

AWS Integration

Table 1: Feature History

Feature Name	Release Information	Description
Integration of AWS Branch with Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	Cisco Catalyst SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS) extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into Cisco Catalyst SD-WAN fabric. This feature enables Transit Gateway when the standard Cloud OnRamp solution is not sufficient. For example, one host VPC is connected to the Cisco Catalyst SD-WAN edge router using an Internet Gateway. If the internet gateway bandwidth limit is less, then transit gateway is used for SD-WAN integration. It provides a way to interconnect VPCs and VPNs.
Support for Pay As You Go License for Cisco Catalyst 8000V Edge Software Instances	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	Cisco Catalyst 8000V Edge Software instances can be used with pay as you go (PAYG) licenses when creating a new cloud gateway in Amazon Web Services (AWS), in addition to the previously supported bring your own license (BYOL) model.
Integration of Cisco Catalyst SD-WAN Branches with AWS using Cisco IOS XE Catalyst SD-WAN Devices and the AWS Transit Gateway Connect feature	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This release enables the use of the AWS Transit Gateway Connect feature to connect a cloud gateway to an AWS transit gateway. This GRE based connection type offers improved bandwidth, scaling, and security compared to the use of IPSec VPN tunnel connections.

Feature Name	Release Information	Description
AWS Branch Connect Solution	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature leverages the AWS Transit Gateway support to connect branch devices to the cloud. The branch devices connect to transit gateway using an IPSec tunnel-based secure channel to access the applications hosted in the cloud. This feature supports scenarios where Cisco SD-WAN Manager instantiates, manages, and controls the AWS Transit Gateway.
AWS Cloud WAN Integration	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enables the use of AWS Cloud WAN to easily connect and route traffic from remote sites, regions and cloud applications over the AWS global network. This feature uses static routing for site-to-site communication.
AWS Cloud WAN Integration with Dynamic Routing	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature is an enhancement to the AWS Cloud WAN integration to support site-to-site communication using dynamic routing, leveraging AWS tunnel-less connect attachment.
Configure Devices for AWS Integration Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for AWS integration.

- Information about AWS Integration, on page 2
- Restrictions for AWS Integration, on page 7
- Configure AWS Integration, on page 8
- Intent Management - Connectivity, on page 22
- Transit Gateway Peering, on page 25
- Audit Management, on page 25
- Monitor AWS Integration using Cisco SD-WAN Manager, on page 29

Information about AWS Integration

A transit gateway is a network transit hub that you can use to interconnect your VPC and on-premises networks. You can attach a VPC, or a VPN connection to a transit gateway. It acts as a virtual router for traffic flowing between your VPC and VPN connections.

You can configure and manage Cloud OnRamp for Multicloud environments through the Cisco SD-WAN Manager controller. A configuration wizard in Cisco SD-WAN Manager automates the bring-up of the transit gateway to your public cloud account, the creation of cloud gateways that includes transit gateways and Cisco

Catalyst 8000V Edge, and the connections between public-cloud applications and the users of those applications at branches in the overlay network. This feature works with AWS virtual private clouds (VPCs) on Cisco cloud routers.

Cloud OnRamp for Multicloud supports integration with multiple AWS accounts. See Limitations for AWS Integration for details.

Supported Platforms

Cloud OnRamp for Multicloud on AWS supports the following platforms:

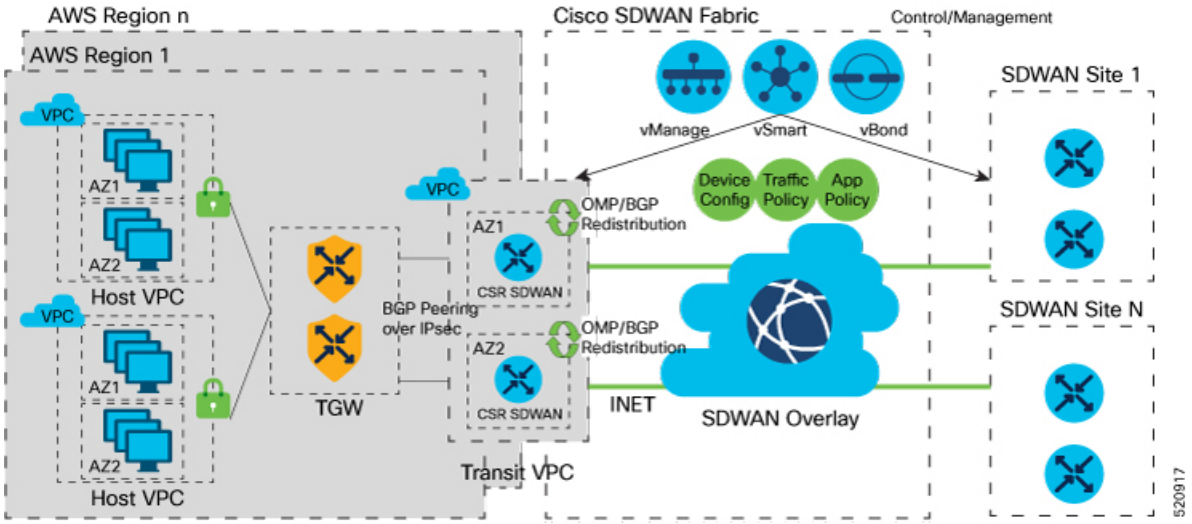
- Cisco Cloud Services Router 1000V Series (Cisco CSR1000V)

Note This platform is supported by Cisco SD-WAN Manager Release 20.3.x.

- Cisco Catalyst 8000V Edge Software

Note This platform is supported by Cisco SD-WAN Manager Release 20.4.x and later.

Architecture



Multicloud Dashboard

Multicloud dashboard in Cisco SD-WAN Manager consists of the following workflows:

- Setup
- Discover
- Manage
- Intent Management

Setup

You can create and manage cloud accounts and configure global settings in Cisco SD-WAN Manager for AWS automation. You can create multiple accounts, pick a specific account for transit gateway, mark one or more accounts for transit VPC automation and use other accounts for host VPC discovery and connectivity.

The multicloud dashboard supports **AWS key** and **IAM role** models for authentication. IAM roles only work for AWS cloud deployed Cisco SD-WAN Manager, as this requires special AWS AssumeRole functions. AssumeRole is used for cross-account access.

Global Settings

Global settings enables you to set a configuration one time and repeat across regions and handle resource management globally (per cloud). The software image and instance size specified are used for instantiation of CSRs in the cloud as part of the cloud gateway.

Global settings include:

- Software image: CSR software image used for creating cloud gateway.
- AWS Instance Size: CSR instance size used depending upon bandwidth requirements.
- Cloud Gateway Solution: The gateway solution used for AWS cloud. For example, transit gateway with transit VPC.
- IP subnet pool: IP subnet pool used for transit VPC creation across regions. Subnet pool can be customized per cloud gateway using custom settings option, if desired.
- Intra-Tag Communication: Allows or denies communication between the VPCs under the same tag.
- Default Route in Host VPCs: Default routes are automatically added to the main route table of the VPC that points to the transit gateway.
- Full Mesh of Transit VPCs: Setup a full mesh connectivity between TVPCs of cloud gateways in different regions so as to carry site to site traffic (through CSRs) over public cloud backbone.



Note When full mesh of transit VPCs is enabled in the global setting for Cisco Catalyst 8000V in an AWS deployment, the GigabitEthernet3 interface is automatically used for the configurations. This interface cannot be used for anything else, nor can the configuration of the interface be modified.



Note The image and the instance size selected once for global settings are not applicable to all the regions. The accounts used for the image discovery can be different and the selected image or the instance size may not be supported in all the regions. AWS instance size and the software image parameters can be changed only for the new cloud gateways that are created after the settings are updated.

For site-to-site communication, an additional interface is configured. The required configuration gets pushed or removed automatically when the site-to-site communication is enabled or disabled respectively in the global settings.

Discover VPCs

You can discover all the VPCs in all the accounts provided across regions. You can tag and untag these VPCs and use it for future connectivity. Cisco SD-WAN Manager creates tag with the key **Cisco-SDWAN-key** and you can customize the tag value for all VPCs within the same tag. The same tag can be used to map VPCs (that is, establish connectivity between VPCs) if the **Intra-Tag communication** in global settings is enabled. You can edit tags and change the membership of a tag associated with a VPC.



Note If you add a tag that is associated with an interconnect gateway, you cannot map it to an AWS cloud gateway in **Intent Management**.

