

# Cloud OnRamp for IaaS


- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, on page 1
- Overview, on page 2
- Supported Cisco Cloud Service Providers and Supported Cisco Catalyst SD-WAN Cloud Devices, on page 4
- Prerequisites of Cisco Catalyst SD-WAN Cloud Devices, on page 4
- AWS Prerequisite, on page 7
- Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS, on page 8
- Manage Host and Transit VPCs, on page 13
- Microsoft Azure Prerequisites, on page 18
- Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure, on page 21
- Manage Host and Transit VNets, on page 25
- Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, on page 27
- Sample Feature Template Settings , on page 30
- Sample Device Template Variable Values, on page 36
- Example for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, on page 36


# Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

***Table 1: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Azure Government Cloud Support for Cisco IOS XE Catalyst SD-WAN Devices | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a<br>Cisco vManage Release 20.4.1 | This feature allows you to configure the Cisco Catalyst 8000V devices on Microsoft Azure Government Cloud. With these cloud devices now supported on Microsoft Azure Government Cloud, Government Cloud customers can use the same advanced routing and security benefits, which are already available on Azure public cloud. |

| Feature Name | Release Information | Description |
|---|---|---|
| AWS Government Cloud Support for Cisco IOS XE Catalyst SD-WAN Devices | Cisco IOS XE Catalyst SD-WAN Release 17.3.1a<br>Cisco vManage Release 20.3.1 | This feature allows you to configure Cisco CSR1000V on Amazon Web Services (AWS) Government Cloud. With Cisco CSR1000V now supported on AWS Government Cloud, Government Cloud customers can move sensitive workloads into the cloud and manage the data securely by using all routing benefits. |
| | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a<br>Cisco vManage Release 20.4.1 | Starting from this release, Cisco Catalyst 8000V devices are supported on AWS Government Cloud. |

# Overview

**Note** Beginning with Cisco vManage Release 20.9.1, we recommend setting up your cloud infrastructure using Cloud OnRamp for Multicloud. Cloud OnRamp for IaaS will be phased out in a future release.

Cisco Catalyst SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS) extends the fabric of Cisco Catalyst SD-WAN overlay network to public cloud instances. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS allows branches with Cisco Cloud Services Router 1000V Series and Cisco Catalyst 8000V devices to connect directly to public-cloud application providers. By eliminating the need for a physical data center, Cisco Catalyst SD-WAN Cloud OnRamp for IaaS improves the performance of SaaS applications.

To know more about Cisco Catalyst 8000V devices, see the Cisco Catalyst 8000V Edge Software Configuration Guide.

The connection between the overlay network and a public-cloud application is provided by one to four pairs of redundant Cisco Catalyst SD-WAN cloud devices. These devices act together as a transit between the overlay network and an application. By using redundant devices to form the transit, Cisco Catalyst SD-WAN Cloud OnRamp for IaaS offers path resiliency to the public cloud. In addition, having redundant routers helps in brownout protection to improve the availability of public-cloud applications. Together, the two routers can remediate link degradation that might occur during brownouts. You can configure these devices as part of the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow.

With Cisco Catalyst SD-WAN Cloud OnRamp for IaaS support on Amazon Web Services (AWS) and Microsoft Azure government cloud (GovCloud), you can configure Cisco CSR1000V and Cisco Catalyst 8000V devices to host sensitive data. AWS or Microsoft Azure GovCloud (US) are isolated AWS or Azure regions that allow the U.S. government agencies and customers to move sensitive workloads into the government cloud. The customers can use these devices that provide routing capabilities and support full path encryption with powerful cipher suites. The regions that you can choose during Cisco Catalyst SD-WAN Cloud OnRamp for IaaS configuration are related to the AWS or Microsoft Azure GovCloud specifications. See AWS GovCloud documentation and Microsoft Azure GovCloud documentation for details on setting up your GovCloud (US) account.

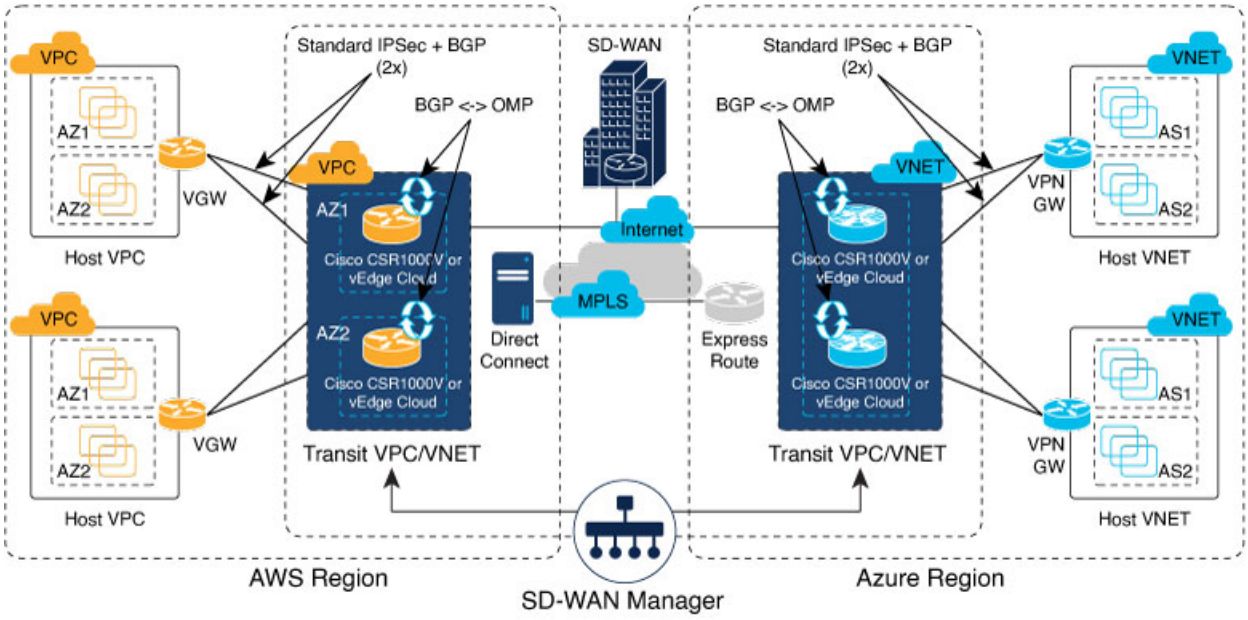
The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS works along with AWS Virtual Private Cloud (VPC) and Azure Virtual Network (VNet).

The key steps to deploy a Cisco Catalyst SD-WAN Cloud OnRamp for IaaS solution are:

1. Identify one to four pairs of unused Cisco Catalyst SD-WAN cloud devices in Cisco SD-WAN Manager that you can use forCisco Catalyst SD-WAN Cloud OnRamp for IaaS.
2. Configure and attach a basic device template to both the Cisco Catalyst SD-WAN cloud devices.
3. Enter AWS or Azure API credentials (access key and secret key) when configuring using Cisco SD-WAN Manager.
4. Add the transit Virtual Private Cloud (VPC) or transit Virtual Network (VNet) configuration.
5. Discover and map host VPCs or host VNets to the transit VPC or transit VNet.

The following image shows the topology of Cisco Catalyst SD-WAN Cloud OnRamp for IaaSwith AWS and Microsoft Azure integrated. You can apply the same policy, security, and other Cisco Catalyst SD-WAN policies everywhere with Cisco SD-WAN Manager as a single server for all the Cisco Catalyst SD-WAN devices, which are on-premises and on multiple clouds. The infrastructure on AWS and Microsoft Azure can be seamlessly integrated into the Cisco Catalyst SD-WAN fabric. The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow automates all steps, and the Cisco SD-WAN Manager server builds the whole solution within minutes.

***Figure 1: Cisco Catalyst SD-WAN Cloud OnRamp for IaaS Topology***



# Supported Cisco Cloud Service Providers and Supported Cisco Catalyst SD-WAN Cloud Devices

The following IaaS public cloud providers are supported with Cisco Catalyst SD-WAN Cloud OnRamp for IaaS:

- Amazon AWS
- Microsoft Azure

The following devices are supported:

- Cisco Cloud Services Router 1000V Series (Cisco CSR1000V)
- Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V)



**Note** From Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco Catalyst 8000V replaces Cisco CSR1000V. Therefore, Azure Government Cloud support is only available for Cisco Catalyst 8000V, and we recommend that you use Cisco Catalyst 8000V devices.

