random VPC IDs cannot be given while defining these unmanaged cloud context profiles on the Cisco Cloud APIC.
 - The region should be same as the one where the brownfield VPC has been created.
 - The CIDR should be same as the one configured in the brownfield VPC.
 - Even though you can selectively import all or a particular set of CIDRs under the brownfield VPC, you cannot import a brownfield VPC without its primary CIDR. Importing the primary CIDR is mandatory when importing a brownfield VPC. The primary CIDR can't be altered or changed.
- A hosted VRF can't be used for importing a brownfield VPC.

Workflow for Importing Existing Brownfield Cloud VPCs Into Cisco Cloud APIC



Note The information in this section is applicable if you are running on a release prior to release 25.0(4). Several updates became available as part of the 25.0(4) release, such as changes to access policies and the ability to copy route tables, that affect the workflow for importing existing brownfield VPCs. See [How the Brownfield VPC Import Differs in Release 25.0\(4\), on page 16](#) for more information.

Following is the general workflow for having greenfield VPCs (VPCs configured in and managed by Cisco Cloud APIC) send traffic to and receive traffic from brownfield VPCs (VPCs that are not managed by Cisco Cloud APIC):

1. Verify that the brownfield (unmanaged) VPC has already been created in AWS.

2. Import this brownfield (unmanaged) VPC into Cisco Cloud APIC.

a. Create a new tenant to be used with the unmanaged (brownfield) cloud context profile, if necessary.

The brownfield VPC can be present in the same AWS account or in a different AWS account from the greenfield VPC.

If the brownfield VPC is in a different AWS account, then you must create a new tenant with the AWS Account ID field (`cloudAwsProvider`) field pointing to this account. If this AWS account is used only to manage brownfield VPCs, this tenant will have a relation to the Read Only access policy. This read-only policy means that the events and statistics tasks won't be triggered and flow logs won't be configured on this account. Only the inventory pull will be done on this account.

For instructions on creating a new tenant, see "Configuring a Tenant AWS Provider For Release 4.2(3) and Later" in the [Cisco Cloud APIC for AWS User Guide](#), Release 25.0(x) or later

b. Import the existing brownfield VPC, CIDR, and subnet configurations in to Cisco Cloud APIC.

You do this by creating a cloud context profile corresponding to the brownfield VPC, which creates an association between the brownfield VPC and a VRF. The cloud context profile in Cisco Cloud APIC is an object that is used to link between the brownfield VPC and a VRF. To import the brownfield VPC, you must first create a VRF object, which is a placeholder for the cloud context profile association that will be used later when importing the brownfield VPC.

See [Creating an Unmanaged \(Brownfield\) Cloud Context Profile, on page 25](#) for those procedures.

3. Add the transit gateway attachment for the unmanaged (brownfield) VPC in AWS.

Cisco Cloud APIC does not configure the AWS transit gateway attachment between the unmanaged (brownfield) VPC and the infra transit gateway (TGW created by Cisco Cloud APIC) in AWS. The AWS transit gateway that is created as part of the infra configuration is shared with the brownfield user account, but you must manually configure the AWS transit gateway attachment between the unmanaged (brownfield) VPC and the infra transit gateway in AWS.

See [Adding the Transit Gateway Attachment for an Unmanaged VPC in AWS, on page 32](#) for more information.

4. Create cloud EPGs under this VRF and configure contracts toward any greenfield EPGs.

See [Creating an EPG Associated With the Brownfield Cloud Context Profile, on page 33](#) for those procedures.

When you import the brownfield (unmanaged) VPC into Cisco Cloud APIC:

- Based on the contracts with between the brownfield cloud EPGs and the greenfield cloud EPGs, Cisco Cloud APIC programs the route tables and security group rules for the greenfield VPC.

- Cisco Cloud APIC creates a VRF corresponding to the brownfield VPC on all of the CSRs with the access control lists and routes corresponding to the CIDRs in the brownfield VPC. Cisco Cloud APIC also configures route leaking in the CSR based on the configured contracts.
 - Cisco Cloud APIC does not create any cloud resources with regards to the brownfield VPC, such as configuring route programming, or creating security group rules or transit gateway VPC attachments.
5. Cisco Cloud APIC associates the transit gateway route table and configures the propagation for the brownfield transit gateway VPC attachment. However, Cisco Cloud APIC does not configure the security group rules programming for the brownfield VPC, so you must manually make these configurations yourself through the AWS portal.

Updates in Release 25.0(4)



Note The information in this section describe updates that are available beginning in release 25.0(4).

To understand how certain configurations (such as access policies) were done prior to release 25.0(4), see [What Cisco Cloud APIC Does and Does Not Do With Brownfield VPCs, on page 6](#) and [Workflow for Importing Existing Brownfield Cloud VPCs Into Cisco Cloud APIC, on page 8](#).

- Following are the updates to the access policies beginning in release 25.0(4):
 - Prior to release 25.0(4), you can import a brownfield VPC into Cisco Cloud APIC only using a Read Only access policy (previously referred to as **unmanaged**), where the Cisco Cloud APIC has no write privileges on that brownfield VPC. With the Read Only access policy, the brownfield VPC co-exists in the Cisco Cloud APIC fabric with Cisco Cloud APIC-created (greenfield) VPCs, but any security group or route table configurations that are required on the brownfield VPC are not done through the Cisco Cloud APIC.

Beginning with release 25.0(4), you can now apply the following additional access policies when you import a brownfield VPC into Cisco Cloud APIC:

- Routing & Security
- Routing Only

Based on the access policy that you apply, the Cloud APIC can take full ownership of that imported brownfield VPC.

- Beginning with release 25.0(4), support is also available for changing from one access policy to another access policy. For example, if you initially imported a brownfield VPC with a Routing & Security access policy, you can change the access policy for that imported brownfield VPC to Routing Only at a later date.
- In addition, prior to release 25.0(4), you could only apply access policies at the VPC level. Beginning with release 25.0(4), you can also apply access policies at the global (Cloud APIC), account/tenant, VPC, or subnet levels (note that the Read Only access policy is not supported at the global level).
- In the absence of an explicitly-applied access policy, an object will inherit the access policy from its parent. See [Hierarchy of Access Policies, on page 10](#) for more information.

See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

- When importing a brownfield VPC, you can also copy routes from route tables that are associated with the subnets in that brownfield VPC. Cisco Cloud APIC does not take over existing route tables that are already present in that brownfield VPC in

this case. Instead, Cisco Cloud APIC copies the existing route tables that are associated with the subnets in the brownfield VPC that is being imported, then controls routes through Cloud APIC-created route tables that are copied from the brownfield VPC route tables.

- The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

Updates to Access Policies in Release 25.0(4)

Following are the updates to the access policies that are available beginning in release 25.0(4):

- [About the New Access Policies, on page 10](#)
- [Hierarchy of Access Policies, on page 10](#)
- [When You Might Use Different Access Policies, on page 13](#)
- [Guidelines and Limitations, on page 13](#)

About the New Access Policies

Prior to release 25.0(4), support was available only for the Read Only access policy. Beginning with release 25.0(4), the following access policies are now available, listed in order of greater privileges (least restrictive) to lesser privileges (more restrictive):

- **Routing & Security access policy:** The default access policy. If you do not assign an access policy to an object, then that object has a Routing & Security access policy applied to it by default.

Assigning a Routing & Security access policy to an object means that it has full permissions, where it is able to control Routing & Security. This is the typical access policy that would normally be applied to an object if you were to create that object through Cisco Cloud APIC (if this were a greenfield object created through Cisco Cloud APIC).

- **Routing Only access policy:** Assigning a Routing Only access policy to an object means that it can control only the routing policy and the network connectivity.
- **Read Only access policy:** The existing access policy that was available prior to release 25.0(4). Assigning a Read Only access policy to an object means that it does not have write permissions and can only read the inventory. Note that the Read Only access policy is not supported at the global (Cisco Cloud APIC) level.

Hierarchy of Access Policies

Following is the hierarchy of the objects where access policies can be applied, in order from the highest level to the lowest level. Note that for each level, while the children objects under a parent object automatically inherit the access policy applied at the parent level, you can also manually change the access policy for any child under a parent object within the guidelines provided later in this section.

1. **Global Level:** Access policies applied at the global level (the `cloudDomP` level) are attached to a cloud account or cloud provider and affect the entire Cisco Cloud APIC system. All objects created or imported with the Inherit option under this Cisco Cloud APIC (such as tenants, VPCs, and subnets) automatically inherit the access policy applied at this global level.

You can configure the access policy at the global level during the initial first time setup of the Cisco Cloud APIC.

- By default, the access policy at the global level will be set to Routing & Security.
- Routing Only is the only other valid alternate access policy at the global level. The Read Only access policy is not supported at the global level.

2. **Account/Tenant Level:** Access policies applied at the account/tenant level (the `cloudAccount` level) apply to all resources within that account. All objects created or imported with the Inherit option under the account or tenant (such as VPCs and subnets) automatically inherit the access policy applied at the account or tenant level.

If the account is set to a Read Only access policy, then the extra resources are not created on the cloud in this account.

3. **VPC Level:** Access policies applied at the VPC level (the `cloudCtxProfile` level) apply to all resources within that VPC. All objects created or imported with the Inherit option under the VPC (such as subnets) automatically inherit the access policy applied at the VPC level.

Assigning an access policy at the VPC level affects the following resources within that VPC:

- Route tables in the VPC or resource group
- The attachment for the VPC to the transit gateway
- Security groups and their rules

4. **Subnet Level:** Access policies applied at the subnet level (the `cloudSubnet` level) apply to all resources under that subnet.

Assigning an access policy at the subnet level affects the following resources under that subnet:

- Association of the subnet to the given routing table
- Association of the subnet to the NSG or the endpoints in that subnet that are associated with that security group

The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

In addition, following is a list of the access policies mentioned earlier, listed in order of greater privileges (least restrictive) to lesser privileges (more restrictive):

1. **Routing & Security access policy**
2. **Routing Only access policy**
3. **Read Only access policy**

For any of the levels listed above, the following rules apply:

- When you set an access policy at a parent level, any objects created or imported with the Inherit option underneath that level automatically inherit the access policy of the parent.
- However, policies can be overridden at any child level. At any child level in the hierarchy shown above, if you want a more restrictive policy than the policy set for the parent, setting a different policy at that child level will override the policy applied at parent level. Note that the policy applied at the child level (the overriding policy) must be more restrictive or equal to the policy applied at the parent level.
- If the children access policies are using the Inherit options and you change an access policy at a parent level at some point in the future, then the access policy for all of the children under that parent policy automatically change to match the parent at that point.