Cloud Gateway

Cloud gateway comprises of a transit VPC, two CSR devices, and a transit gateway. Cisco SD-WAN Manager creates all the components when you pick the account and region to instantiate the cloud gateway. You can attach the appropriate device template to any free, available CSR universally unique identifiers (UUIDs) that are synced from PnP Smart Account.

You can override the global settings with custom settings to pick a different image, instance size, and subnet pool for a specific deployment. Only one cloud gateway instance per region is supported.



Note Ensure that you are subscribed to the image desired for the cloud gateway in the AWS marketplace. If you are not subscribed, then the cloud gateway creation fails.

AWS Branch Connect Overview

The edge devices connect to the host VPCs in the cloud over secure point-to-point tunnels. IPSec tunnels are set up between edge devices and the AWS Transit Gateway. These tunnels carry the branch VPNs traffic and BGP routing traffic. Using BGP, the devices and the transit gateway exchange the routing information and build routing tables.

A branch device can have any number of VPNs that require connectivity to the host VPCs. Each of these VPNs is represented as a VPN attachment to the transit gateway. As part of the VPN attachment, AWS customer gateway and VPN gateway cloud objects are created, which allow VPN connectivity from the branch device to the transit gateway. The transit gateway and the branch devices of a given site are in different BGP ASNs. The mapping information of VPNs to the tags (host VPCs) is derived from the global mapping. This mapping is realized in the cloud.

When you configure a new service VPN in a branch device template, an update event is generated, which triggers mapping based on the connectivity matrix. Similarly, when you remove a service VPN from the device template, another update event is generated, which triggers unmapping.

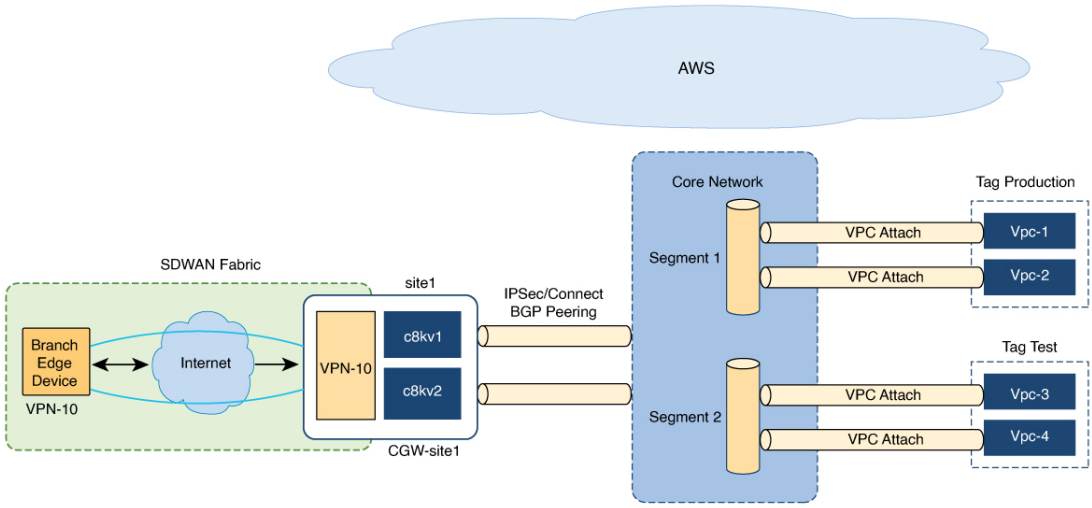


Note The number of branch edge WAN interfaces need to be proportional to the number of regions that the branch edge device needs to connect to. For example, if a branch needs to connect to hosts in two AWS regions, you need one WAN interface attached to each of the cloud gateway in that region. The WAN interfaces within a branch cannot have the same color.

AWS Cloud WAN

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

Figure 1: AWS Cloud WAN



AWS Cloud WAN is a managed WAN service that you can use to build, manage, and monitor a unified global network. You can easily connect and route traffic from different sites and regions over the AWS global network.

AWS Cloud WAN enables you to use simple network policies to configure and secure your network. The network policy is defined and populated in the backend, as you configure AWS integration using Cisco SD-WAN Manager workflows.

Using AWS integration workflows you can create global AWS Cloud WAN network, define different segments and attach different VPCs in different regions to these segments.