In this document, the supported devices are collectively referred to as Cisco Catalyst SD-WAN cloud devices.

# Prerequisites of Cisco Catalyst SD-WAN Cloud Devices

Before you can configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, ensure that the following device requirements are met.

- Verify you have available tokens or licenses for at least two Cisco CSR1000V or Cisco Catalyst 8000V devices in Cisco SD-WAN Manager. See Verify Presence of Cisco Catalyst SD-WAN Cloud Devices in Cisco SD-WAN Manager, on page 5.
- Configure feature and device templates for the Cisco CSR1000V or Cisco Catalyst 8000V devices that you'll use within the transit VPCs or VNets during configuration. See Configure Device Template for Cisco Catalyst SD-WAN Cloud Devices, on page 6.
- Attach the device template to the software tokens representing the Cisco CSR1000V or Cisco Catalyst 8000V devices that you'll use within the transit VPCs or VNets. See Attach a Device Template to Cisco Catalyst SD-WAN Cloud Devices, on page 6.

## Provision Cisco SD-WAN Manager Server

Before you can configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, provision the Cisco SD-WAN Manager server.

1. Ensure that your Cisco SD-WAN Manager server can access the Internet, and you configure the DNS server so that it can reach AWS or Microsoft Azure. To configure a DNS server, in the Cisco SD-WAN

Manager VPN feature configuration template, enter the IP address of a DNS server. Next, reattach the configuration template to the VPN feature using Cisco SD-WAN Manager.

2. Ensure that you add at least two Cisco Catalyst SD-WAN cloud devices to the Cisco SD-WAN Manager server to bring up Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. Attach these two Cisco Catalyst SD-WAN cloud devices to the appropriate configuration template. Ensure that the configuration for these devices include the following attributes:
   - Hostname
   - IP address of Cisco Catalyst SD-WAN Validator
   - Site ID
   - Organization name
   - Tunnel interface configuration on the eth1 interface

     In Cisco CSR1000V or Cisco Catalyst 8000V devices, the tunnel interface is on the GigabitEthernet2 interface.

3. Ensure that you synchronize the Cisco SD-WAN Manager server with the current time. To check the current time, click the **Help (?)** icon at the top bar of the Cisco SD-WAN Manager screen. The **Timestamp** field shows the current time. If the time isn't correct, configure the Cisco SD-WAN Manager server time to point to an NTP time server, such as the Google NTP server. To configure the server time, in the Cisco SD-WAN Manager NTP feature configuration template, enter the hostname of an NTP server. Next, reattach the configuration template to the NTP feature using Cisco SD-WAN Manager. The Google NTP servers are time.google.com, time2.google.com, time3.google.com, and time4.google.com, and so on.

# Verify Presence of Cisco Catalyst SD-WAN Cloud Devices in Cisco SD-WAN Manager

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

**Step 2** On the Device listing page, verify that there are at least two valid Cisco CSR1000V or Cisco Catalyst 8000V devices, which aren't used already.

The valid unused devices are:

- The devices that have the word, "valid"under the **Validity** column.
- The devices that have the **Assigned Template**, **Device Status**, **Hostname**, **System IP**, and **Site ID** columns blank.

Go to software.cisco.com, and use the Plug and Play Connect portal to add tokens or licenses if you have insufficient Cisco CSR1000V or Cisco Catalyst 8000V devices.

# Configure Device Template for Cisco Catalyst SD-WAN Cloud Devices

Ensure that you have at least a minimal device template assigned within Cisco SD-WAN Manager to the two Cisco CSR1000V or Cisco Catalyst 8000V devices. A minimal device template is the one that uses factory default feature templates within the device template. You need at least one service VPN and the management (VPN 512) interface configured within the device template. However, we recommend that you configure a fully functional device template that includes settings specific to your deployment within custom feature templates. See Configure the Cisco SD-WAN Routers for step-by-step instructions on how to create individual feature templates and device templates using Cisco SD-WAN Manager.

Ensure that you don't modify the feature templates after these templates have been attached to the device templates and configured using the Cloud onRamp for IaaS. The Cloud onRamp for IaaS configuration overwrites these feature templates configuration that is modified.

A sample device template, and the various feature templates which make up the device template, is available in Sample Feature Template Settings topic that you can use for Cisco CSR1000V or Cisco Catalyst 8000V devices.

# Attach a Device Template to Cisco Catalyst SD-WAN Cloud Devices

When you attach a device template to the Cisco CSR1000V or Cisco Catalyst 8000V devices, Cisco SD-WAN Manager builds the configurations based on the feature templates and then saves the configurations to the designated , Cisco CSR1000V or Cisco Catalyst 8000V devices. Before you can build and save the configurations, define all variables within the feature templates attached to the device template.

To enter values of the variables manually using Cisco SD-WAN Manager, instead of uploading a .csv file:

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

**Note**
In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

**Step 2** For the desired device template, click **…** and choose **Attach Devices**.

A pop-up window listing the available devices to be attached to this configuration appear. The list of available devices contains either:

- The hostname and IP address of a device if it’s known using Cisco SD-WAN Manager.
- The chassis serial number of the devices that aren't available on the network and aren’t known to Cisco SD-WAN Manager.

Cisco CSR1000V or Cisco Catalyst 8000V devices are assigned a chassis serial number although there’s no physical chassis. The list contains only the device model that was defined when the device template was created.

**Step 3** To apply the configuration template, choose one or more devices from **Available Devices** and move them to **Selected Devices**.

**Note**
In this document, we’re using two Cisco Catalyst SD-WAN cloud devices on which you apply the configurations.

**Step 4** Click **Attach**.

The window that appears, lists the Cisco Catalyst SD-WAN cloud devices that you had chosen.

**Step 5** For the first Cisco CSR1000V or Cisco Catalyst 8000V devices, click **…** and choose **Edit Device Template**.

A pop-up window appears with a list of variables and empty text boxes. There can be variables with check boxes to check and uncheck for on and off values. Make sure that you fill all text boxes. You can use the sample information available in the Sample Device Template Variable Values, on page 36 topic to fill in the variable values.

**Step 6** Click **Update**.

**Step 7** Repeat Steps 5–6 for the second Cisco CSR1000V or Cisco Catalyst 8000V devices.

You can download the variable values into the .csv file for future use.

**Step 8** Click **Next**.

The window indicates that the configure action is applied to the two devices, which are attached to one device template.

You can select a device from the left pane to view the configuration that is saved on the Cisco Catalyst SD-WAN cloud device.

**Step 9** Click **Configure Devices**.

**Step 10** In the pop-up window that appears, check **Confirm configuration changes on 2 devices**.

**Step 11** Click **OK**.

The **Task View** window appears.

After some time, the status of the two Cisco CSR1000V or Cisco Catalyst 8000V devices appears as **Done – Scheduled** with a message indicating that the device is offline and that the template will be attached to the device when it's online.

### What to do next

You can now deploy the two Cisco CSR1000V or Cisco Catalyst 8000V devices within the AWS transit VPC or Azure transit VNet using Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

# AWS Prerequisite

### Procedure

**Step 1** Have a valid AWS account.

**Step 2** Have a valid AWS Government account for GovCloud access.

**Step 3** Subscribe to the Cisco CSR1000V, Cisco Catalyst 8000V devices Amazon machine image (AMI) in your account within the AWS Marketplace. To subscribe to Amazon machine image (AMI) in your account within the AWS Marketplace:

a) Log in to Amazon Web Services Marketplace.

b) Search AWS Marketplace for: "Cisco CSR1000V or Cisco Catalyst 8000V devices".

A list of AMIs appears.

c) From the list, click the Cisco CSR1000V or Cisco Catalyst 8000V devices link that you're planning to deploy.

The subscription screen appears where you can subscribe to the Cisco CSR1000V or Cisco Catalyst 8000V devices AMI.

d) Click **Continue to Subscribe**.

e) Click **Accept Terms**.

After a few moments, a message appears that you're subscribed to use the Cisco CSR1000V or Cisco Catalyst 8000V devices AMI.

**Note**
Don't click **Continue to Configuration**, because Cisco Catalyst SD-WAN Cloud OnRamp for IaaS automatically configures the Cisco Catalyst SD-WAN cloud devices when it creates the transit VPC.

f) Log out of from the AWS Marketplace.

# Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS

**Points to Consider**

- Transit VPCs provide the connection between the Cisco overlay network and the cloud-based applications running on host VPCs. You can provision up to four pairs of redundant Cisco Catalyst SD-WAN cloud devices within each VPC dedicated to function as a transit point for traffic from the branch to host VPCs. The individual Cisco Catalyst SD-WAN devices of each redundant pair are deployed within a different availability zone in the AWS region of the transit VPC. Multiple Cisco Catalyst SD-WAN devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two Cisco Catalyst SD-WAN cloud devices, the transport VPN (VPN 0) connects to a branch router, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.
- The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VPCs to a transit VPC. To add the public IP address of the WAN interface, configure the VPN interface ethernet template with GigabitEthernet2 interface for the devices used in Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. In Cisco CSR1000V and Cisco Catalyst 8000V devices, the tunnel interface is on the GigabitEthernet2 interface. See sample VPN interface ethernet template configuration in VPN0 Interface Feature Template, on page 33.
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS supports autoscale for AWS. To use the AWS autoscale feature, ensure that you associate one to four pairs of Cisco Catalyst SD-WAN cloud devices with a transit VPC.
- Host VPCs are virtual private clouds in which your cloud-based applications reside. When a transit VPC connects to an application or application provider, it's simply connecting to a host VPC.
- All host VPCs can belong to the same AWS account, or each host VPC can belong to a different account. You can map a host that belongs to one AWS account to a transit VPC that belongs to a different account. You configure cloud instances or cloud accounts by using the Cloud OnRamp configuration wizard.

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for IaaS**.

If you're configuring Cisco Catalyst SD-WAN Cloud OnRamp for IaaS the first time, no cloud instances appear in the screen. A cloud instance corresponds to an AWS account with one or more transit VPCs created within an AWS region.

**Step 2** Click **Add New Cloud Instance**.

**Step 3** Click the **Amazon Web Services (AWS)** radio button.

**Step 4** In the next pop-up window, perform the following:

a) To log in to the cloud server, click **IAM Role** or **Key**. We recommend that you use IAM Role.

b) If you click **IAM Role**, then create an IAM role with Cisco SD-WAN Manager provided **External ID**. Note the displayed external Id from the window and provide the **Role ARN** value that is available when creating an IAM role.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, to create an IAM role, you must enter the Cisco SD-WAN Manager provided External Id into a policy by using the AWS Management Console. Do the following:

1. Attach an IAM Role to an existing Cisco SD-WAN Manager EC2 instance.

   a. See the Creating an IAM role (console) topic of AWS documentation to create a policy. In the AWS **Create policy** wizard, click **JSON** and enter the following JSON policy document.

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]

}
```

   b. See the Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console blog of AWS Security Blog for information about creating an IAM role and attaching it to the Cisco SD-WAN Manager EC2 instance based on the policy created in Step 1.

   **Note**
   On the **Attach permissions policy** window, choose the AWS-managed policy that you created in Step 1.

2. Create an IAM role on an AWS account that you want to use for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

   a. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require external ID** and pasting the external Id that you noted in Step 4(b).

**b.** See the Modifying a role trust policy (console) topic of AWS Documentation to change who can assume a role.

In the **IAM Roles** window, scroll down and click the role you created in the previous step.

In the **Summary** window, note the **Role ARN**.

**Note**
You can enter this role ARN value when you choose the IAM role in Step 4(b).

**c.** After modifying the trust relationship, click **JSON** and enter the following JSON document. Save the changes.

**Note**
The account Id in the following JSON document is the Cisco SD-WAN Manager EC2 instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
       }
      }
    }
  ]
}
```

c) If you click the **Key** radio button:

1. In the **API Key** field, enter your Amazon API key.
2. In the **Secret Key** field, enter the password associated with the API key.
3. From the **Environment** drop-down list, choose **commercial** or **govcloud**.

   By default, commercial environment is selected. You can choose the geographical regions based on the environment specifications.

**Step 5** Click **Login** to log in to the cloud server.

The cloud instance configuration wizard appears. This wizard consists of three screens that you use to select a region, add a transit VPC, discover host VPCs, and map host VPCs to transit the VPC. A graphic on each wizard screen illustrates the steps in the cloud instance configuration process. The steps that aren't yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

**Step 6** Select a region:

From the **Choose Region** drop-down list, choose a region where you want to create the transit VPC.

**Step 7** Add a transit VPC:

a) In the **Transit VPC Name** field, enter the transit VPC name.

The name can contain 128 alphanumeric characters, hyphens (–), and underscores (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VPC:

1. In the **WAN Edge Version** drop-down list, choose the software version of the Cisco Catalyst SD-WAN cloud device to run on the transit VPC.
2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of the Cisco Catalyst SD-WAN cloud devices that run on the transit VPC.
   - See the Supported Instance Types topic for Cisco CSR1000V devices of the *Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services*.
   - See the Supported Instance Types topic for Cisco Catalyst 8000V in the *Deploying Cisco Catalyst 8000V on Amazon Web Services*.

   **Note**
   We recommend that you choose the following size:

   For Cisco CSR1000V and Cisco Catalyst 8000V, choose c5 instance type with four or more than four vCPUs, such as c5.xlarge (4 vCPU).

3. In the **Max. Host VPCs per Device Pair** field, select the maximum number of host VPCs that can be mapped to each device pair for the transit VPC. Valid values are 1–32.
4. To set up the transit VPC devices for Direct Internet Access (DIA), click one of the following:
   - **Disabled**: No Internet access.
   - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.
   - **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.
5. In the **Device Pair 1#** field, choose the serial numbers of each device in the pair. To remove a device serial number, click **X** that appears in the field.

   The serial numbers of the devices that appear are associated with a configuration template and supports the Cisco Catalyst SD-WAN WAN edge version that you selected in Step 1.
6. To add more device pairs, click .

   To remove a device pair, click .

   A transit VPC can be associated with one to four device pairs. To enable the autoscale feature on AWS, associate at least two device pairs with the transit VPC.
7. Click **Advanced**, if you wish to enter more specific configuration options:
   a. In the **Transit VPC CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16. There must be sufficient address space to create six subnets within the CIDR block.
   b. (Optional) In the **SSH PEM Key** drop-down list, choose a PEM key pair to log into an instance. The key pairs are region-specific. See the AWS Documentation for instructions about creating key pairs.

8. To complete the transit VPC configuration, click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

   With this cloud instance, a single transit VPC with two Cisco Catalyst SD-WAN cloud devices has been created. You can configure multiple transit VPCs within a single cloud instance (AWS account within a region). When multiple transit VPCs exist within a cloud instance, you can map host VPCs to any one of the transit VPCs.

9. Discover host VPCs:

   a. In the **Select an account to discover** field, choose the AWS account from which you wish to discover host VPCs.

      Alternatively, to add a new AWS account from which you wish to discover host VPCs, click **New Account**.

   b. Click **Discover Host VPCs**.

      A table appears that display the VPCs, which are available to be mapped to a transit VPC. Only the host VPCs in the selected AWS account and within the same AWS region as the transit VPC appears.

   c. In the table that appears, check one or more hosts to map to the transit VPC.

      To filter the search results, use the Filter option in the search bar and display only host VPCs that match specific search criteria.

      Click the **Refresh** icon to update the table with current information.

      Click the **Show Table Columns** icon to specify which columns to be displayed in the table.

10. Map the host VPCs to a transit VPC:

    a. In the table with all host VPCs, choose the desired host VPCs.

    b. Click **Map VPCs**. The Map Host VPCs pop-up opens.

    c. In the **Transit VPC** drop-down list, choose the transit VPC to map to the host VPCs.

    d. In the **VPN** drop-down list, choose a service VPN in the overlay network in which to place the mapping.

    e. Enable the **Route Propagation** option if Cisco SD-WAN Manager automatically propagates route to the host VPC routes table.

       By default, **Route Propagation** is disabled.

    f. Click **Map VPCs**.

After a few minutes, the **Task View** screen appears, confirming that the host VPC has been mapped to the transit VPC.

**Note**
When configuring the VPN feature template for VPN 0 for the two Cisco Catalyst SD-WAN cloud devices that form the transit VPC, ensure that the color you assign to the tunnel interface is a public color, and not a private color. The following are the public colors:

- **3g**
- **biz-internet**
- **blue**
- **bronze**

- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

# Manage Host and Transit VPCs

## Display Host VPCs

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

By default, the **Mapped Host VPCs** field is selected, and the table under mapped host VPCs list the mapped host and transit VPCs, the state of the transit VPC, and the VPN ID.