For example, assume the following scenario:

1. You set the access policy at the **global level** to a **Routing & Security** access policy. At this point, if you create or import objects under the global level with the Inherit option along with the access policy, all objects under that Cisco Cloud APIC is set with a Routing & Security access policy, which is the access policy with the greatest privileges (the least restrictive access policy).

2. You then manually change the access policy at the **subnet level** to a **Read Only** access policy. The access policies are then set for the objects within the Cisco Cloud APIC in this way:

- All objects created or imported with the Inherit option under the global level, but above the subnet level, are set with a Routing & Security access policy.
- All objects created or imported with the Inherit option under the subnet level are set with a Read Only access policy.

Note that the changes take effect only for the subnet where the access policy was changed. New subnets imported will continue to have the Inherit access policy by default unless otherwise changed.

3. Then, at some point in the future, you decide to change the access policy at the **global level** again, this time setting the global level access policy to a **Routing Only** access policy. At that point, all of the children objects under the global level, but above the subnet level, that are created or imported with the Inherit option are set to the parent's Routing Only access policy.

However, because you had manually set the access policy at the subnet level to the Read Only access policy, the access policy does not change at the subnet level, even though the access policy changed at the global level; this is because the access policy at the subnet level was not set to Inherit the access policy at the global level. All objects created or imported with the Inherit option under the subnet level remain with a Read Only access policy.

Following is a set of example scenarios and how access policies would be applied at various levels for each scenario.

Table 1: Example Access Policy Scenarios

Levels				
Global	Account/Tenant	VPC	Subnet	Notes
Routing & Security access policy	Inherit	Inherit	Inherit	Valid configuration <ul style="list-style-type: none"> • Routing & Security access policy applied at the global level by default • All objects created or imported with the Inherit option under global level (account/tenant, VPC, and subnet levels) inherit the Routing & Security access policy that was applied at the global level
Routing & Security access policy	Inherit	Routing Only access policy	Inherit	Valid configuration <ul style="list-style-type: none"> • Routing & Security access policy applied at global level and inherited at the account/tenant level • Routing Only access policy applied at VPC level and inherited at the subnet level

Levels				
Global	Account/Tenant	VPC	Subnet	Notes
Routing Only access policy	Routing & Security access policy (invalid configuration)	Inherit	Inherit	Invalid configuration <ul style="list-style-type: none"> • Routing Only access policy is more restrictive than Routing & Security access policy • Policy at child (account/tenant) level cannot be more restrictive than parent (global) level • As long as the access policy is set to Routing Only at the global level, the account/tenant and lower objects can have only the Routing Only or Read Only access policies

When You Might Use Different Access Policies

Following are several use cases where you might use different access policies:

- **Gradual migration of brownfield resources:** Assume that you have an existing brownfield VPC with a number of subnets and you want to migrate one subnet, leaving the remaining subnets untouched. You could accomplish this task using access policies in the following manner:
 - Assign a Routing & Security access policy for the one subnet that you want to migrate.
 - Assign a Read Only access policy for the remaining subnets that you want to leave untouched.
- **Granular control over what the Cisco Cloud APIC does to the cloud resources:** Using different access policies, you can have Cisco Cloud APIC-managed resources and brownfield resources co-existing in the same VPC.

For example, assigning a Routing Only access policy at any level means that you are entirely in control of the network at that level. Conversely, assigning a Routing & Security access policy at any level means that the Cisco Cloud APIC controls the Routing & Security at that level.
- **Having brownfield and greenfield VPCs co-exist in Cisco Cloud APIC fabric:** When importing a brownfield VPC into Cisco Cloud APIC, that brownfield VPC is able to co-exist with Cisco Cloud APIC-created and managed VPCs by using different access policies.
- **Determining overall functionality of Cisco Cloud APIC:** For example, if you wanted to use the Cisco Cloud APIC only for routing, and have the security policy managed outside of Cisco Cloud APIC. In that case, you would assign a Routing Only access policy at the Cisco Cloud APIC level.

Guidelines and Limitations

Following are the guidelines and limitations for the new access policies that are available in release 25.0(4):

- Following are the restrictions for the access policies at various levels:
 - At the global level, only the Routing & Security and Routing Only access policies are supported; the Read Only access policy is not a valid option at the global level.
 - However, all three access policies (Routing & Security, Routing Only, and Read Only) are supported for all remaining levels (account/tenant, VPC, and subnet).

- For greenfield VPCs:
 - You can apply the Routing Only access policy if you want the Cisco Cloud APIC to manage only the routing and not the security.
 - The Read Only access policy is not supported for greenfield VPCs.

About Route Table Copying

Beginning with release 25.0(4), support is available for copying routes from certain route tables that are created outside of Cisco Cloud APIC. This provides the ability to copy routes from route tables that are associated with the subnets in a brownfield VPC when you import that brownfield VPC into Cisco Cloud APIC.

In this situation, Cisco Cloud APIC does not modify any existing route tables that are associated with the subnets in a brownfield VPC, but rather copies the routes from that route table into a Cisco Cloud APIC-created route table when you import a brownfield VPC into Cloud APIC or when you use the **Copy Existing Routes** option in the Cloud APIC GUI. You can then make modifications to that Cloud APIC-created route table that is associated with the imported brownfield VPC, if necessary. An option is also available for you to select multiple route tables so that all of the routes from multiple route tables will be copied into this Cloud APIC-created route table.

In order to copy routes from route tables that are associated with the subnets in a brownfield VPC to a Cloud APIC-created route table:

1. You will be provided with an option to select one or more route tables that you can opt to copy and the source VRF that will be used for the brownfield VPC route table.
2. Select subnets corresponding to the route tables.
3. Cisco Cloud APIC then creates its own routing table and populates the routes from the route tables and associates all selected subnets with this table.

You can copy a route table at two different points in time:

- As part of the initial first time setup operation, where you are importing a brownfield VPC while you are setting up the Cisco Cloud APIC and you want to copy the routes in a route table that is associated with the subnets in that imported brownfield VPC.
- As an update operation at some point later on. Note that this applies only in the following situations:
 - If you imported a brownfield VPC as part of the initial first time setup operation and did not copy the route table associated with the subnets in that imported brownfield VPC at that time
 - If you imported only **some** of the subnets associated with a route table that you copied previously, or if that copied route table is associated with subnets in multiple VPCs

Then you can copy that route table after the initial first time setup operation as long as there are still subnets in those VPCs associated with that route table that have not been imported into Cloud APIC.

Routes are classified in the following manner in the inventory:

- **Cloud APIC-Owned:** Greenfield routes that are created through Cisco Cloud APIC
- **Cloud APIC-Copied:** Brownfield routes that were created outside of Cisco Cloud APIC but were copied into the Cisco Cloud APIC-created route table when you imported a brownfield VPC into Cloud APIC or when you used the **Copy Existing Routes** option in the Cloud APIC GUI.

- **Other:** Brownfield routes that were created outside of Cisco Cloud APIC but were not copied in the Cisco Cloud APIC-created route table.

Guidelines and Limitations

Following are the guidelines and limitations for the route table copying feature in Cisco Cloud APIC:

- The copying feature applies only to routes. Cisco Cloud APIC does not copy existing security groups associated with the brownfield VPCs. Cisco Cloud APIC creates its own security groups based on the contracts and associates those Cisco Cloud APIC-created security groups with the necessary subnets or endpoints.
- The Cisco Cloud APIC route-leak policy will always override any existing copied routes in the Cisco Cloud APIC-created route table. Cisco Cloud APIC will not delete any brownfield routes in the Cisco Cloud APIC-created route table.

For example, if existing brownfield routes that are copied in the Cloud APIC-created route table match the prefix for Cisco Cloud APIC-created routes, those matched routes are not deleted in the Cisco Cloud APIC-created route table; instead, the Cisco Cloud APIC-created routes take precedence.

- Prior to release 25.0(4), if you manually added a route on a Cloud APIC-created route table, Cisco Cloud APIC would automatically remove that route that you added. Beginning with release 25.0(4), this is no longer the case; any routes that you manually add to a Cloud APIC-created route table is no longer removed, as long as it does not conflict with a Cloud APIC-created route.
- When you copy routes from existing route tables that are associated with the subnets in a brownfield VPC, the existing route tables are affected in the following ways, depending on the access policy:
 - Read Only access policy: The existing route table is not impacted. The option to copy routing is not available. The Cisco Cloud APIC-created route table is not created.
 - Routing & Security access policy:
 - If you select **Copy Existing Routes** when you import a brownfield VPC:
 1. The Cisco Cloud APIC-created route table is created.
 2. The entries are copied from one or multiple route tables into one Cisco Cloud APIC-created route table.
 3. Then the subnets are disassociated from the existing route table.
 - If you select **Do Not Copy Existing Routes** when you import a brownfield VPC:
 1. The Cisco Cloud APIC-created route table is created.
 2. The entries are *not* copied from the existing route tables into the Cisco Cloud APIC-created route table.
 3. However, the subnets are still disassociated from the existing route table - in this case, you should expect traffic loss.

How the Brownfield VPC Import Differs in Release 25.0(4)



Note The information in this section describe updates that are available beginning in release 25.0(4).

To understand how certain configurations (such as access policies) were done prior to release 25.0(4), see [What Cisco Cloud APIC Does and Does Not Do With Brownfield VPCs, on page 6](#) and [Workflow for Importing Existing Brownfield Cloud VPCs Into Cisco Cloud APIC, on page 8](#).

Beginning with release 25.0(4), the following things occur when you import a brownfield VPC into Cisco Cloud APIC:

- You select the subnets in the brownfield VPC that you want to bring under Cisco Cloud APIC ownership, and Cisco Cloud APIC takes ownership of the brownfield VPC and its subnets, based on the access policy that you apply. See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.
- Cloud APIC does not take over existing route tables that are already present in that brownfield VPC in this case, and instead removes the associations with the subnets in the brownfield VPC from the brownfield route tables and controls routes through Cloud APIC-created route tables that are copied (see [About Route Table Copying, on page 14](#) for more information). You select the route tables that you want to copy that are present under the brownfield VPC. Routing is controlled through the Cisco Cloud APIC-created routing table, and existing subnets on the brownfield VPCs are associated with these Cisco Cloud APIC-created routing tables.

The subnet association is removed from the brownfield route tables.