(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1) AWS Cloud WAN integration uses BGP-based dymanic routing to route traffic from different sites and regions instead of using static routes. In the AWS integration workflows, the cloud gateways have BGP peering with segments which allow IPSec based connectivity. This adds flexibility and redundancy to the workflows.

Upgrade Considerations from Cisco Catalyst SD-WAN Manager Release 20.12.1 to Cisco Catalyst SD-WAN Manager Release 20.13.1

- Disable the site-to-site communications (in global settings) for AWS in Cisco SD-WAN Manager before you upgrade to Cisco Catalyst SD-WAN Manager Release 20.13.1. After the upgrade is complete you can enable the site-to-site communications in global settings.

Information About Configuring Devices for AWS Integration Using Configuration Groups

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can use configuration groups in Cisco SD-WAN Manager to configure devices in AWS integration workflows. The use of same configuration groups between two cloud gateways is not supported.

You can enable configuration of devices using configuration groups in the global settings. When you create a cloud gateway, if you have enabled configuration using configuration groups in the global settings, you can choose an existing configuration group or create a new one. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups.

Note After you enable configuration of devices using configuration groups in the global settings, you can configure devices using both templates and configuration groups.

Software-Defined Cloud Interconnect Cloud Gateway Extension

From Cisco Catalyst SD-WAN Manager Release 20.15.1, in the Software-Defined Cloud Interconnect (SDCI) workflow, while creating a cloud gateway, you cannot configure devices using configuration groups.

Restrictions for AWS Integration

- The AWS Government cloud (AWS GovCloud) is not supported.

Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, AWS GovCloud (US) is supported.

- AWS integration on IPv6 is not supported.
- Tags that are associated with host VPCs that have overlapping CIDRs cannot be mapped to each other.
- Overlapping IP addresses in different VPNs mapped to one host-VPC are not supported.
- AWS has a limit of 1000 routes per VPN connection. You need to provision a template with the aggregate-address or the network in BGP if you have more routes per VPN.
- AWS transit gateway has only 20 route tables by default.
- Auto-correct removal of cloud gateway through AWS console is not configured.
- Only one cloud gateway per region can be created.
- Only a single pair of Cisco cloud routers is instantiated.
- The CSR image version selected should be 16.12.02r or later.

- Cisco SD-WAN Manager configures one VPN tunnel per CSR 1000 device. This limits the bandwidth of the solution to 2.5 GBPS (1.25 GBPS throughput for each tunnel).
- Beginning with Cisco IOS XE Release 17.6.2, Cloud OnRamp for Multicloud supports integration with 10 AWS accounts.
- Multi cloud AWS Branch Connect Solution works only with Cisco SD-WAN branch or devices deployed using feature templates. The branches or devices based on configuration groups or CLI template are not supported.
- The CGW deployment with local zone enabled in AWS region is not supported.

Restrictions for AWS Cloud WAN

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

- You can only create cloud gateways from the same AWS account.
- The AWS Government cloud (AWS GovCloud) is not supported.
- AWS Cloud WAN supports only up to 20 segments per core network.
- The maximum number of supported peerings per core network is 50.
- You cannot create cloud gateways in regions that do not support AWS Cloud WAN. For information about currently supported regions, see the AWS documentation.
- The API support to get the status of the BGP sessions of the tunnels is not available in AWS. Therefore, the tunnel to AWS Cloud WAN network may be shown as reachable even when the cloud gateway is powered off in Cisco SD-WAN Manager.

Configure AWS Integration

AWS Configuration Prerequisites

You need the following to configure AWS integration using Cisco SD-WAN Manager.

- AWS cloud account details
- Subscription to AWS marketplace
- Cisco SD-WAN Manager must have two cloud router licenses that are free to use for creating a new account

Create AWS Cloud Account

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. The Cloud OnRamp for Multicloud dashboard displays.
2. Click **Associate Cloud Account** in the Setup pane. Note the external Id from the **Associate Cloud Account** page.

3. In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.
4. Enter the account name in the **Account Name** field.
5. (Optional) Enter the description in the **Description** field.
6. In **Use for Cloud Gateway**, choose **Yes** if you want to create cloud gateway in your account, or choose **No**.
7. Choose the authentication model you want to use in the field **Login in to AWS With**.
   - **Key**
   - **IAM Role**

   If you choose the **Key** model, then provide **API Key** and **Secret Key** in the respective fileds.