**Step 2** To list unmapped host VPCs, click **Un-Mapped Host VPCs**. Then, click **Discover Host VPCs**.

**Step 3** To display the transit VPCs, click **Transit VPCs**.

# Map Host VPCs to a Transit VPC

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Un-Mapped Host VPCs**.

**Step 3** In the **Select an account to discover** field, choose the AWS account from which you wish to discover host VPCs.

**Step 4** Click **Discover Host VPCs**.

**Step 5** From the list of discovered host VPCs, choose the desired host VPCs.

**Step 6** Click **Map VPCs**. The **Map Host VPCs** pop-up opens.

**Step 7** From the **Transit VPC** drop-down list, choose the desired transit VPC.

**Step 8** From the **VPN** drop-down list, choose the VPN in the overlay network in which to place the mapping.

**Step 9** Click **Map VPCs**.

# Unmap Host VPCs

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Mapped Host VPCs**.

**Step 3** From the list of VPCs, choose the desired host VPC that you wish to unmap.

**Step 4** Click **Un-Map VPCs**.

**Step 5** Click **OK** to confirm the unmapping.

Unmapping host VPCs deletes all VPN connections to the VPN gateway in the host VPC, and then deletes the VPN gateway. When you make more VPN connections to a mapped host VPC, these connections are terminated as part of the unmapping process.

# Display Transit VPCs

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Transit VPCs**.

# Add Transit VPC

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Transit VPCs**.

**Step 3** Click **Add Transit VPC**.

To add a transit VPC, follow the instructions in Step 7 of Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS, on page 8.

# Delete Device Pair

**Note** To delete the last pair of online device pairs, ensure to delete a transit VPC.

### Before you begin

The device pair to be deleted should be offline.

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**.

**Step 2** Click a device pair ID.

**Step 3** Verify that the status of the device pair is offline.

**Step 4** To descale the device pairs, click the trash can icon under the **Action** column, or click **Trigger Autoscale**.

# Delete Transit VPC

**Note** To delete the last pair of online device pairs, you should delete a transit VPC.

### Before you begin

Delete the device pairs that are associated with the transit VPC.

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Host VPCs**.

**Step 3** Choose all host VPCs, and click **Un-Map VPCs**.

Ensure that all host VPCs mapped with the transit VPCs are unmapped.

**Step 4** Click **OK** to confirm the unmapping.

**Step 5** Click **Transit VPCs**.

**Step 6** For the desired transit VPC to be deleted, click the trash icon.

**Note**
The trash icon isn't available for the last device pair of transit VPC. Therefore, to delete the last device pair, click the **Delete Transit** drop-down list item. The trash icon is only available from the second device pair onwards.

**Step 7** Click **OK** to confirm.

# Add Device Pairs

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Transit VPCs**.

A table with the list of transit VPCs appears.

**Step 3** For the desired transit VPC, click **...** and choose **Add Device Pair**.

**Step 4** In the **Add Device Pairs** dialog box, click **Add** to add more device pairs.

**Note**
Ensure that the devices you're adding are already associated with a device template.

You can add up to a total of four device pairs to the transit VPC.

**Step 5** Click **Save**.

# History of Device Pairs for Transit VPCs

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Transit VPCs**.

A table with the list of transit VPCs appears.

**Step 3** For the desired transit VPC, click **...** and choose **History for a device pair**.

This displays the Transit VPC Connection History page with all the corresponding events.

**Step 4** View a histogram of events that occurred in the previous one hour and a table of all events for the transit VPC that you've chosen. The table lists all the events generated in the transit VPC. The events can be one of the following:

- Device Pair Added
- Device Pair Spun Up
- Device Pair Spun Down
- Device Pair Removed
- Host Vpc Mapped
- Host Vpc Unmapped
- Host Vpc Moved
- Transit Vpc Created
- Transit Vpc Removed

# Edit Transit VPC

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

**Step 2** Click **Transit VPCs**.

A table with the list of transit VPCs appears.

**Step 3** For the desired transit VPC, click **...** and choose, and click **Edit Transit Details**.

**Step 4** To enter DIA information, follow the instructions in Step 7 (iv) of Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS, on page 8.

This operation might trigger autoscale, if required.

# Microsoft Azure Prerequisites

1. Have a valid Microsoft Azure account.
2. Have a valid Azure Government account for GovCloud access.



**Note** Azure Government Cloud support is only available for Cisco Catalyst 8000V.

3. Accept the terms and conditions for the Cisco CSR1000V or Cisco Catalyst 8000V devices in the Azure Marketplace.

   To use a Cisco Catalyst SD-WAN cloud router as part of the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow, you must accept marketplace terms for using a virtual machine (VM). You can accept the Azure Terms of Service in one of the following ways:

   - Bring up the cloud device on the portal manually, and accept the terms as part of the final page of the onboarding wizard.
   - In the Azure APIs or on the Powershell/Cloud Shell scripts, use the Set-AzureRmMarketplaceTerms command.

4. Create an App Registration in Microsoft Azure and retrieve the credentials for your Azure account. For Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, these credentials are used to authenticate the Cisco SD-WAN Manager server with Azure and bring up the VNet and the Virtual Machine instances.

   To create and retrieve Azure credentials, create an App Registration in Azure with Owner privileges:

   a. Launch the Microsoft Azure Portal.

   b. Verify Azure Active Directory (AD) Permissions. Select Azure Active Directory, and note your role. Only roles with admin privileges can register applications in your Azure AD tenant.

   c. Verify subscription permissions.

      After verifying your role and privileges associated with the Azure AD, ensure that your Azure subscription account has **Microsoft.Authorization/*/Write** access to assign a role to an Azure AD application. This access is associated only with the Owner role or User Access Administrator role.

      1. On the Azure portal, click **Subscriptions**.
      2. Navigate to a **Subscriptions** service, and click the **More Actions** icon to the right of the row.

         The **Microsoft Azure Enterprise** page appears.
      3. Choose **My permissions**. Then, click **Click here to view complete access details for this subscription**.
      4. Click **View my access** to view your assigned roles.
      5. Determine if you have adequate permissions to assign a role to an AD application. If not, ask your Azure subscription administrator to add you to **User Access Administrator** role.

**d.** Create an application ID and service principal:

1. In the left pane of the Azure portal, click **Azure Active Directory**.
2. From the sub-menu, click **App registrations**.
3. Click **New registration**. The system displays the **Register an application** screen.
4. In the **Name** field, enter a descriptive name such as, CloudOnRampApp.
5. In **Suported account types**, choose **Accounts in this organizational directory only (Microsoft only - Single tenant)**.
6. Under **Redirect URI**, choose **Web** for the type of application you want to create.
7. After setting the values, click **Register**.

You've now created your Azure AD application and service principal.

**e.** Create a secret key for the Cloud OnRamp application:

1. From **App registrations** in Azure AD, click your application.
2. On the left pane, click **Certificates & secrets**.
3. Under **Client secrets**, click **New client secret**.
4. Provide a description of the secret key, and an expiry time period for the secret key.
5. Click **Add**.

After saving the client secret, the value of the client secret or key value appears. Note this value because you can't retrieve the key later, if required. You need to provide the key value with the application ID to sign into the application you have created.

**f.** Get Subscription ID:

1. On the Azure portal, click **Subscriptions**.
2. Navigate to a **Subscriptions** service, and click the **More Actions** icon to the right of the row.

   The **Microsoft Azure Enterprise** page appears.
3. From the page, note the **Subscription ID**.

   You need the Subscription ID to provide Cisco SD-WAN Manager with programmatic access to your Azure Subscription.

If you have multiple subscriptions, copy and save the subscription ID which you’re planning to use for configuring the CloudOnRampApp.

**g.** View the Tenant ID:

1. On the left pane of the Azure portal, click **Azure Active Directory**.
2. From the left pane, click **Properties**. The system displays the directory ID which is equivalent to the tenant ID.

**h.** Assign the Owner role to the application:

In this guide, we've provided the steps for assigning the Owner role, which lets you access and manage everything.



**Note** To know an appropriate role for an application, contact your Azure administrator.

1. On the left pane of the Azure portal, click **Subscriptions**.
2. Click the subscription to assign to the Cloud OnRamp application.
3. In the subscription pane, navigate to Access Control (IAM).
4. Click **Add a role assignment**. The **Add role assignment** pop-up appears.
5. From the **Role** drop-down list, choose **Owner**.
6. In the **Assign Access To** drop-down list, choose the default value, **Azure AD user**, **group**, or **service principal**.
7. From the **Select** drop-down list, choose the Cloud OnRamp application that you created in Step d.
8. Click **Save**.