- The brownfield VPC will be attached to the Cisco Cloud APIC-created infra network (the Cisco Cloud APIC-created transit gateway to the Cisco Cloud APIC-created infra VPCs). When you import a brownfield VPC with the corresponding access policy, Cisco Cloud APIC automatically attaches this VPC to the AWS transit gateway. However, Cisco Cloud APIC does not remove attachments, if any, in the brownfield side; instead, it creates an attachment to the Cisco Cloud APIC-created routing table.
- A brownfield VPC might contain existing CIDRs and subnets, so you can import those existing CIDRs and subnets when you import a brownfield VPC into Cisco Cloud APIC. Additionally, you can also create new CIDRs or subnets in that brownfield VPC through the Cisco Cloud APIC, depending on the access policy. For example, if the access policy of a brownfield VPC that you are importing has Routing & Security access privileges, then you can create new CIDRs and subnets on that particular brownfield VPC through the Cisco Cloud APIC.

You can create or modify additional CIDRs or subnets on brownfield VPCs by directly posting the configuration under the brownfield cloud context profile on the Cisco Cloud APIC.

Configuring Access Policies at Different Levels

Following are the updates to the access policies beginning in release 25.0(4):

- Prior to release 25.0(4), you can import a brownfield VPC into Cisco Cloud APIC only using a Read Only access policy, where the Cisco Cloud APIC has no write privileges on that brownfield VPC. With the Read Only access policy, the brownfield VPC co-exists in the Cisco Cloud APIC fabric with Cisco Cloud APIC-created (greenfield) VPCs, but any security group or route table configurations that are required on the brownfield VPC are not done through the Cisco Cloud APIC.

Beginning with release 25.0(4), you can now apply the following additional access policies when you import a brownfield VPC into Cisco Cloud APIC:

- Routing & Security

- Routing Only

Based on the access policy that you apply, the Cloud APIC can take full ownership of that imported brownfield VPC.

- Beginning with release 25.0(4), support is also available for changing from one access policy to another access policy. For example, if you initially imported a brownfield VPC with Security & Routing access, you can change the access policy for that imported brownfield VPC to Read Only at a later date.
- In addition, prior to release 25.0(4), you could only apply access policies at the VPC level. Beginning with release 25.0(4), you can also apply access policies at the global (Cloud APIC), account/tenant, VPC, or subnet levels (note that the Read Only access policy is not supported at the global level).
- In the absence of an explicitly-applied access policy, an object will inherit the access policy from its parent. See [Hierarchy of Access Policies, on page 10](#) for more information.

See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

Configuring Access Policies at the Global Level

Access policies applied at the global level (the `cloudDomP` level) are attached to a cloud account or cloud provider and affect the entire Cisco Cloud APIC system. All objects configured under this Cisco Cloud APIC (such as tenants, VPCs, and subnets) automatically inherit the access policy applied at this global level.


This topic describes how to configure access policies at the global level.

- For instructions on configuring access policies at the account or tenant level, see [Configuring Access Policies at the Account/Tenant Level, on page 18](#).
- For instructions on configuring access policies at the VPC level, see [Configuring Access Policies at the VPC Level, on page 19](#).
- For instructions on configuring access policies at the subnet level, see [Configuring Access Policies at the Subnet Level, on page 20](#).

Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 10](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.

Procedure

- Step 1** In the Cloud APIC GUI, click the Intent icon () and select **Cloud APIC Setup**.
- Step 2** In the **Region Management** area, click **Edit Configuration**.
The **Regions to Manage** screen appears.
- Step 3** Click **Next** to advance past the **Regions to Manage** screen.
The **General Connectivity** screen appears.
- Step 4** In the **General Connectivity** screen, scroll down to the **Cloud APIC Access Privilege** area.
- Step 5** Click the scroll-down menu and choose one of the access policies to apply globally, to the entire Cisco Cloud APIC.
 - **Routing & Security**: The default access policy. If you do not assign an access policy to the Cisco Cloud APIC, then the Cisco Cloud APIC has the Routing and Security access policy applied to it by default.

Assigning a Routing and Security access policy to a Cisco Cloud APIC means that it has full permissions, where it is able to control routing and security.

- **Routing Only:** Assigning a routing-only access policy to a Cisco Cloud APIC means that it can control only the routing policy and the network connectivity.

Note The Read Only access policy is not available at the global (Cisco Cloud APIC) level.

Configuring Access Policies at the Account/Tenant Level

Access policies applied at the account/tenant level (the `cloudAccount` level) apply to all resources within that account. All objects under the account or tenant (such as VPCs and subnets) automatically inherit the access policy applied at the account or tenant level.

This topic describes how to configure access policies at the account/tenant level.

- For instructions on configuring access policies at the global level, see [Configuring Access Policies at the Global Level, on page 17](#).
- For instructions on configuring access policies at the VPC level, see [Configuring Access Policies at the VPC Level, on page 19](#).
- For instructions on configuring access policies at the subnet level, see [Configuring Access Policies at the Subnet Level, on page 20](#).

Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 10](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.

Procedure

- Step 1** In the Cloud APIC GUI, click **Application Management > Tenants**.
The **Tenants** screen appears.
- Step 2** In the **Tenants** screen, double-click on the tenant that you want to change the access policies for.
The **Overview** screen appears for this tenant.
- Step 3** Scroll to the bottom of the screen and click **Advanced Settings** to expand that menu option.
- Step 4** Locate the **Cloud Access Privilege** area to see the current access policy setting.

The current access policy setting for the account/tenant is displayed in the following format:

```
<inherit setting>(<current access policy>)
```

For example, if you see this in the **Cloud Access Privilege** for a tenant:

```
Inherited(Routing & Security)
```

That means:

- The access policy for this account/tenant is set to the Routing & Security access policy
- This access policy was inherited from the parent level (in this case, the global, or Cisco Cloud APIC level), which was also set to the Routing & Security access policy

- Step 5** If you want to change the current access policy setting at the account/tenant level, click **Actions > Edit**. The Edit screen for the tenant appears.
- Step 6** Scroll to the bottom of the screen and, if necessary, click **Advanced Settings** again to expand that menu option.
- Step 7** In the **Cloud Access Privilege** area, click the scroll-down menu and choose the access policy for this account/tenant.
- **Routing & Security:** Assigning a Routing & Security access policy to an account/tenant means that it has full permissions, where it is able to control routing and security.
 - **Routing Only:** Assigning a routing-only access policy to an account/tenant means that it can control only the routing policy and the network connectivity.
 - **Read Only:** The existing access policy that was available prior to release 25.0(4). Assigning a read-only access policy to an account/tenant means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the account/tenant level are based on the access policy that was assigned at the parent level (in this case, at the global level). For example, if the access policy at the parent global level is set to Routing Only, then you will only see Routing Only and Read Only as options at the child account/tenant level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

- Step 8** Click **Save**.
-

Configuring Access Policies at the VPC Level

Access policies applied at the VPC level (the `cloudCtxProfile` level) apply to all resources within that VPC. All objects under the VPC (such as subnets) automatically inherit the access policy applied at the VPC level.

Assigning an access policy at the VPC level affects the following resources within that VPC:

- Route tables in the VPC or resource group
- The attachment for the VPC to the transit gateway or the ability to peer with the infra VPC
- Security groups and their rules

This topic describes how to configure access policies at the VPC level.

- For instructions on configuring access policies at the global level, see [Configuring Access Policies at the Global Level, on page 17](#).
- For instructions on configuring access policies at the account/tenant level, see [Configuring Access Policies at the Account/Tenant Level, on page 18](#).
- For instructions on configuring access policies at the subnet level, see [Configuring Access Policies at the Subnet Level, on page 20](#).

Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 10](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.

Procedure

- Step 1** In the Cloud APIC GUI, click **Application Management > Cloud Context Profiles**.
The **Cloud Context Profiles** screen appears.
- Step 2** In the **Cloud Context Profiles** screen, double-click on the cloud context profile that you want to change the access policies for.
The **Overview** screen appears for this cloud context profile.
- Step 3** Scroll to the bottom of the screen and click **Advanced Settings** to expand that menu option.
- Step 4** Locate the **Cloud Access Privilege** area to see the current access policy setting.
The current access policy setting for the cloud context profile is displayed in the following format:
`<inherit setting>(<current access policy>)`
For example, if you see this in the **Cloud Access Privilege** for a cloud context profile:
`Inherited(Routing & Security)`
That means:
- The access policy for this cloud context profile is set to the Routing & Security access policy
 - This access policy was inherited from the parent level (in this case, the account/tenant level), which was also set to the Routing & Security access policy
- Step 5** If you want to change the current access policy setting at the cloud context profile level, click **Actions > Edit**.
The Edit screen for the cloud context profile appears.
- Step 6** Scroll to the bottom of the screen and, if necessary, click **Advanced Settings** again to expand that menu option.
- Step 7** In the **Cloud Access Privilege** area, click the scroll-down menu and choose the access policy for this account/tenant.
- **Routing & Security:** Assigning a Routing & Security access policy to a cloud context profile means that it has full permissions, where it is able to control routing and security.
 - **Routing-Only:** Assigning a routing-only access policy to a cloud context profile means that it can control only the routing policy and the network connectivity.
 - **Read-Only:** Assigning a read-only access policy to a cloud context profile means that it does not have write permissions and can only read the inventory.
- Keep in mind that the access policies available to you at the VPC (cloud context profile) level are based on the access policy that was assigned at the parent level (in this case, at the account/tenant level). For example, if the access policy at the parent account/tenant level is set to Read Only, then you will only see Read Only as an option at the child VPC (cloud context profile) level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\)](#), on page 10 for more information.
- Step 8** Click **Save**.
-

Configuring Access Policies at the Subnet Level

Access policies applied at the subnet level (the `cloudSubnet` level) apply to all resources under that subnet. All objects under the subnet automatically inherit the access policy applied at the subnet level.

Assigning an access policy at the subnet level affects the following resources under that subnet:

- Association of the subnet to the given routing table

- Association of the subnet to the NSG or the endpoints in that subnet that are associated with that security group

The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

This topic describes how to configure access policies at the subnet level.

- For instructions on configuring access policies at the global level, see [Configuring Access Policies at the Global Level, on page 17](#).
- For instructions on configuring access policies at the account/tenant level, see [Configuring Access Policies at the Account/Tenant Level, on page 18](#).
- For instructions on configuring access policies at the VPC (cloud context profile) level, see [Configuring Access Policies at the VPC Level, on page 19](#).

Before you begin

Review the information in [Updates to Access Policies in Release 25.0\(4\), on page 10](#) to understand what is allowed and what is not allowed when assigning or changing access policies at different levels.