   Or

   If you choose the **IAM Role** model, 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 External Idprovided by Cisco SD-WAN Manager into a policy by using the AWS Management Console.



Note When deploying Cloud OnRamp for Multicloud for an AWS account, if EC2 instance that hosts Cisco SD-WAN Manager is using Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) then the hop limit needs to be updated to 2 so that the IAM role credentials can be retrieved and used for communication with Cisco SD-WAN Manager. EC2 instances using Amazon EC2 Instance Metadata Service Version 1 (IMDSv1) do not require this step.

Do the following:

a. Attach an IAM Role to an existing Cisco SD-WAN Manager EC2 instance.
   1. 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": "*"

    }
]
```

```
}
```

2. 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.

Note The following set of permissions are allowed:

- AmazonEC2FullAccess
- IAMReadOnlyAccess
- AWSNetworkManagerFullAccess
- AWSResourceAccessManagerFullAccess

For more information on creating an AWS IAM Role, refer Creating an AWS IAM Role.

b. Create an IAM role on an AWS account that you want to use for the multicloud environment.

1. 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 2.
2. 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** that is displayed at the top.

Note You can enter this role ARN value when you choose the authentication model as IAM role in Step 7.

3. 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 belongs to 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]"
          }
        }
      }
    ]
}
```

8. Click **Add**.

To view or update cloud account details, click **...** on the Cloud Account Management page.

You can also remove the cloud account if there are no associated host VPC tags or cloud gateways.



Note During Multicloud resource cleanup process, Cisco SD-WAN Manager compares the current database to running resources in the account with org name and account detail tags. If there are any resources that matches the tags, but not in the current database are deleted. Therefore, the AWS Multicloud resources of Cisco SD-WAN Manager can be deleted by another Cisco SD-WAN Manager, if the organization name and the associated AWS account details are same. We recommend that if you are using the same AWS account across different Cisco SD-WAN Manager overlays, ensure that you use different organization and overlay name for each Cisco SD-WAN Manager.

Configure Cloud Global Settings

To configure cloud transit gateway global settings, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Cloud Global Settings** in the **Setup** pane. The **Cloud Global Settings** window appears.
2. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)

   Enable the **Enable Configuration Group** option to use configuration groups to configure devices.
3. In the **Cloud Provider** field, choose **Amazon Web Services**.
4. Click **Cloud Gateway Solution** drop-down list to choose the AWS Transit Gateway and CSR in Transit VPC, or, beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, one of the following options.

   Beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, a combination of options is not supported. For example, if there are cloud gateways that were created using VPN connections, you must delete these cloud gateways before you can create AWS Transit Gateway Connect connections.

   - **Transit Gateway–VPN based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach.
   - **Transit Gateway–Connect based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud

gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS TGW Connect (GRE tunnels) approach.

- **Transit Gateway–Branch-connect**—Allows connectivity of different Cisco Catalyst SD-WAN edge devices to VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. This option uses the AWS VPN connection (IPSec) approach.
- (Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1)

  Cloud WAN–VPN based (using TVPC)—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach.
- (Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1)

  Cloud WAN–Connect based (using TVPC)—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS Connect attachments (supporting GRE tunnels) approach.

5. Beginning with Cisco vManage Release 20.8.1, the following fields are available:
   - Click the **Reference Account Name** drop-down list to choose the reference account name. Cisco SD-WAN Manager discovers the software images and instance sizes using this reference account name.



Note You can still choose a different account, if required, at the time of a cloud gateway creation.

   - Click the **Reference Region** drop-down list to choose the reference region. Cisco SD-WAN Manager discovers the software images and instance sizes in this reference region under the referenced account name.

6. In the **Software Image** field, do the following:
   a. Click **BYOL** to use a bring your own license software image or **PAYG** to use a pay as you go software image.
   b. From the drop-down list, select a software image.
7. Click the **Instance Size** drop-down list to choose the required size.
8. Enter the **IP Subnet Pool**.
9. Enter the **Cloud Gateway BGP ASN Offset**.
10. Choose the **Intra Tag Communication**. The options are **Enabled** or **Disabled**.
11. Choose the **Default Route**. The options are **Enabled** or **Disabled**.
12. Click **Update**.

Parameter	Description
Software Image	Specifies the preinstalled or the subscibed software images for your account.