You can see your application in the list of users with a role for that scope.

You can now log into the Cloud OnRamp application with the Azure credentials you created and saved.

5. Check the Azure limits associated with your account by going to your subscription in the Azure portal. Under **Settings**, choose **Usage + Quotas**.
   a. Choose a provider from the **All Providers** drop-down list.
   b. Check **Microsoft.Network**.

   You can view the amount of available availability sets for this subscription. Ensure that availability sets are sufficient that allows you to create the following resources in your account:

   - One VNet, which is required for creating the transit VNet.
   - One availability set required for Virtual Machine distribution in the transit VNet.
   - Six Static Public IP addresses associated with the transit cloud routers.
   - One Azure Virtual Network transit and two Static Public IP Addresses for each host VNet
   - Four VPN connections for mapping each host VNet



**Note** F-Series Azure VMs (F4 and F8) are supported on the Cisco Catalyst SD-WAN cloud devices.

# Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure

In the configuration process, map one or more host VNets to a single transit VNet. When mapping, you're configuring the cloud-based applications that branch users can access.

The mapping process establishes IPsec and BGP connections between the transit VNet and each host VNet. The IPsec tunnel that connects the transit and host VNet runs IKE to provide security for the connection. For Azure, the IPsec tunnel uses IKE version 2. The BGP connection that is established over the secure IPsec tunnel allows the transit and host VNet to exchange routes. The BGP connections or the BGP routes are then re-distributed into OMP within the Cisco Catalyst SD-WAN cloud devices, which then advertises the OMP routes to the Cisco SD-WAN Controller in the domain. The transit VNet can then direct traffic from the branch to the proper host VNet and to the proper cloud-based application.

During the mapping process, the IPsec tunnels and BGP peering sessions are configured and established automatically. After establishing the mappings, you can view the IPsec and BGP configurations in the VPN Interface IPsec and BGP feature configuration templates, and modify them as necessary.

**Points to Consider:**

To configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Azure, create Azure transit VNets, each of which consist of a pair of routers. Then, map the host VNets to transit VNets that exist in the Azure cloud. All VNets reside in the same resource group.

- Transit VNets provide the connection between the overlay network and the cloud-based applications running on the host VNet. Each transit VNet consists of two cloud devices that reside in their own VNet. Two cloud devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two cloud devices, the transport VPN (VPN 0) connects to the simulated branch device, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.
- The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VNets to a transit VNet. To add the public IP address of the WAN interface, configure the VPN Interface Ethernet template with GigabitEthernet2 interface for the devices used in Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. In Cisco CSR1000V and Cisco Catalyst 8000V, the tunnel interface is on the GigabitEthernet2 interface. See sample VPN Interface Ethernet template configuration in VPN0 Interface Feature Template, on page 33.
- Host VNets are virtual private clouds in which your cloud-based applications reside. When a transit VNet connects to an application or application provider, it's simply connecting to a host VNet.

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for IaaS**.

**Step 2** Click **Add New Cloud Instance**

**Step 3** Click the **Microsoft Azure** radio button.

**Step 4** In the next pop-up screen, perform the following:

a) In the **Subscription ID** field, enter the ID of the Microsoft Azure subscription you want to use as part of the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow.
b) In the **Client ID** field, enter the ID of an existing application or create a new application. To create an application, go to your **Azure Active Directory** > **App Registrations** > **New registration**. See Microsoft Azure documentation for more information on creating an application.
c) In the **Tenant ID** field, enter the ID of your account. To find the tenant ID, go to your Microsoft Azure Active Directory and click **Properties**.
d) In the **Secret Key** field, enter the password associated with the client ID.
e) In the **Environment** field, choose **commercial** or **GovCloud**.

   By default, commercial environment is selected. You can choose the geographical locations based on the environment specifications.

f) Click **Login**.

The cloud instance configuration wizard opens.

The wizard consists of three screens that you use to select a location, add a transit VNet, discover host VNets, and map host VNets to the transit VNet. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. The steps not yet completed are shown in light gray. The current step is highlighted within a blue box. All completed steps are indicated with a green checkmark and are shown in light orange.

**Step 5** From the **Choose Location** drop-down list, choose a location where you want to create the transit VNet.

The locations available are based on the commercial cloud or GovCloud selection.

**Step 6** Add a transit VNet:

a) In the **Transit VNet Name** field, type a name for the transit VNet.

   The name can contain 32 alphanumeric characters, hyphens (–), and underscore (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VNet:

   1. In the **WAN Edge Version** drop-down list, choose the software version to run on the transit VNet. The drop-down list includes the published versions of the device software in the Microsoft Azure marketplace.
   2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of theCisco Catalyst SD-WAN cloud devices that run on the transit VNet.
      - See Supported Instance Types for Cisco CSR1000V in the *Cisco CSR 1000v Deployment Guide for Microsoft Azure*.
      - See Supported Instance Types for Cisco Catalyst 8000V in the *Deploying Cisco Catalyst 8000V on Microsoft Azure*.

      **Note**
      We recommend that you choose the following size:

      For Cisco CSR1000V and Cisco Catalyst 8000V, choose DS3 instance type with four or more than four vCPUs such as, Standard DS3 v2 (4vCPU).

   3. To set up the transit VNet devices for Direct Internet Access (DIA), click one of the following:
      - **Disabled**: No Internet access.
      - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.

- **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.

4. In the **Device 1** drop-down list, choose the serial number of the first device.
5. In the **Device 2** drop-down list, choose the serial number of the second device in the device pair.
6. Click **Advanced** if you wish to enter more specific configuration options.
7. In the **Transit VNet CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you leave this field empty, the Transit VNet is created with a default CIDR of 10.0.0.0/16.

c) To complete the transit VNet configuration. click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

**Step 7** Map host VNets to transit VNets:

a) In the **Select an account to discover** drop-down list, choose your Azure subscription ID.

Alternatively, to add a new Azure account from which you wish to discover host VNets, click **New Account**.

b) Click **Discover Host VNets**.
c) In the **Select a VNet** drop-down list, choose a desired host VNet.
d) Click **Next**.
e) From the table of host VNets, choose a desired host VNet.
f) Click **Map VNets**. The Map Host VNets pop-up appears.
g) In the **Transit VNet** drop-down list, choose the transit VNet to map to the host VNets.
h) In the **VPN** drop-down list, choose a VPN in the overlay network in which to place the mapping.
i) In the IPSec Tunnel CIDR section, to configure IPSec tunnels to reach the Azure virtual network transit, enter two pairs of interface IP addresses and a pair of loopback IP addresses for each of the Cisco CSR1000V or Cisco Catalyst 8000V devices . Ensure that the IP addresses are network addresses in the /30 subnet, unique across the overlay network, and they aren't part of the host VNet CIDR. If they are part of the host VNet CIDR, Microsoft Azure returns an error when attempting to create VPN connections to the transit VNet.

**Note**
The IP addresses aren't part of the host VNet and Transit VPC CIDR.

Microsoft Azure supports single Virtual Private Gateway (VGW) configuration over IPSec tunnels with redundancy provided over a single tunnel. Therefore, Cisco Catalyst SD-WAN Cloud OnRamp for IaaS supports two VGWs for redundancy. During a planned maintenance or an unplanned event of a VGW, the IPSec tunnel from the VGW to the cloud devices get disconnected. This loss of connectivity causes the cloud devices lose BGP peering with Cisco SD-WAN Manager over IPSec tunnel. To enable BGP peering with the cloud routers rather than the IP address of the IPSec tunnel, provide the loopback addresses for each cloud device.

**Note**
The loopback option for BGP peering supports single and multiple Virtual Gateways, or Customer Gateway configuration or both on Azure cloud. The loopback option applies only to the new host VNets mapped to transit VNets and not on the existing VNets.

j) In the Azure Information section:

1. In the **BGP ASN** field, enter the ASN that you configure on the Azure Virtual Network Gateway, which is brought up within the host VNet. Use an ASN that isn't part of an existing configuration on Azure. For acceptable ASN values, refer to Microsoft Azure documentation.

2. In the **Host VNet Gateway Subnet** field, enter a host VNet subnet in which the Virtual Network Gateway can reside. We recommend you use a /28 subnet or higher. Ensure not to provide a subnet that is already created in the VNet.