Procedure

-
- Step 1** In the Cloud APIC GUI, click **Application Management > Cloud Context Profiles**.
The **Cloud Context Profiles** screen appears.
- Step 2** In the **Cloud Context Profiles** screen, double-click on the cloud context profile that you want to change the access policies for.
The **Overview** screen appears for this cloud context profile.
- Step 3** Click **Actions > Edit**.
The Edit screen for the cloud context profile appears.
- Step 4** Scroll down until you see the **CIDRs** area.
The CIDRs and subnets associated with this cloud context profile are displayed.
- Step 5** Click on the pencil icon on the appropriate CIDR and subnet line.
- Step 6** Locate the **Cloud Access Privilege** column in the **Subnets** area to determine the current access policy setting for the subnet.
The current setting for the access policy for the subnet is displayed in the following format:
<inherit setting> (<current access policy>)
For example, if you see this in the **Cloud Access Privilege** column for a subnet:
Inherited (Routing & Security)
That means:
- The access policy for this subnet is set to the Routing & Security access policy
 - This access policy was inherited from the parent level (in this case, the VPC, or cloud context profile, level), which was also set to the Routing & Security access policy
- Step 7** In the **Cloud Access Privilege** area, click the scroll-down menu and choose the access policy for this subnet.

- **Routing & Security:** Assigning a Routing & Security access policy to a cloud context profile means that it has full permissions, where it is able to control routing and security.
- **Routing Only:** Assigning a routing-only access policy to a cloud context profile means that it can control only the routing policy and the network connectivity.
- **Read Only:** Assigning a read-only access policy to a cloud context profile means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the subnet level are based on the access policy that was assigned at the parent level (in this case, at the VPC level). For example, if the access policy at the parent VPC level is set to Read Only, then you will only see Read Only as an option at the child subnet level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

Step 8 Click **Done**, then click **Save** in the Edit screen for the cloud context profile.

Configuring Access Policies Using the REST API

This topic describes how to configure the new access policies that are available in release 25.0(4). Following are the entries that you would use for the new access policies:

- Security & Routing: `accesspolicy-default`
- Routing Only: `accesspolicy-routing-only`
- Read Only: `accesspolicy-read-only` (not supported at global level)

Before you begin

Review the information provided in [Updates in Release 25.0\(4\), on page 9](#) to better understand the new access policies and other update available in release 25.0(4).

Procedure

Step 1 To set the access policy at the global (Cisco Cloud APIC) level:

```
<polUni>
  <cloudDomP>
    <cloudRsDomPToAccessPolicy tDn="uni/tn-infra/accesspolicy-routing-only" />
  </cloudDomP>
</polUni>
```

Step 2 To set the access policy at the account/tenant level:

```
<polUni>
  <fvTenant name="pepsi" status="">
    <cloudAwsProvider accountId="<account-id>" accessKeyId="<key-id>"
secretAccessKey="<access-key>" shareableAcrossTenant="yes" providerId="aws" status="">
      <cloudRsProviderToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only" />
    </cloudAwsProvider>
  </fvTenant>
</polUni>
```

Step 3 To set the access policy at the cloud context profile and subnet levels:

```
<polUni>
  <fvTenant name="pepsi">
    <cloudCtxProfile name="c3" status="">
      <cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-default"/>
      <cloudBrownfield status="">
        <cloudIDMapping cloudProviderId="vpc-0123456789abcd" status=""/>
      </cloudBrownfield>
      <cloudCidr name="cidr1" addr="40.0.0.0/16" primary="yes" >
        <cloudSubnet ip="40.0.1.0/24" usage="gateway">
          <cloudRsSubnetToAccessPolicy tDn="uni/tn-infra/accesspolicy-routing-only"/>
          <cloudBrownfield status="">
            <cloudIDMapping cloudProviderId="subnet-0123456789abcd" status=""/>
          </cloudBrownfield>
        </cloudSubnet>
        <cloudSubnet ip="40.0.2.0/24" usage="gateway">
          <cloudRsSubnetToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only"/>
          <cloudBrownfield status="">
            <cloudIDMapping cloudProviderId="subnet-dcba987654321" status=""/>
          </cloudBrownfield>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>
```

Copying a Route Table Associated with a Brownfield VPC

Beginning with release 25.0(4), support is available for copying routes from certain route tables that are created outside of Cisco Cloud APIC. This provides the ability to copy routes from route tables that are associated with the subnets in a brownfield VPC when you import that brownfield VPC into Cisco Cloud APIC.

In this situation, Cisco Cloud APIC does not modify any existing route tables that are associated with the subnets in a brownfield VPC, but rather copies the routes from that route table into a Cisco Cloud APIC-created route table when you import a brownfield VPC into Cloud APIC or when you use the **Copy Existing Routes** option in the Cloud APIC GUI. You can then make modifications to that Cloud APIC-created route table that is associated with the imported brownfield VPC, if necessary. An option is also available for you to select multiple route tables so that all of the routes from multiple route tables will be copied into this Cloud APIC-created route table.

You can copy a route table at two different points in time:

- As part of the initial first time setup operation, where you are importing a brownfield VPC while you are setting up the Cisco Cloud APIC and you want to copy the routes in a route table that is associated with the subnets in that imported brownfield VPC. See [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI, on page 25](#) for those instructions.
- As an update operation at some point later on. The procedures in this topic describe how to copy a route table after the initial first time setup operation.

Note that this applies only in the following situations:

- If you imported a brownfield VPC as part of the initial first time setup operation and did not copy the route table associated with the subnets in that imported brownfield VPC at that time
- If you imported only **some** of the subnets associated with a route table that you copied previously, or if that copied route table is associated with subnets in multiple VPCs

Then you can copy that route table after the initial first time setup operation as long as there are still subnets in those VPCs associated with that route table that have not been imported into Cloud APIC.

Before you begin

You can copy a route table at two different points in time. The following sections describe how to copy a route table at either of those points in time:

- To copy a route table as part of the initial first time setup operation, go to [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI](#), on page 25.
- To copy a route table after the initial first time setup operation, follow the procedures in this topic.

Procedure

- Step 1** In the Cloud APIC GUI, click **Application Management > Cloud Context Profiles**.
The **Cloud Context Profiles** screen appears.
- Step 2** In the **Cloud Context Profiles** screen, double-click on the cloud context profile that is associated with the brownfield VPC that you imported previously.
The **Overview** screen appears for this cloud context profile.
- Step 3** Click **Actions > Edit**.
The **Edit Cloud Context Profile** screen for the cloud context profile appears.
- Step 4** Locate the **Copy Existing Routing Tables from VPC** area and click **Copy Existing Routes**.
The **Brownfield Route Tables** fields appear.
- Step 5** Click **Add Brownfield Route Tables**.
The **Select Brownfield Route Tables** page appears, displaying a list of routing tables associated with the subnets in the existing brownfield (unmanaged) VPC that you are importing.
- Step 6** Select the route tables that you want to copy, then click **Select**.
You are returned to the **Edit Cloud Context Profile** screen for the cloud context profile.
- Step 7** Determine if you want import subnets from the VPC.
Make sure that all the desired subnets and their associated route tables are selected for import and copy in order to avoid traffic disruption.
- Note** The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.
- Follow these steps to import the subnets from this VPC.
- a) Scroll up to the CIDRs area and click on the pencil icon to edit a CIDR block range.
The **Edit CIDR** page appears.
 - b) In the **Import Subnets from VPC** area, click the box next to **Enabled**.
The subnets available to import from this brownfield VPC are displayed.
 - c) Select the subnets to import from this VPC, then click **Done**.
You are returned to the **Edit Cloud Context Profile** page for the cloud context profile.
- Step 8** In the **Edit Cloud Context Profile** page, click **Save**.
-

Creating an Unmanaged (Brownfield) Cloud Context Profile

The following topics provide information for creating an unmanaged (brownfield) cloud context profile.

About Unmanaged (Brownfield) Cloud Context Profiles

An unmanaged (brownfield) cloud context profile refers to a configuration that is posted on the Cisco Cloud APIC that is associated with the unmanaged (brownfield) VPC.

An account can have read-write access (which can support the creation of both greenfield and brownfield VPCs) or read-only access (which can support the creation of only brownfield VPCs). Therefore, you can create an unmanaged (brownfield) cloud context profile under an account with the default access policy (read-write) and also under an account with a read-only access policy.

In addition, if you have an account with the default access policy (read-write) where you already have Cisco Cloud APIC-configured VPCs, and you also have unmanaged VPCs in the same AWS account, you can define the unmanaged cloud context profile under the tenant associated with this account. In other words, if you already have a tenant created that is being used with a greenfield cloud context profile, that same tenant can be used for the brownfield cloud context profile (the unmanaged VPC import) creation as well.

Following are the necessary parameters that you will have to configure for an unmanaged (brownfield) cloud context profile:

- **VRF:** The VRF on the Cisco Cloud APIC where you want to associate the unmanaged VPC
- **Region:** The region where the unmanaged VPC is present on the cloud
- **VPC ID:** The cloud provider ID of this unmanaged VPC on the cloud
- **CIDRs:** The CIDRs that need to be referred to on the Cisco Cloud APIC

The Cisco Cloud APIC will use these parameters to map the brownfield cloud context profile to the given VPC on the cloud.

Creating an Unmanaged (Brownfield) Cloud Context Profile Using the GUI

Before you begin

Review the information provided in [About Unmanaged \(Brownfield\) Cloud Context Profiles, on page 25](#) before going through these procedures.

Procedure

- Step 1** Create a new tenant to be used with the unmanaged (brownfield) cloud context profile, if necessary.
- If the unmanaged (brownfield) VPC is in a different AWS account, then you must create a new tenant.
- For instructions on creating a new tenant, see "Configuring a Tenant AWS Provider For Release 4.2(3) and Later" in the [Cisco Cloud APIC for AWS User Guide](#), Release 25.0(x) or later.
- Note that this tenant should use the same AWS account as the unmanaged (brownfield) VPC in AWS.
- Step 2** Create a VRF that will be associated with the cloud context profile for the brownfield VPC.
- a) In the Cisco Cloud APIC GUI, in the left nav bar, click **Application Management > VRFs**.
A list of configure VRFs appears.
 - b) Click **Actions > Create VRF**.

The **Create VRF** page appears.

- c) Enter the appropriate values in each field as listed in the following *Create VRF Dialog Box Fields* table then continue.