Parameter	Description
Instance Size	

Parameter	Description
	Specifies the instance size. The options are: • t2.medium • t3.medium • c4.2xlarge • c4.4xlarge • c4.8xlarge • c4.xlarge • c5.2xlarge • c5.4xlarge • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge • c5n.4xlarge • c5n.9xlarge • c5n.large • c5n.xlarge **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, following instance types are supported: • t3.medium • c5.2xlarge • c5.4xlarge **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, c5.4xlarge is not supported. • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge • c5n.4xlarge

Parameter	Description
	• c5n.9xlarge • c5n.large • c5n.xlarge Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, following instance is supported: • c5n.18xlarge **Note** Upgrade Cisco Catalyst SD-WAN Cloud devices running on Cisco SD-WAN Manager Release 19.2.1 on c3.2xlarge to Cisco SD-WAN Manager Release 20.4.1 or later in the following order. **1.** Resize c3.2xlarge to c5.4xlarge **2.** Upgrade the software to Cisco SD-WAN Manager Release 20.4.1 or later. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, following instance types are supported: • t3.medium • c5.large • c5.xlarge • c5.2xlarge • c5.9xlarge • c5n.4xlarge • c5n.18xlarge • c6in.large • c6in.xlarge • c6in.2xlarge • c6in.8xlarge
Cloud Gateway Solution	Specifies the combination of the Cloud Gateway Solution. For example, AWS Transit Gateway and CSR in Transit VPC.

Parameter	Description
IP Subnet Pool	Specifies the list of IP subnets separated by comma in CIDR format. More than one subnets can be specified. A single /24 subnet pool is able to support one cloud gateway only. You cannot modify the pool when a few cloud gateways are already making use of pool. Overlapping of subnets is not allowed.
Cloud Gateway BGP ASN Offset	Specifies the offset for allocation of transit gateway BGP ASNs. It is used to block routes learnt from one transit gateway (eBGP) to another. A band of 30 ASNs are reserved for transit gateway ASNs. Starting offset plus 30 will be the organization side BGP ASN. For example, if the offset is 64830, Org BGP ASN will be 64860. Acceptable start offset range is 64520 to 65500. It must be a multiple of 10.
Tunnel Count	This field appears if you choose **Transit Gateway–Connect based (using TVPC)** from the **Cloud Gateway Solution** drop-down list. Enter the number of tunnels for a VPN connection. You can configure up to 4 tunnels for each VPN connection. Each tunnel supports up to 5 Gbps of traffic. **Note** Changing the value of this parameter does not affect existing cloud gateways. To update the tunnel count for an existing cloud gateway, edit the cloud gateway from the **Configuration** > **Cloud OnRamp For Multicloud** > **Cloud Gateway** page.
Intra Tag Communication	Specifies if the communication between host VPCs under the same tag is enabled or disabled. If any tagged VPCs are already present and cloud gateways exist in those regions, then this flag cannot be changed.
Program Default Route in VPCs towards TGW	Specifies if the main route table of the host VPCs is programmed with default route is enabled or disabled.
Full Mesh of Transit VPCs	Specifies the full mesh connectivity between TVPCs of cloud gateways in different regions to carry site to site traffic (through CSRs).

Table 2: Expected Behavior for Global Settings

Item	Changeable after cloud gateway is created (Yes/No)	Default (Enabled/Disabled)
Software Image	Yes	NA
Instance Size	Yes	NA
IP Subnet Pool	See the description below	NA
Cloud Gateway BGP ASN Offset	No	NA
Intra Tag Communication	Cannot be changed if both cloud gateways and tagged host VPCs exist in any region	Enabled at the API level
Program Default Route in VPCs towards TGW	No	Enabled at the API level
Full Mesh of Transit VPCs	Yes	Disabled

Global IP Subnet Pool – can only be updated if there is no cloud gateway using global subnet pool. A cloud gateway uses global subnet pool whether it has custom setting or not. The subnet pool value is similar to the one in global setting (you can compare after splitting the list of CIDRs by comma; for example, *10.0.0.0/8, 10.255.255.254/8* and *10.255.255.254/8, 10.0.0.0/8* are similar).

If there is no cloud gateway using global subnet pool, the updated subnet pool in the global setting should not overlap with any of the existing custom subnet pools.