   **Note**
   Ensure that there's an unused CIDR inside the host VNet CIDR.

k) Click **Map VNets**.
l) Click **Save and Complete**.

**Note**
When configuring the VPN feature template for VPN 0 for the two Cisco Catalyst SD-WAN cloud devices that form the transit VNet, ensure that the color you assign to the tunnel interface is a public color, and not a private color. Public colors are:

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

The **Task View** screen appears, confirming that the host VNet has been mapped to the transit VNet successfully.

The creation of VNet Gateway can take up to 45 minutes.

# Manage Host and Transit VNets

## Display Host VNets

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

By default, the **Mapped Host VNets** field is selected and the table under mapped host VNets list the mapped host and transit VNets, the state of the transit VNets, and the VPN ID.

**Step 2** To list unmapped host VNets, click **Un-Mapped Host VNets**. Then click **Discover Host VNets**.

**Step 3** To display the transit VNets, click **Transit VNets**.

## Map Host VNets to an Existing Transit VNet

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

**Step 2** Click **Un-Mapped Host VNets**.

**Step 3** Click **Discover Host VNets**.

**Step 4** From the list of discovered host VNets, choose the desired host VNets.

**Step 5** Click **Map VNet**. The Map Host VNets pop-up opens.

**Step 6** From the **Transit VNet** drop-down list, choose the desired transit VNet.

**Step 7** From the **VPN** drop-down list, choose the VPN in the overlay network in which to place the mapping.

**Step 8** Click **Map VNets**.

## Unmap Host VNets

**Procedure**

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

**Step 2** Click **Mapped Host VNets**.

**Step 3** From the list of VNets, choose the desired host VNets. We recommend that you unmap one VNet at a time. If you want to unmap multiple VNets, don't choose more than three in a single unmapping operation.

**Step 4** Click **Un-Map VNets**.

**Step 5** Click **OK** to confirm the unmapping.

# Display Transit VNets

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

**Step 2** Click **Transit VNets**.

A table lists all the transit VNets.

# Add Transit VNet

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

**Step 2** Click **Transit VNets**.

**Step 3** Click **Add Transit VNet**.

To add a transit VNet, follow the instructions in step 5 of Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure, on page 21.

# Delete Transit VNet

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

**Step 2** Click **Mapped Host VNets**.

**Step 3** Choose the desired host VNet, and click **Un-Map VNets**.

Ensure that you unmap all host VNets that are mapped to the transit VNet that you want to delete.

**Step 4** Click **OK** to confirm the unmapping.

**Step 5** Click **Transit VNets**.

**Step 6** For the desired transit VNet to be deleted, click the trash icon.

**Step 7** Click **OK** to confirm.

# Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

This section describes how to troubleshoot common problems with Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

### Two Cisco CSR1000V or Cisco Catalyst 8000V Devices are Not Available

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. After you click **Add New Cloud Instance**, you see an error message indicating that two Cisco CSR1000V or Cisco Catalyst 8000V devices aren't available.

**Resolve the Problem**

The Cisco SD-WAN Manager server doesn't have two Cisco CSR1000V or Cisco Catalyst 8000V devices that are running licensed Cisco Catalyst SD-WAN software. Contact your operations team so that they can create the necessary Cisco CSR1000V or Cisco Catalyst 8000V devices.

If the Cisco CSR1000V or Cisco Catalyst 8000V devices are present and the error message persists, then the two devices aren't attached to configuration templates. Attach these templates in the Cisco SD-WAN Manager **Configuration** > **Templates** Device window. For the desired device templates, click **…** and choose **Attach Devices**.

### Required API Permissions are Unavailable

When you enter your API keys, you get an error message indicating that this user doesn't have the required permissions.

**Resolve the Problem**

Ensure that the Cisco SD-WAN Manager server can reach the internet and has a DNS server configured so that it can reach AWS or Microsoft Azure. To configure a DNS server, in the Cisco SD-WAN Manager VPN feature configuration template, enter the IP address of a DNS server, and then reattach the configuration template to the Cisco SD-WAN Manager server.

For AWS, check the API keys belonging to your AWS account. If you think you have the wrong keys, generate another pair of keys.

For AWS, if you're entering the correct keys and the error message persists, the keys don't have the required permissions. Check the user permissions associated with the key. Give necessary permissions to the user to create and edit VPCs and EC2 instances.

If the error message persists, check the time of the Cisco SD-WAN Manager server to ensure that it's set to the current time. If it's not, configure the Cisco SD-WAN Manager server time to point to the Google NTP server. To configure the server time, in the Cisco SD-WAN Manager NTP feature configuration template, enter the hostname of an NTP server. Next, reattach the configuration template to the NTP feature using Cisco SD-WAN Manager. The Google NTP servers are time.google.com, time2.google.com,time3.google.com, and time4.google.com, and so on.

### WAN Edge Router Software Versions don't Appear in the Drop-Down When Configuring for AWS

**Problem Statement**

When you're trying to configure transit VPC parameters for the transit VPC, Cisco CSR1000V and Cisco Catalyst 8000V devices software versions aren't listed in the drop-down list.

**Resolve the Problem**

Ensure that you subscribe to the Cisco CSR1000V or Cisco Catalyst 8000V devices Amazon machine image (AMI) in your account within the AWS Marketplace.

Ensure that the Cisco CSR1000V is using software Release 16.12.1b or later and Cisco Catalyst 8000V is using software Release 17.4.1a or later.

### VPNs aren't Listed During Configuration

**Problem Statement**

After you select the host VPCs or VNets to map, VPNs aren't listed in the drop-down list.

**Resolve the Problem**

The problem occurs when the device configuration template attached to the Cisco Catalyst SD-WAN cloud devices doesn't include service-side VPNs. You require the service-side VPNs (VPNs other than VPN 0 and VPN 512) to configure the IPsec connection between the two Cisco Catalyst SD-WAN cloud devices that you select for the transit and host VPCs or VNets.

This problem can also occur if the two Cisco Catalyst SD-WAN cloud devices that you select for the transit VPC or VNet have no overlapping service-side VPNs. Because the two Cisco Cloud Services router 1000V or Cisco Catalyst 8000V devices form an active–active pair, configure the same service-side VPNs on both of them.

To configure service-side VPNs, in the Cisco SD-WAN Manager VPN feature configuration template, configure at least one service-side VPN. Ensure that at least one of the service-side VPNs is the same on both routers. Then reattach the configuration template to the routers.

### Cisco Catalyst SD-WAN Cloud OnRamp for IaaS Task Fails

**Problem Statement**

After you have completed mapping the host VPCs to the transit VPCs, or host VNets to transit VNets, the configuration of Cisco Catalyst SD-WAN Cloud OnRamp for IaaS fails.

**Resolve the Problem**

Review the displayed task information that appears on the screen to determine why the task failed. If the errors are related to AWS or Azure resources, ensure that all required resources are in place.

### Cisco Catalyst SD-WAN Cloud OnRamp for IaaS Task Succeeds, but Cisco Catalyst SD-WAN Cloud Devices Are Down

**Problem Statement**

The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS task was successful, but the Cisco Catalyst SD-WAN cloud devices are still in the down state.

**Resolve the Problem**

Check the configuration templates:

- Check that all portions of the Cisco Catalyst SD-WAN cloud devices configuration, including policies, are valid and correct. If the configurations are invalid, they aren't applied to the router, and the router never comes up.
- Check that the configuration for the Cisco Catalyst SD-WAN Validator is correct. If the DNS name or IP address configured in the Cisco Catalyst SD-WAN Validator is wrong, the Cisco CSR1000V or Cisco Catalyst 8000V device are unable to reach the Cisco Catalyst SD-WAN Validator, and hence they are unable to join the overlay network.

After you have determined what the configuration issues are:

1. Delete the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS components:
   a. Unmap the host VPCs or VNets and the transit VPCs or VNets.
   b. Delete the transit VPC for Cisco CSR1000V or Cisco Catalyst 8000V devices.
2. Edit the configuration templates and reattach them to the Cisco Catalyst SD-WAN cloud devices.
3. Repeat the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS configuration process.

### Desired Routes are Not Exchanged

**Problem Statement**

The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS configuration workflow is successful, the Cisco CSR1000V or Cisco Catalyst 8000V devices are available and running, but the desired routes aren't getting exchanged.