Table 2: Create VRF Dialog Box Fields

Properties	Description
General	
Name	Enter a name for the VRF in the Name field. All VRFs are assigned a <i>vrfEncoded</i> value. If the Tenant and VRF name combination has more than 32 characters, then, a VRF name (which also contains the tenant name) is identified in the cloud router using the <i>vrfEncoded</i> value. To see the <i>vrfEncoded</i> value, navigate to Application Management > VRFs subtab. Click a VRF on the right hand pane and look for <i>Encoded VRF Name in Cloud Router</i> .
Tenant	To choose a tenant: <ol style="list-style-type: none"> 1. Click Select Tenant. The Select Tenant dialog box appears. 2. From the Select Tenant dialog, click to choose a tenant in the left column then Select the tenant that is associated with the unmanaged (brownfield) VPC. 3. Click Select. You return to the Create VRF dialog box.
Description	Enter a description of the VRF.

- d) When finished, click **Save**.

Step 3 In the Cisco Cloud APIC GUI, click the Intent icon ().

A slide-in pane appears from the right of the window, asking **What would you like to do?**

Step 4 Click the **Import Brownfield VPC** option.

A setup wizard for creating an unmanaged cloud context profile appears.

Step 5 In the **Import Brownfield VPC** window, in the **Settings** area, click **Select Brownfield VPC**.

The **Select Brownfield VPC** window appears, with a list of all available brownfield VPCs (VPCs that are not managed by Cisco Cloud APIC) that are available in AWS under the AWS account where you created the tenant. The list of VPCs that is populated in this window is based on the inventory pull on this AWS account.

Note It might take 8-10 minutes to complete the inventory pull, so if you do not see the brownfield VPC listed, wait for 8-10 minutes for the inventory pull to complete.

Step 6 Locate the unmanaged VPC from the list that you want to import and associate with the unmanaged cloud context profile.

In this window in the Cisco Cloud APIC GUI, the unmanaged VPCs in this list are shown with this format in the **Cloud Provider ID** column:

VPC_ID

AWS > {tenant} > {AWS_region}

And the name of the brownfield VPC in the **Name** column in the Cisco Cloud APIC GUI page.

Go to the Amazon VPC console at <https://console.aws.amazon.com/vpc/> and locate the unmanaged VPC in the AWS page, then locate the **Name** and **VPC ID** fields for this brownfield VPC to verify that the information matches with the information displayed in the Cisco Cloud APIC GUI page.

- Step 7** Click on the appropriate unmanaged VPC from the list.
The right pane in the window is populated with additional information about this unmanaged VPC.
- Step 8** Click **Select**.
You are returned to the main **Import Brownfield VPC** window.
- Step 9** In the **Tenant** field, the tenant entry is automatically populated.
Once an unmanaged VPC is selected from the list to import, the corresponding tenant is automatically populated in this field. This unmanaged cloud context profile will be created under this tenant.
- Step 10** In the **VRF** field, select an existing VRF or create a new VRF that will be associated with this unmanaged cloud context profile.
- Step 11** In the **Cloud Context Profile** field, enter a name for this unmanaged cloud context profile.
- Step 12** Click **Advanced Settings** to expand that menu option, if necessary.
- Step 13** In the **Cloud APIC Access Privilege** field, determine how the current access policy is set at the VPC (cloud context profile) level.
Beginning with release 25.0(4), additional access policies are available at the VPC (cloud context profile) level. The access policy is set to Inherit by default, unless you explicitly change the access policy at this level. See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.
The current access policy setting for the cloud context profile is displayed in the following format:
<inherit setting>(<current access policy>)
For example, if you see this in the **Cloud Access Privilege** for a cloud context profile:
Inherited(Routing & Security)
That means:
- The access policy for this cloud context profile is set to the Routing & Security access policy
 - This access policy was inherited from the parent level (in this case, the account/tenant level), which was also set to the Routing & Security access policy
- Step 14** If you want to change the access policy, click the scroll-down menu in the **Cloud APIC Access Privilege** field and choose one of the access policies to apply at the VPC (cloud context profile) level.
- **Routing & Security:** The default access policy. If you do not assign an access policy to at the VPC level, then the VPC has the Routing & Security access policy applied to it by default.
Assigning a Routing & Security access policy to a VPC means that it has full permissions, where it is able to control routing and security.

- **Routing Only:** Assigning a routing-only access policy at the VPC level means that it can control only the routing policy and the network connectivity.
- **Read Only:** Assigning a read-only access policy at the VPC level means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the VPC (cloud context profile) level are based on the access policy that was assigned at the parent level (in this case, at the account/tenant level). For example, if the access policy at the parent account/tenant level is set to Read Only, then you will only see Read Only as an option at the child VPC (cloud context profile) level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

Step 15

Determine if you want to copy any route tables that are associated with the subnets in the existing VPC that you are importing.

Beginning with release 25.0(4), you can copy route tables that are associated with the subnets in the existing brownfield (unmanaged) VPC that you are importing. See [About Route Table Copying, on page 14](#) for more information.

- If you do not want to copy any route tables that are associated with the subnets in the existing VPC that you are importing, in the **Copy Existing Routing Tables from VPC** area, click **Do Not Copy Existing Routes**, then go to [Step 16, on page 28](#).
- If you want to copy route tables that are associated with the subnets in the existing VPC that you are importing, in the **Copy Existing Routing Tables from VPC** area, click **Copy Existing Routes**.

The **Brownfield Route Tables** fields appear. Follow the steps below to copy the existing route tables from the brownfield VPC.

- Click **Add Brownfield Route Tables**.
The **Select Brownfield Route Tables** page appears, displaying a list of route tables associated with the subnets in the existing brownfield (unmanaged) VPC that you are importing.
- Select the route tables that you want to copy, then click **Select**.

Step 16

In the **Resources to Import** area, select any additional CIDRs available inside the unmanaged VPC that you want to have imported into this unmanaged cloud context profile, if necessary.

The primary CIDR block range in the unmanaged VPC is imported automatically and is tagged as the primary CIDR.

Step 17

In the **Resources to Import** area, select the subnets inside the unmanaged VPC that you want to have imported into this unmanaged cloud context profile.

If you are copying an existing route table from the brownfield VPC, select the necessary subnets that are associated with the route table that you are copying that you want to import. Make sure that all the desired subnets and their associated route tables are selected for import and copy in order to avoid traffic disruption.

Note The subnet associations of the brownfield route tables change when subnets with a Routing & Security or Routing Only access policy are imported into a Cloud APIC, where these subnets are then associated to the Cloud APIC-created route tables.

- Click the box in the **Subnet** column to import the corresponding subnets for an imported CIDR.
- Determine how the current access policy is set at the subnet level.

Beginning with release 25.0(4), additional access policies are available at the subnet level. The access policy is set to Inherit by default, unless you explicitly change the access policy at this level. See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

The current access policy setting for the subnet is displayed in the following format:

`<inherit setting>(<current access policy>)`

For example, if you see this in the **Access Privilege** area for a subnet:

Inherited (Routing & Security)

That means:

- The access policy for this subnet is set to the Routing & Security access policy
- This access policy was inherited from the parent level (in this case, the VPC, or cloud context profile, level), which was also set to the Routing & Security access policy

c) Click the pencil icon next to the entry in the **Subnet** column to change the access policy at the subnet level.

- **Routing & Security:** The default access policy. If you do not assign an access policy to at the subnet level, then the subnet has the Routing & Security access policy applied to it by default.

Assigning a Routing & Security access policy to a subnet means that it has full permissions, where it is able to control routing and security.

- **Routing Only:** Assigning a routing-only access policy at the subnet level means that it can control only the routing policy and the network connectivity.
- **Read Only:** Assigning a read-only access policy at the subnet level means that it does not have write permissions and can only read the inventory.

Keep in mind that the access policies available to you at the subnet level are based on the access policy that was assigned at the parent level (in this case, at the VPC level). For example, if the access policy at the parent VPC level is set to Read Only, then you will only see Read Only as an option at the child subnet level because the access policy at the child level cannot be more restrictive than the access policy at the parent level. See [Updates to Access Policies in Release 25.0\(4\), on page 10](#) for more information.

Step 18 In the **TGW Attachment** field, click the box next to **Enable** to enable AWS Transit Gateway for this unmanaged cloud context profile.

Enabling this field allows you to select the hub network and the transit gateway route table association scope in the next steps. Based on the selections that you make in those steps, the route tables are created on the infra transit gateway. For more information, see the [Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect](#) document.

Step 19 In the **Hub Network** field, select the hub network to associate with this cloud context profile.

You should have created this hub network when you first set up AWS Transit Gateway or AWS Transit Gateway Connect. If you did not create a hub network yet, create the hub network using the procedures provided in [Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect](#).

Step 20 In the **TGW Route Table Association Scope** field, choose from one of the following options.

The following choices are based on the change beginning with release 25.0(2), where the transit gateway route tables are deployed per VRF by default when configuring AWS Transit Gateway. As part of this change, label-based deployments for transit gateway route tables are also available, where, for each new label, a new transit gateway route table that is named after the label will be deployed. For more information, see the "Transit Gateway External Networking" section in the [Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect](#) document.

- **Network Level:** Choose this option if you want to deploy the transit gateway route tables at the network or VRF level.

In the **TGW Route Table Association Label** field, the name for the transit gateway route table is automatically populated using the following format:

<tenantName>-<vrfName>

- **Account Level:** Choose this option if you want to deploy the transit gateway route tables at the account or tenant level.

In the **TGW Route Table Association Label** field, the name for the transit gateway route table is automatically populated using the following format:

<tenantName>

- **Label Based:** Choose this option if you want to use the custom label for the deployment of the transit gateway route table, where the VPC is associated with the transit gateway route table that is deployed based on this custom label.

In the **Custom Label** area, click **Select Custom Label**, then select the custom label that you want to use for the deployment of the transit gateway route table.

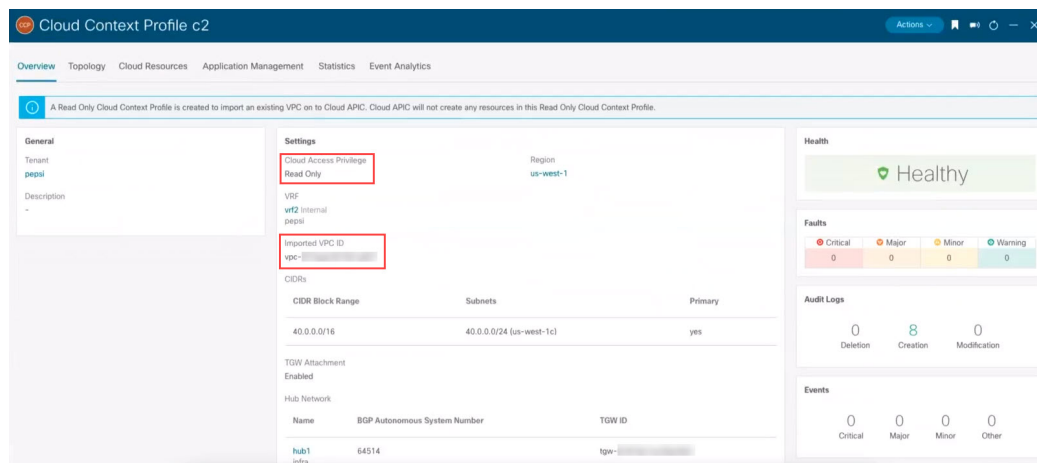
Step 21 Click **Save** in the **Import Brownfield VPC** window to save this cloud context profile.