Custom IP Subnet Pool – when a custom setting is created, its subnet pool should not overlap with any of the existing custom subnet pools. It cannot partially overlap with the configured global subnet pool.

Discover Host Private Networks

You can discover host VPCs in all the accounts across all the respective regions of the account that are available. When the **Host VPC Discovery** is invoked, the discovery of the VPCs is performed without any cache.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Host Private Networks** under **Discover**. The **Discover Host Private Networks** window appears with the list of available VPCs.

   The host VPC table includes the following columns:

   - Cloud Region
   - Account Name
   - Host VPC Name
   - Host VPC Tag
   - Account ID
   - Host VPC ID

Click a column to sort the VPCs, as required.

2. Click the **Region** drop-down list to select the VPCs based on particular region.
3. Click **Tag Actions** to perform the following actions:
   - **Add Tag** - group the selected VPCs and tag them together.
   - **Edit Tag** - migrate the selected VPCs from one tag to another.
   - **Delete Tag** - remove the tag for the selected VPCs.

   A number of host VPCs can be grouped under a tag. All VPCs under the same tag are considered as a singular unit. A tag ensures connectivity and is essential to view the VPCs in **Intent Management**.

Create Cloud Gateway

Cloud gateway is an instantiation of Transit VPC (TVPC), CSRs within TVPC and transit gateway in the cloud. To create a cloud gateway, perform the following steps.

Note Before beginning this procedure, ensure that you have two devices with templates attached, which have the same type of license (BYOL or PAYG).

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Create Cloud Gateway** under **Manage**. The **Manage Cloud Gateway - Create** window appears.
2. In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.
3. In the **Cloud Gateway Name** field, enter the cloud gateway name.
4. (Optional) In the **Description**, enter the description.
5. Choose the account name from the **Account Name** drop-down list.
6. Choose the region from the **Region** drop-down list.
7. (Optional) Choose the SSH Key from the drop-down list.
8. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.
9. In the **Software Image** field, do the following:
   a. Choose a licensing option: **BYOL** for bring your own license or **PAYG** for pay as you go.
   b. In the drop-down menu, choose a software image.

Note The software image options are determined by the selection of **BYOL** or **PAYG**.

Note For information about onboarding a Cisco Catalyst 8000V without using Cisco Cloud OnRamp for Multicloud, see the Cisco SD-WAN Getting Started Guide.

10. Click the **Instance Size** drop-down list to choose the required size. Pick the size of the WAN edge based on the capacity needs.
11. Enter the **IP Subnet Pool**. Subnet pool is used for transit VPC creation, needs between /16 to /24.System allocates /27 per transit VPC 8 subnet(s).
12. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)

    If you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for AWS, from the **Configuration Group** drop-down list, perform one of these actions:

    - Choose a configuration group.
    - To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow.

Note When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers.

    a. Select the **Chassis number** to associate a pair of chassis to the configuration group.
    b. Click **Configure Device Parameters** and enter the following:
        1. **System IP**
        2. **Hostname**
        3. **TLOC Color**
        4. **Username**
        5. **User Password**
    c. Click **Create Gateway**.

13. The option is applicable only to configuration using device templates.

    Choose the UUID details in the **UUID (specify 2)** drop-down list.

Note

- Only logical devices (UUIDs) with a template attached appear in the list.
- From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

14. (Minimum release: Cisco vManage Release 20.10.1) In the **Multi-Region Fabric Settings** area, for **MRF Role**, choose **Border** or **Edge**.

    This option is available only when Multi-Region Fabric is enabled.

15. Click **Add** to create a new cloud gateway.

Note Creating cloud gateways for AWS Cloud WAN can take over an hour depending on the resources deployed. The first deployment in a region can fail if AWS verifying and validating the resources in this region.

You cannot create cloud gateways in regions that do not support AWS Cloud WAN. For information about currently supported regions, see the AWS documentation.

Configure Site Attachment

Perform the following steps to attach sites to a cloud gateway:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Gateway Management** under **Manage**. The **Cloud Gateways** window appears. A table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.

   For each of the cloud gateways, you can view, delete, or attach more sites.