**Resolve the Problem**

In Cisco SD-WAN Manager, check the BGP configuration on the transit cloud routers. During the mapping process, when you configureCisco Catalyst SD-WAN Cloud OnRamp for IaaS service, BGP is configured to advertise the network address, 0.0.0.0/0. Make sure that the service-side VPN contains an IP route that points to 0.0.0.0/0. If necessary, add a static route in the VPN feature configuration template, and then reattach the configuration to the two cloud routers that you selected for the transit VPC or VNet.

On AWS, go to the host VPC and check the route table. In the route table, click **Enable route propagation** to ensure that the VPC receives the routes.

### End-to-End Ping Is Unsuccessful

**Problem Statement**

Routing is working properly, but an end-to-end ping isn't working.

**Resolve the Problem**

On AWS, check the security group rules of the host VPC. On Azure, check the network security group rules of the host VNet. The security group rules must allow the source IP address range subnets of the on-premises or branch-side devices to allow traffic from the branch to reach AWS.

# Sample Feature Template Settings

### Feature Templates

The following is a sample of the various feature templates settings for Cisco CSR1000V, Cisco Catalyst 8000V devices.

### System Feature Template

Template: Basic Information/Cisco System

Template Name: Cisco_System_cEdge_Template

Description: System Template

***Table 2: System feature template settings***

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic Configuration | Site ID | Device Specific | system_site_id |
| | System IP | Device Specific | system_system_ip |
| | Hostname | Device Specific | system_host_name |
| | Device Groups | Device Specific | system_device_groups |
| | Console Baud Rate | Global | 115200 |
| GPS | Latitude | Device Specific | system_latitude |
| | Longitude | Device Specific | system_longitude |
| Advanced | Port Hopping | Device Specific | system_port_hop |
| | Port Offset | Device Specific | system_port_offset |

### Logging Feature Template

Template: Other Templates/Cisco Logging

Template Name: Cisco_Logging_cEdge_Template

Description: Logging Template

*Table 3: Logging feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Server (Optional) | Hostname/IP address | Global | 10.1.0.68 |
| | VPN ID | Device Specific | logging_server_vpn |

The logging server is optional within the Logging_Template.

### BFD Feature Template

Template: Basic Information/Cisco BFD_Template

Template Name: BFD_cEdge_Template

Description: BFD Template

*Table 4: BFD feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic Configuration | Poll Interval | Global | 120000 |
| Color (Biz Internet) | Color | Drop-down list | Biz Internet |
| | Hello Interval (milliseconds) | Device Specific | biz_internet_bfd_hello_interval |
| | Path MTU | Global | Off |

### VPN512 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN512_Template_cEdge_Template

Description: VPN 512 Out-of-Band Management

*Table 5: VPN512 feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic Configuration | VPN | Global | 512 |
| | Name | Global | Management VPN |

### VPN512 Interface Ethernet Feature Template

Template: VPN / Cisco VPN Interface Ethernet

Template Name: Cisco_Transit_VPN512_Interface_Template_cEdge_Template

Description: VPN 512 Management Interface

*Table 6: VPN512 Interface Ethernet feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic Configuration | Shutdown | Global | No |
| | Interface Name | Device Specific | vpn512_mgmt_int |
| | Description | Global | Management Interface |
| IPv4 Configuration | IPv4 Address | Radio Button | Dynamic |

### NTP Feature Template

Template: Basic Information/Cisco NTP

Template Name: Cisco_NTP_cEdge_Template

Description: NTP Template

*Table 7: NTP feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Server | Hostname/IP address | Global | time.nist.gov |

You should be careful to use only known and trusted NTP servers. Disruptions to time synchronizations can affect the ability of the Cisco Catalyst SD-WAN Cloud devices within the transit VPC or transit VNet to connect to the Cisco SD-WAN Control Components, and the ability to establish IPsec connections to other Cisco Catalyst SD-WAN devices.

### AAA Feature Template

Template: Basic Information/Cisco AAA

Template Name: Cisco_AAA_cEdge_Template

Description: AAA Template

*Table 8: Cisco AAA feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Local | User/admin/Password | Global | <your admin password> |
| | User/admin/Privilege | Global | 15 |
| AAA | ServerGroups priority order | Global | local |

### OMP Feature Template

Template: Basic Information/Cisco OMP

Template Name: Cisco_OMP_cEdge_Template

Description: OMP Template

*Table 9: Cisco OMP feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| OMP | Number of Paths Advertised per Prefix | Global | Factory_Default_Cisco_OMP__ipv46_Template |

### Security Feature Template

Template: Basic Information/Cisco Security

Template Name: Cisco_Security_cEdge_Template

Description: Security Template

*Table 10: Security feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Security | Replay window | Global/drop-down list | Factory_Default_Cisco_Security_Template |

### VPN0 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN0_cEdge_Template

Description: VPN0 Transport Template

*Table 11: VPN0 feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic configuration | VPN | Global | 0 |
| | Name | Global | Transport VPN |

### VPN0 Interface Feature Template

Template: VPN/Cisco VPN Interface Ethernet

Template Name: Cisco_Transit_VPN0_cEdge_gigabit-ethernet2

Description: VPN0 Transport Interface

*Table 12: Cisco VPN0 interface feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic configuration | Shutdown | Device Specific | vpn0_inet_int_shutdown |
| | Interface Name | Drop-down list | GigabitEthernet2/ |
| | Description | Global | Internet Interface |
| IPv4 Configuration | IPv4 Address | Radio Button | Dynamic |
| | Bandwidth Upstream | Device Specific | vpn0_inet_int_bandwidth_up |
| | Bandwidth Downstream | Device Specific | vpn0_inet_int_bandwidth_down |
| Tunnel | Tunnel Interface | Global | On |
| | Color | Global | biz-internet |
| | Allow Service>All | Global | On |
| **Tunnel** > **Advanced Options** > **Encapsulation** | IPsec Preference | Device Specific | vpn0_inet_tunnel_ipsec_preference |
| Advanced | TCP MSS | Global | 1350 |

### VPN1 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN1_cEdge_Template

Description: VPN1 Service Template

*Table 13: VPN1 feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic configuration | VPN | Global | 1 |
| | Name | Global | Service VPN 1 |
| | Enhance ECMP Keying | Global | On |
| Advertise OMP | BGP (IPv4) | Global | On |
| | Connected (IPv4) | Global | On |

### VPN2 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN2_cEdge_Template

Description: VPN2 Service Template

*Table 14: VPN2 feature template settings*

| Section | Parameter | Type | Variable/Value |
|---|---|---|---|
| Basic configuration | VPN | Global | 2 |
| | Name | Global | Service VPN 2 |
| | Enhance ECMP Keying | Global | On |
| Advertise OMP | BGP (IPv4) | Global | On |

### Device Templates

The following table summarizes the device template for the Cisco CSR1000V or Cisco Catalyst 8000V devices.

Template Name: Cloud_OnRamp_cEdge_Template

*Table 15: Transit VPC or Transit VNet Device Template*

| Template Type | Template Sub-Type | Template Name |
|---|---|---|
| Cisco System | | Cisco_System_cEdge_Template |
| | Cisco Logging | Cisco_Logging_cEdge_Template |
| | Cisco NTP | Cisco_NTP_cEdge_Template |
| | Cisco AAA | Cisco_AAA_cEdge_Templatee |
| Cisco BFD | | BFD_cEdge_Template |
| Cisco OMP | | Cisco_OMP_cEdge_Template |
| Cisco Security | | Cisco_Security_cEdge_Template |
| Cisco VPN0 | | Cisco_Transit_VPN0_cEdge_Template |
| | Cisco VPN Interface Ethernet | Cisco_Transit_VPN0_cEdge_gigabit-ethernet2 |
| Cisco VPN512 | | Cisco_Transit_VPN512_Template_cEdge_Template |
| | Cisco VPN Interface Ethernet | Cisco_Transit_VPN512_Interface_Template_cEdge_Template |
| Cisco VPN1 | | Cisco_Transit_VPN1_cEdge_Template |

| Template Type | Template Sub-Type | Template Name |
|---|---|---|
| VPN2 | | Cisco_Transit_VPN2_cEdge_Template |

# Sample Device Template Variable Values

The following sample information provides the device template variable values that you can use for the first and second Cisco CSR1000V or Cisco Catalyst 8000V devices.