A **What's Next** page is displayed.

Step 22 Click **Go to Cloud Context Profile Details** at the bottom right of the window.

The details screen for the cloud context profile that you just created is displayed.

The following figure shows a configured unmanaged cloud context profile, with the Read Only flag enabled and the associated VPC ID.



Step 23 In the Cisco Cloud APIC GUI, in the left nav bar, click **Application Management > VRFs**.

A list of configure VRFs appears.

Step 24 Locate the VRF that you created earlier in these procedures that would be associated with the cloud context profile for the brownfield VPC and click that VRF.

Verify that the VRF is associated with the imported brownfield VPC.

What to do next

Configure the AWS transit gateway attachment between the unmanaged (brownfield) VPC and the infra transit gateway in AWS using the procedures provided in [Adding the Transit Gateway Attachment for an Unmanaged VPC in AWS, on page 32](#).

Creating an Unmanaged (Brownfield) Cloud Context Profile Using the REST API

Before you begin



Note The information in this section is applicable if you are running on a release prior to release 25.0(4). For equivalent information for release 25.0(4) and later, including how to configure new access policies that are available beginning with release 25.0(4) see [Configuring Access Policies Using the REST API, on page 22](#).

Review the information provided in [About Unmanaged \(Brownfield\) Cloud Context Profiles, on page 25](#) before going through these procedures.

Procedure

To create an unmanaged (brownfield) cloud context profile, post the following.

The areas below show the lines that are used when creating an unmanaged cloud context profile, where:

- The `cloudRsCtxProfileToAccessPolicy` line sets the cloud context profile to be read-only.
- The `cloudBrownfield` and `cloudIDMapping` lines are used to import a brownfield VPC, using the VPC ID of the brownfield VPC in the AWS cloud.
- The `cloudRsCtxProfileToRegion` line points to the region where the VPC exists in the AWS cloud.
- The `cloudCidr` lines are one or more CIDRs (one of which is the primary CIDR) that match the CIDRs in the AWS cloud.

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml
<fvTenant name="unmanagedTenant1">
  <fvCtx name="vrf1" />
    <cloudCtxProfile name="BrownfieldCtxProfile1">
      <cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only"/>
      <cloudRsCtxProfileToRegion tDn="uni/cloudcomp/provp-aws/region-us-west-1"/>
      <cloudRsToCtx tnFvCtxName="vrf1" />
      <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default-foo"
label="system=='vrf'"/>
      <cloudBrownfield status="">
      <cloudIDMapping cloudProviderId="vpc-0fe1afe17568417c8"/>
    </cloudBrownfield>
      <cloudCidr name="cidr1" addr="40.0.0.0/16" primary="yes" />
    </cloudCtxProfile>
  </fvTenant>
```

What to do next

Create an EPG to be associated with the brownfield cloud context profile using the information provided in [Creating an EPG Associated With the Brownfield Cloud Context Profile, on page 33](#).

Adding the Transit Gateway Attachment for an Unmanaged VPC in AWS

In this task, you will be configuring the AWS transit gateway attachment between the unmanaged (brownfield) VPC and the infra transit gateway in AWS, as described in [About Transit Gateway Attachments for Unmanaged \(Brownfield\) VPCs, on page 5](#).

As described in [What Cisco Cloud APIC Does and Does Not Do With Brownfield VPCs, on page 6](#) and [About Transit Gateway Attachments for Unmanaged \(Brownfield\) VPCs, on page 5](#), Cisco Cloud APIC does not configure the AWS transit gateway attachment between the unmanaged (brownfield) VPC and the infra transit gateway in AWS. The AWS transit gateway that is created by Cisco Cloud APIC as part of the infra configuration is shared with the brownfield AWS user account, but you must manually create the transit gateway VPC attachment with the shared infra transit gateways for all of the brownfield VPCs that you imported into Cisco Cloud APIC.

Before you begin

Complete the procedures provided in [Creating an Unmanaged \(Brownfield\) Cloud Context Profile, on page 25](#) before beginning these procedures. At the end of those procedures, the Cisco Cloud APIC will have configured the transit gateway VPC attachment with all the infra transit gateways.

Procedure

- Step 1** In the AWS portal, navigate to the **Transit Gateway Attachments** page.
The **Transit gateway attachments** page is displayed.
- Step 2** Click **Create transit gateway attachment**.
The **Create transit gateway attachment** page is displayed.
- Step 3** In the **Details** area, enter the necessary information for the transit gateway attachment that you are creating.
- In the **Name tag** field, enter a name tag for this transit gateway attachment.
 - In the **Transit gateway ID** field, select the AWS transit gateway that was created as part of the greenfield VPC configuration that was shared with the brownfield user account.
 - In the **Attachment type** field, select **VPC**.
- Step 4** In the **VPC attachment** area, enter the necessary information for the transit gateway attachment that you are creating.
- Leave the **DNS support** field selected and **IPv6 support** field unselected.
 - In the **VPC ID** field, select the brownfield VPC ID.
- Step 5** Leave the default entries for the remaining fields as-is and click **Create transit gateway attachment**.
-

What to do next

Create an EPG to be associated with the brownfield cloud context profile using the information provided in [Creating an EPG Associated With the Brownfield Cloud Context Profile, on page 33](#).

Creating an EPG Associated With the Brownfield Cloud Context Profile

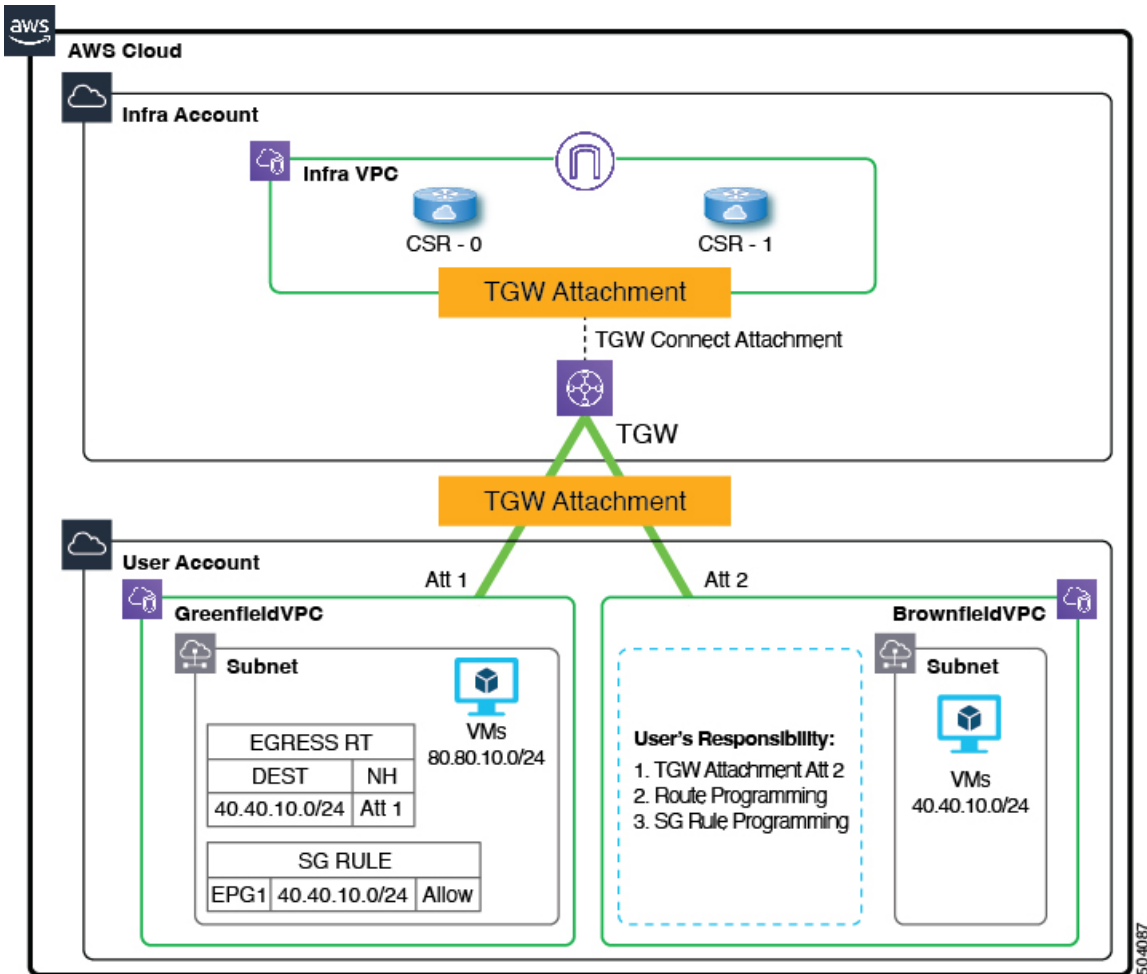
The following topics provide information on creating an EPG associated with the brownfield cloud context profile.

How EPGs are Associated With Brownfield Cloud Context Profiles Through VRFs

In order to better understand how EPGs are associated with brownfield cloud context profiles through VRFs, it's helpful to compare it to how EPGs are mapped normally:

- **Regular EPG mapping:** Typically, when you define a regular cloud EPG, you associate the cloud EPG with a VRF. The cloud context profile also gets associated with the VRF as part of this process. Thus, when an EPG is defined, it gets translated into the appropriate security group under each and every cloud context profile (VPC) associated with this VRF, which then gets converted into security group rules in the AWS cloud.
- **EPGs associated with brownfield cloud context profiles:** When an unmanaged (brownfield) cloud context profile is defined and associated with a VRF, and when you define an EPG that is associated with this same VRF, then this EPG can be referred to as an **EPG associated with a brownfield cloud context profile**. The reason for creating an EPG associated with a brownfield cloud context profile is to orchestrate all the networking and security constructs on the greenfield VPC to allow the communication to the brownfield VPC, because everything in the Cisco Cloud APIC, such as security and routing, depends on EPG contracts.

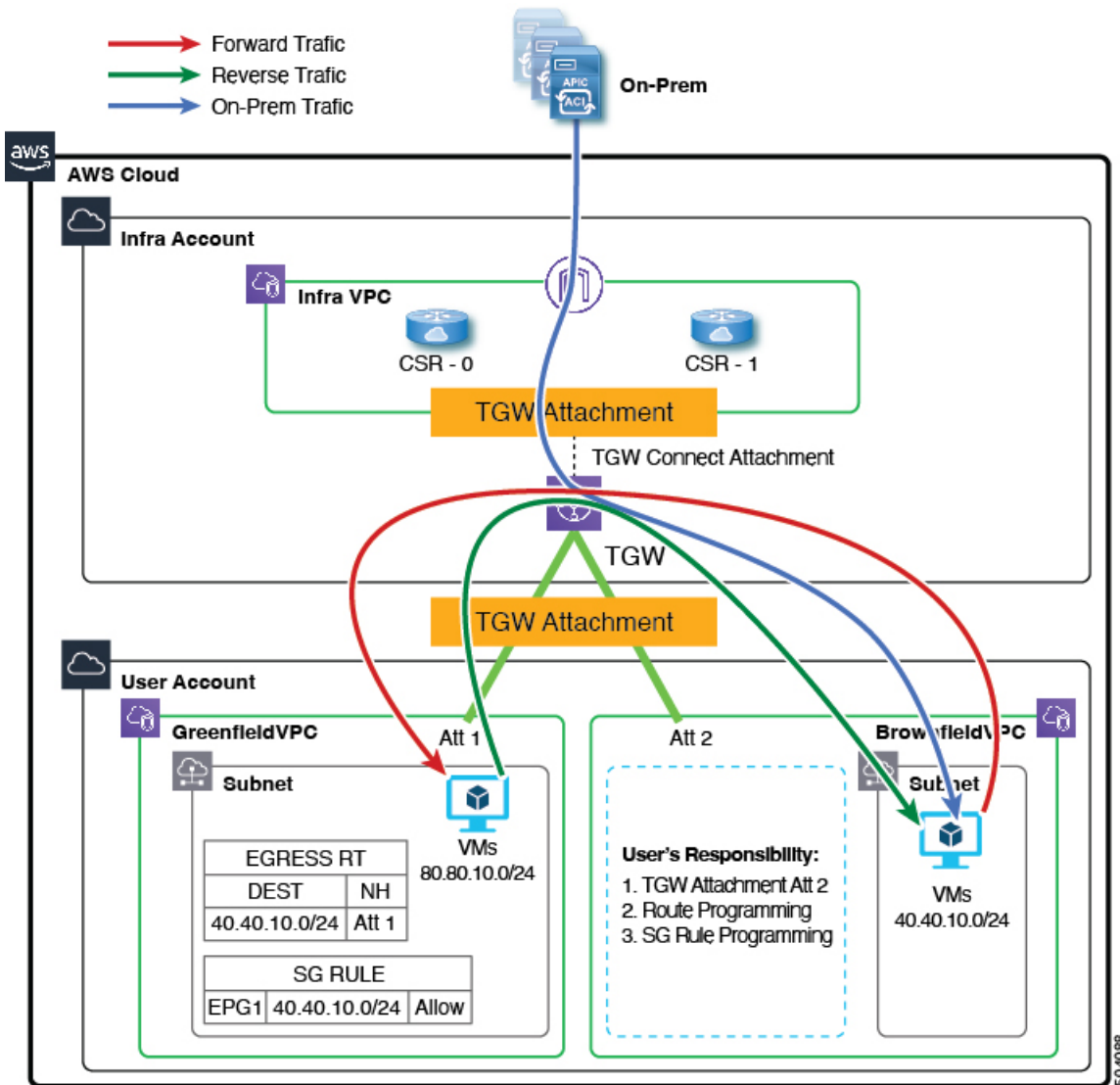
For example, consider the configuration in the following figure:



In this configuration, the reason for creating the EPG that is associated with the brownfield cloud context profile and creating a contract is to provision the routing and security on the greenfield VPC side to allow the traffic to reach this unmanaged (brownfield) VPC.

- The programming of the route table entries and security group rules, and the creation of the transit gateway attachment for the **greenfield** VPC (Att 1 in the example illustration) are all done by Cisco Cloud APIC.
- However, for the **brownfield** VPC, Cisco Cloud APIC does not program the route table entries and security group rules, nor does Cisco Cloud APIC create the transit gateway attachment for the brownfield VPC. You are therefore responsible for making these configurations manually for the brownfield VPC.
- Cisco Cloud APIC does program the CSR to allow routing between the greenfield and brownfield VPCs.

In this example, the goal is to allow a packet flow on the greenfield VPC to send and receive the packets to 40.40.10.0/24 (security group rules) and to send the traffic destined to this subnet to the infra transit gateway and then program the CSR to send the packet to the brownfield VPCs. All of this is achieved using contracts.



Cisco Cloud APIC does not program the route entries or the security group rules on the brownfield VPC side. Instead, Cisco Cloud APIC programs only the greenfield VPC side to send packets to or receive packets from the brownfield VPC subnets, based on the contracts. Cisco Cloud APIC programs the CSR accordingly to make the routing occur between the greenfield VPC and the brownfield VPC.

This is why you create EPGs associated with the brownfield cloud context profiles, so that the other greenfield VPCs can send and receive traffic to and from these brownfield VPCs.

Note that EPGs associated with the brownfield cloud context profiles should only have subnet-based or exact IP-based endpoint selectors and not tag-based endpoint selectors. Cisco Cloud APIC won't recognize endpoints belonging to an unmanaged VPC. Because of this, Cisco Cloud APIC won't recognize tag-based endpoints belonging to an unmanaged (brownfield) VPC. If Cisco Cloud APIC can't detect the endpoints, then it can't find the IP addresses and therefore can't program the security rules on the greenfield VPC side to send/receive the packets to and from the brownfield VPC side.

The reason to create an EPG that is associated with the brownfield cloud context profile and then define a subnet-based or specific IP-based endpoint selector in that EPG is:

- When you create a contract from this EPG (associated with the brownfield cloud context profile) to another EPG (associated to the greenfield cloud context profile), this drives the programming of the route entries to the unmanaged VPC CIDRs in the route table on the greenfield VPC side.
- This also drives the programming of all the security group rules on the greenfield VPC side to allow the packets to be sent to or received from these subnets defined on the EPG's endpoint selector.
- If an EPG is configured with tag-based endpoint selectors and is associated with the brownfield cloud context profile, then a fault will be raised saying that this EPG cannot be used.

Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VRF]-addr-[redacted]/16/sgroup-[uni/fn-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudScaleSetNicGroup	Tag-Based EpSelector custom:tag=devmgr is not applicable on the EPG uni/fn-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile uni/fn-Dev-Tenant/ctxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VRF]-addr-[redacted]/16/sgroup-[uni/fn-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudEndPoint	Tag-Based EpSelector custom:tag=devmgr is not applicable on the EPG uni/fn-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile uni/fn-Dev-Tenant/ctxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00

Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI

In this topic, you will be creating an EPG that is associated with the brownfield cloud context profile. For a better understanding of why you need to do this, see [How EPGs are Associated With Brownfield Cloud Context Profiles Through VRFs, on page 33](#).

Before you begin

Verify that you have completed all of the previous necessary configurations before going through these procedures, including:

- [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI, on page 25](#)

Procedure

- Step 1** Click the **Intent** icon.
The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Create EPG**.
The **Create EPG** dialog box appears.
- Step 4** Enter the necessary general configurations for the EPG.

Table 3: Create EPG Dialog Box Fields

Properties	Description
General	
Name	Enter the name of the EPG that will be associated with the brownfield cloud context profile.

Properties	Description
Tenant	To choose a tenant: <ol style="list-style-type: none"> 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. Select the tenant that is associated with the unmanaged (brownfield) VPC. c. Click Select. You return to the Create EPG dialog box.
Application Profile	To choose an application profile: <ol style="list-style-type: none"> a. Click Select Application Profile. The Select Application Profile dialog box appears. b. From the Select Application Profile dialog, click to choose an application profile in the left column. c. Click Select. You return to the Create EPG dialog box.
Description	Enter a description of the EPG.
Settings	
Type	Choose Application as the EPG type.
VRF	To choose a VRF: <ol style="list-style-type: none"> a. Click Select VRF. The Select VRF dialog box appears. b. From the Select VRF dialog, click to choose a VRF in the left column. Choose the VRF that is associated with the brownfield cloud context profile. c. Click Select. You return to the Create EPG dialog box.
Route Reachability	Leave the default Internet option selected for the route reachability.

Properties	Description
Endpoint Selectors	<p>Define the subnet-based or specific IP-based endpoint selector corresponding to the AWS brownfield site.</p> <p>For more information, see How EPGs are Associated With Brownfield Cloud Context Profiles Through VRFs, on page 33.</p> <ol style="list-style-type: none"> a. Click Add Endpoint Selector to add an endpoint selector. b. Enter a name in the Name field. c. Enter the following information in the Match Expressions area: <ul style="list-style-type: none"> • Key: Choose IP. • Operator: Choose equals (==). • Value: Enter the appropriate subnet-based or specific IP-based IP endpoint. <p>For example, this could be the Private IP address for the virtual machine in the resource group for the brownfield VPC that you want to import into Cloud APIC.</p> d. Click the checkmark to accept these values for this match expression. e. Click Add to add this endpoint selector. f. Click Add Endpoint Selector again to add additional endpoint selectors, if necessary.

Step 5 Click **Save** to save this EPG.

What to do next

Configure a contract between the EPGs using the procedures provided in [Creating a Contract Between the EPGs Using the GUI, on page 38](#).

Creating a Contract Between the EPGs Using the GUI

In this topic, you will be creating a contract to be used from the external EPG associated with the brownfield cloud context profile to the EPG associated with the greenfield cloud context profile. This is done to drive the programming of the route entries to the unmanaged VPC CIDRs in the route table in the greenfield VPC side. This also drives the programming of all the security group rules on the greenfield VPC side to allow the packets to be sent to or received from these subnets defined on the EPG's endpoint selector.

Before you begin

Create an external EPG associated with the brownfield cloud context profile using the instructions provided in [Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI, on page 36](#).

Procedure

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Application Management**.

A list of **Application Management** options appear in the **Intent** menu.

Step 3 From the **Application Management** list in the **Intent** menu, click **Create Contract**. The **Create Contract** dialog box appears.

Step 4 Enter the appropriate values in each field as listed in the following *Create Contract Dialog Box Fields* table then continue.

Table 4: Create Contract Dialog Box Fields

Properties	Description
Name	Enter the name of the contract.
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. Select the tenant that is associated with the unmanaged (brownfield) VPC. c. Click Select . You return to the Create Contract dialog box.
Description	Enter a description of the contract.
Settings	
Scope	Choose the appropriate scope for the tenant. <ul style="list-style-type: none">• To enable EPGs in one tenant to communicate with EPGs in another tenant, choose Global scope.• To enable an EPG in one VRF to communicate with another EPG in a different VRF, choose Global or Tenant scope.
Add Filter	To choose a filter: a. Click Add Filter . The filter row appears with a Select Filter option. b. Click Select Filter . The Select Filter dialog box appears. c. From the Select Filter dialog, click to choose a filter in the left column then click Select , or click Create Filter to create a new filter, if necessary. For more information on filters, see the Cloud APIC for AWS User Guide . You return to the Create Contract dialog box.

Step 5 Click **Save** when finished.

A **What's Next** window is displayed.

Step 6 Click **Go to Details** in the lower right corner of the window.

The details window for the contract is displayed.

- Step 7** Click **Actions > EPG Communication**.
The **EPG Communication Configuration** window appears.
- Step 8** In the **Consumer EPGs** area on the left side, click **Add Consumer EPGs**.
The **Select Consumer EPGs** window appears.
- Step 9** Choose the EPGs associated with the greenfield and brownfield cloud context profiles and click **Select**.
For example:
- If you had created `epg1` previously for the greenfield EPG
 - And you created `epg2` for the brownfield EPG using the procedures in [Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI, on page 36](#)
- Then you would select both `epg1` (greenfield EPG) and `epg2` (brownfield EPG) in the **Select Consumer EPGs** window.
- Step 10** Click **Select**.
You are returned to the **EPG Communication Configuration** window.
- Step 11** In the **Provider EPGs** area on the right side, click **Add Provider EPGs**.
The **Select Provider EPGs** window appears.
- Step 12** Again, choose the EPGs associated with the greenfield and brownfield cloud context profiles.
Using the examples provided for the consumer EPGs step, you would select the same EPGs (the greenfield EPG `epg1` and the brownfield EPG `epg2`) in the **Select Provider EPGs** window.
- Step 13** Click **Select**.
You are returned to the **EPG Communication Configuration** window.
- Step 14** Click **Save**.
-

What to do next

Complete the remaining configuration tasks in AWS using the procedures provided in [Completing the Remaining Configurations for the Brownfield VPC in AWS, on page 41](#).

Creating an EPG Associated With the Brownfield Cloud Context Profile Using the REST API

Procedure

Create a cloud EPG for the brownfield VPC.

You will be creating a cloud EPG to allow an on-premises site or another cloud site to be able to send or receive the traffic to this unmanaged brownfield VPC.

Note The endpoint selectors for these brownfield cloud EPGs must be subnet- or IP-based., not tag-based.