***Table 16: Cisco CSR1000V or Cisco Catalyst 8000V Device Template Variable Values for First Device***

| Variable | Value |
|---|---|
| Hostname(system_host_name) | CSR_CoR1 |
| System IP(system_system_ip) | 209.165.200.225 |
| Site ID(system_site_id) | 115001 |

***Table 17: Cisco CSR1000V or Cisco Catalyst 8000V Device Template Variable Values for Second Device***

| Variable | Value |
|---|---|
| Hostname(system_host_name) | CSR_CoR2 |
| System IP(system_system_ip) | 209.165.201.1 |
| Site ID(system_site_id) | 115001 |

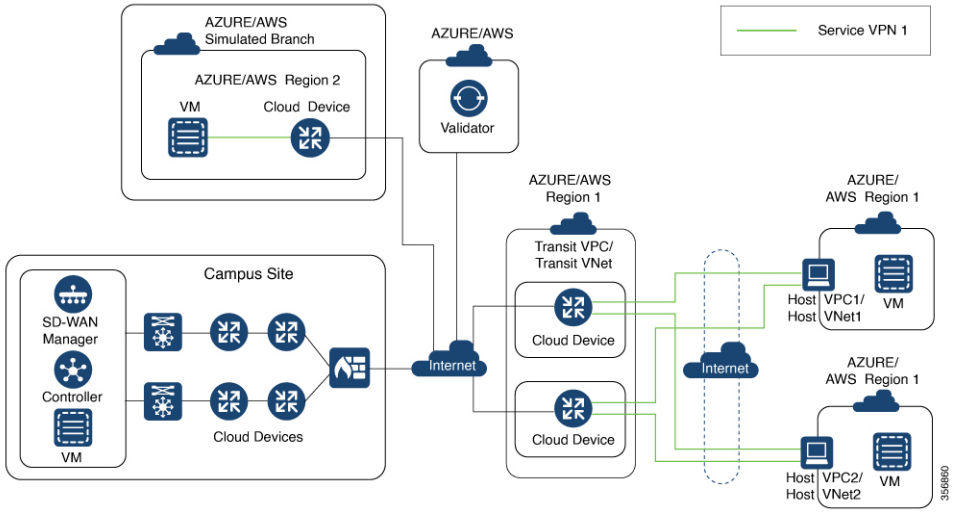
# Example for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

In this example, a single transit VPC or VNet is created within an AWS or Microsoft Azure region and you map two existing host VPCs or VNets within the same region to a transit VPC or VNet. Then, you can access the host VPCs or VNets from a campus and a simulated branch location.

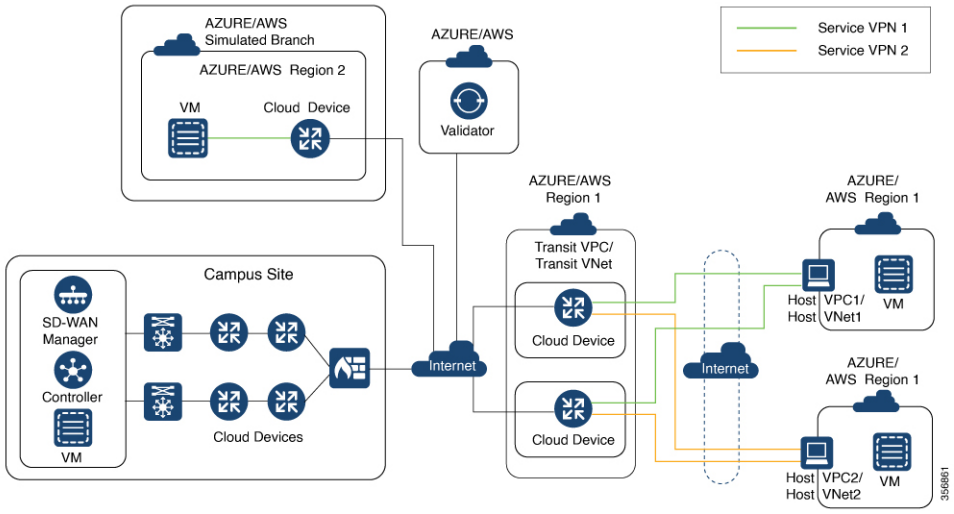
Cisco Catalyst SD-WAN deployments implement connectivity using different VPNs that range 0–512. VPN 0 represents the transport (WAN) network and VPN 512 represents the management network. Use the remaining VPNs (1–511) as service VPNs. The following two scenarios to deploy Cisco Catalyst SD-WAN Cloud OnRamp for IaaS are considered:

- Full connectivity: Map both host VPCs or VNets to service VPN 1 within the transit VPC or VNet. You can configure service VPN 1 on the service-side of Cisco CSR1000V or Cisco Catalyst 8000V devices deployed within the campus, and Cisco CSR1000V or Cisco Catalyst 8000V devices deployed within the simulated branch. This connectivity allows communication from both the campus and the branch sites to AWS Elastic Compute Cloud (EC2) instances within either of the host VPCs. The connectivity also allows communication between AWS or Azure EC2 instances deployed within the two host VPCs. The deployment demonstrates a scenario where all entities within the organization have full connectivity

to the public cloud resources deployed by the organization. The following image illustrates the first scenario.




- Segmentation to the cloud provider: Map one of the host VPCs or VNets to service VPN 1 and the other host VPC or VNet to service VPN 2 within the transit VPC or VNet. This mapping provides segmentation and therefore traffic isolation between the two host VPCs or VNets. You can configure the campus only for service VPN 1, and allowing it to communicate with AWS or Azure EC2 instances within the first host VPC. Configure the branch for service VPN 2, allowing it to communicate with AWS or Azure EC2 instances within the second host VPC. This deployment demonstrates a scenario where different entities within an organization require access only to specific public cloud resources. The following figure illustrates the second scenario.




### Map Host VPCs or VNets to the Transit VPC or VNet in the Same Service VPN

To map both host VPCs or VNets to service VPN 1 within the transit VPC or VNet, perform the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Choose both the host VPCs or host VNets that you want to map, and click **Map VPCs** or **Map VNets**.

The **Map Host VPCs** or **Map Host VNets** pop-up opens.

2. In the **Transit VPC** or **Transit VNet** drop-down list, choose the transit VPC or VNet to map to the host VPCs or VNets.
3. In the **VPN** drop-down list, select **1**.

   Mapping host VPCs or host VNets to the same service VPN allows communication between the host VPCs or VNets.
4. For AWS configuration, disable **Route Propagation**.

   Enabling route propagation propagates the BGP routes to the host VPC selected for mapping.
5. Click **Map VPCs** or **Map VNets**.

   After a few minutes, the Task View window appears, confirming that the host VPC or VNet has been mapped to the transit VPC or VNet.

These steps complete the mapping of both the host VPCs or VNets to service VPN 1. You can verify connectivity between EC2 instances with each host VPC or VNet by establishing an SSH connection between them. Similarly, by mapping both the campus and branch to service VPN 1, you can verify connectivity to both host VPCs or VNets by establishing SSH connections from the campus and branch to the EC2 instances within the host VPCs or VNets.

### Map Each Host VPC or VNet to the Transit VPC or VNet in Different Service VPNs

To map one host VPC or VNet to service VPN 1; while the other host VPC or VNet to service VPN 2, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Choose the host VPC or VNet that you want to map, and click **Map VPCs** or **Map VNets**.

   The **Map Host VPCs** or **Map Host VNets** pop-up opens.
2. In the **Transit VPC** or **Transit VNet** drop-down list, choose the transit VPC or VNet to map to the host VPCs or VNets.
3. In the **VPN** drop-down list, choose **1**.

   The first host VPC or VNet is now mapped to service VPN 1.
4. Click **Map VPCs** or **Map VNets**.

   After a few minutes, the Task View window appears, confirming that the host VPC or VNet has been mapped to the transit VPC or VNet.
5. Repeat Steps 1–3 for the second host VPC or VNet

   When selecting the VPN value, map the host VPC or VNet to service VPN 2.

This process completes the mapping of the first host VPC or VNet to service VPN 1 and the second host VPC or VNet to service VPN 2.

By mapping the campus to service VPN 1, you can verify connectivity to the first host VPC or VNet by establishing SSH connections from the campus to the EC2 instances within that host VPC or VNet. However, SSH connections from the campus to the EC2 instances within the second host VPC or VNet can’t be established. By mapping the branch to service VPN 2, you can verify connectivity to the second host VPC or VNet by establishing SSH connections from the branch to the EC2 instances within that host VPC or VNet.

However, SSH connections from the branch to the EC2 instances within the first host VPC or VNet can’t be established.