```
<fvTenant name="unmanagedTenant1">  
  <fvCtx name="vrf1" />  
    <cloudCtxProfile name="BrownfieldCtxProfile1">
```



```

<cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only"/>
<cloudRsCtxProfileToRegion tDn="uni/cloudcomp/provp-aws/region-us-west-1"/>
<cloudRsToCtx tnFvCtxName="vrf1" />
<cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default-foo"
label="system=='vrf'"/>
  <cloudBrownfield status="">
    <cloudIDMapping cloudProviderId="vpc-0fe1afe17568417c8"/>
  </cloudBrownfield>
  <cloudCidr name="cidr1" addr="40.0.0.0/16" primary="yes" />
</cloudCtxProfile>
</fvTenant>

```

Note that in this example, the EPG is associated with the brownfield cloud context profile through the VRF vrf1 as shown in the following post:

```

<fvTenant name="unmanagedTenant1">
  <fvCtx name="vrf1" />
  <cloudApp name="ap3">
    <cloudEPg name="epg3">
      <cloudRsCloudEPgCtx tnFvCtxName="vrf1"/>
      <fvRsProv tnVzBrCPName="contract4"/>
      <cloudEPSelector name="EP_SEL1" matchExpression="IP=='40.0.0.0/24'" status="" />
    </cloudEPg>
  </cloudApp>
</fvTenant>

```

Completing the Remaining Configurations for the Brownfield VPC in AWS

In these procedures, you will complete these remaining configurations in AWS. The following section provides the general instructions and example configurations to complete these remaining configurations in AWS, but keep in mind that your configuration might be different.

Before you begin

Verify that you have completed all of the previous necessary configurations before going through these procedures, including:

- [Creating an Unmanaged \(Brownfield\) Cloud Context Profile Using the GUI, on page 25](#)
- [Creating an EPG Associated With the Brownfield Cloud Context Profile Using the GUI, on page 36](#)
- [Creating a Contract Between the EPGs Using the GUI, on page 38](#)

Procedure

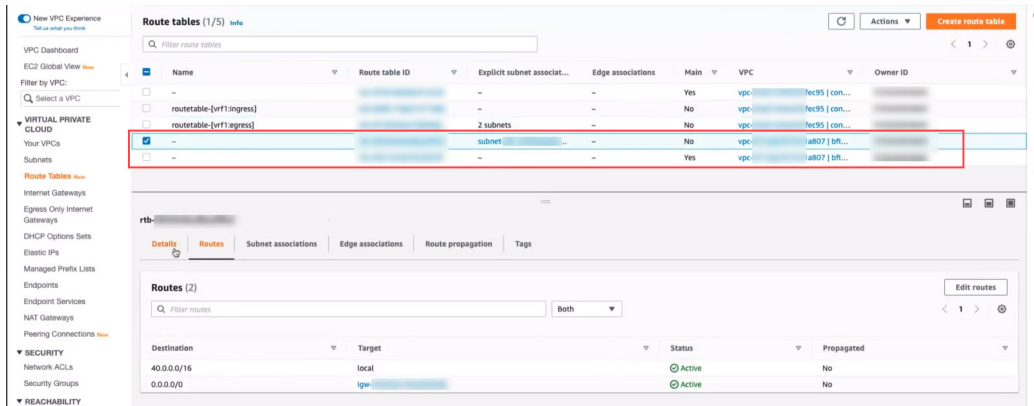
Step 1 In the AWS portal, navigate to the **Route Tables** page.

The **Route tables** page is displayed, which shows all of the already-configured route tables.

Step 2 Locate the two route tables that were created for the brownfield VPC.

Look for the entries with the VPC ID for the brownfield VPC in the **VPC** column to find the two route tables that were created for the brownfield VPC.

For example, if you know that the VPC ID for your brownfield VPC ends in `...a807`, locate the two route tables that have that VPC ID in the **VPC** column, as shown in the following graphic.



Step 3 Determine which of the two route tables is the route table for the subnets.

You will need to select the subnet route table to edit routes. The subnet route table can be located using the following identifiers:

- The `Explicit subnet associations` column has the entry `subnet`
- The `Main` column has the entry `No`

Step 4 Click the box next to the route table for the subnets to select that brownfield route table, then click **Edit routes**. The **Edit routes** window appears.

Step 5 Click **Add routes**.

A new row for the additional route appears.

Step 6 In the **Destination** field, enter the CIDR for the transit gateway.

Step 7 In the **Target** field, select **Transit Gateway**.

The transit gateway attachment that you created earlier is automatically loaded. This is the transit gateway attachment that was created by Cisco Cloud APIC between the brownfield (unmanaged) VPC and the infra transit gateway as part of the process in the [Creating an Unmanaged \(Brownfield\) Cloud Context Profile, on page 25](#).

Step 8 Click **Save changes**.

A details window for this route table appears.

Step 9 Verify that the new route is available through the transit gateway.

a) In the AWS portal, navigate to the **Transit Gateway Route Tables** page.

The **Transit gateway route tables** page is displayed, which shows all of the configured route tables for the transit gateway. Two of the route tables should be associated with two VRFs, where one route table is associated with the VRF for the greenfield VPC and the other route table is associated with the VRF for the brownfield VPC.

b) Click on the box to the left of the first of those two VRF-related route tables.

The details pane for this route table is displayed.

c) Click on the **Routes** tab and verify that the entry in the **CIDR** column that matches the entry that you used in [Step 6, on page 42](#) is shown with an `Active` state in the **Route state** column.

d) Repeat these steps for the second of the two VRF-related route tables and verify that same entry in the **CIDR** column is shown with an `Active` state in the **Route state** column for the second VRF-related route table.

Step 10

Configure the security group rules programming for the brownfield VPC.

Cisco Cloud APIC does not configure the security group rules programming for the brownfield VPC, so you must manually make these configurations yourself through the AWS portal.

Refer to the following AWS article for information that you can use to configure the security group rules programming for the brownfield VPC:

[Security groups for your VPC](#)

Following are example configurations that show how you can configure security group rules programming for the brownfield VPC, where you could spawn a new endpoint or you can apply a security group to an existing endpoint.

For example, if you were to spawn a new endpoint:

- a) In the AWS portal, locate and start the **Launch Instance Wizard**.
- b) Navigate through the **Choose AMI** and **Choose Instance Type** windows in the **Launch Instance Wizard**, until you are at the **Configure Instance Details** window.
- c) In the **Network** field in the **Configure Instance Details** window, select the brownfield VPC.
- d) Complete the remaining configurations in the **Configure Instance Details** based on your setup, then click **Next: Add Storage**.
- e) Navigate through the screens **Add Storage** and **Add Tags** windows, until you are at the **Configure Security Group** window.
- f) Manually add the security group rules in the **Configure Security Group** window.

Click **Add Rule** to add the appropriate security group rules for your setup.

The **Inbound rules** will contain the greenfield CIDR.

- g) When you have finished adding the security group rules, click **Review and Launch**.
- h) Verify the information in the **Review and Launch** window, then click **Launch**.

Complete any remaining configurations based on the security group rules that you configured.

As another example, assume you have an existing endpoint:

- a) In the AWS portal, under **Network & Security**, locate and click **Security Groups**.
 - b) Click **Create security group**.
 - c) Enter the necessary information in the **Create security group** window.
 - In the **VPC** field, select the brownfield VPC.
 - Click **Add Rule** under the **Inbound rules** and **Outbound rules** areas in this window to add the appropriate security group rules for your setup.

The **Inbound rules** will contain the greenfield CIDR.
 - d) Click **Create security group** at the bottom of the page when you have finished adding the necessary security group rules.
 - e) Navigate to the **Instances** page.
 - f) Select the endpoint and click **Actions > Security > Change security groups**.
 - g) In the **Change security groups** window, add the security group that you just created and click **Save**.
-

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, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

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](http://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.