2. For the desired cloud gateway, click **...** and choose **Cloud Gateway**.
3. Click **Attachment**.
4. Click **Attach Sites**.
5. In the **Circuit Color** drop-down list, choose a circuit color. A circuit color defines the search criteria for the sites you want to connect to your cloud gateway.
6. Click **Next**. The **Attach Sites - Select Sites** window appears. The table shows the sites with the selected circuit color.
7. Choose one or more sites from **Available Sites** and move them to **Selected Sites**.
8. Click **Next**.
9. On the **Attach Sites - Site Configuration** window, enter the **Tunnel Count**. The tunnel count ranges from 1 to 8 and each tunnel gives a bandwidth of 2.5 Gbps.
10. For the **Accelerated VPN** option, choose **Enabled** or **Disabled**. AWS Global Accelerator helps in optimized connectivity to the cloud.

11. Click **Next**. The **Attach Sites - Configuration Override** window appears. You can override the configuration that you performed in previous step, if required. You can alter the values for tunnel count and accelerated VPN status.
12. Click **Next**. The **Next Steps** window appears, where you can save the attachments you've added and exit the flow.
13. Click **Save and Exit**. If the configuration is successful, you see a message that indicates that the branch endpoints were successfully attached.

Note To view the tunnel status, go to the **Cloud OnRamp for Multicloud** Dashboard or the **Site Details** window.

Detach Sites

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Gateway Management** under **Manage**. The **Cloud Gateways** window appears. The table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.
2. For the desired cloud gateway, click **...** and choose **Cloud Gateway**. Next, click **Attachment**. The **Attachments - Cloud Gateway Name** window appears. The window displays the list of sites attached to the cloud gateway.
3. Click **Detach Sites**. The **Are you sure you want to detach sites from cloud gateway?** window appears.
4. Click **OK**. The sites attached to a cloud gateway are detached. The unmapping of the site happens and the VPN configuration is removed from the device.

Remove Cloud Gateway

On the **Cloud Gateways** window, for the desired cloud gateway, click **...**, and choose **Delete**. You must detach all the sites from a cloud gateway before trying to delete the cloud gateway.

You can view the cloud resources in the Cloud Resources Inventory for each cloud gateway in Cisco SD-WAN Manager.

Intent Management - Connectivity

Mapping workflow in Cisco SD-WAN Manager enables connectivity between Cisco Catalyst SD-WAN VPNs (segment) and VPCs, and VPCs to VPCs. VPCs are represented based on the tags.

Note Mapping of a new intent for a mapping task in progress is disabled. When intra-tag is enabled and when VPCs within the same region are added to the same tag, the mapping happens as part of tagging.

When the system records the intent for connectivity, mapping is realized in cloud in regions where cloud gateway is present. Mapping intents can be entered without cloud gateways being present in different regions. The user mapping intent is preserved and realized when a new cloud gateway or mapping change is discovered. As and when cloud gateways get instantiated in different regions, the mapping intents are realized in those

regions. Similarly, tagging operations can influence the mapping in different regions as well and mappings as per the tags are realized in the cloud.

In the Cloud OnRamp for Multicloud dashboard, click **Connectivity** under **Management**. The **Intent Management - Connectivity** window appears. The window displays the connectivity status with the following legends:

- Blank - Editable
- Grey color - System Defined
- Blue color - Intent Defined
- Green color - Intent Realized
- Red color - Intent Realized With Errors

On the **Connectivity** window, you can:

- View the changes in connectivity as required.
- Filter and sort.
- Define the connectivity independent of cloud gateways in different regions.
- Realize the connectivity in regions wherever cloud gateways are present.

Mapping is automatically realized when a cloud gateway exists in the same region or when tagging operations take place.

Connectivity information or the intent is entered in a matrix form with VPNs, tags as sources and tags as destinations. When you click on each cell, it provides a detailed information on - Mapped, Unmapped and Outstanding mapping.

VPCs involved in mapping (as part of tags) should have at least one subnet. VPCs with overlapping CIDRs lead to failed mapping.

Starting from Cisco IOS XE Catalyst SD-WANRelease 17.3.2, the mapping is region agnostic and can span a number of regions than confined to a given region. Instead of multiple mapping requests, a single mapping request involving a number of regions is dispatched towards the cloud agent. The information of all the VPCs, VPNs and connectivity elements across regions is put together in the same mapping request. The mapping status is enhanced to get the connectivity information and the current attachment specifications of the entire network of all the regions.

Depending on the mapping, more than one region can be locked at the same time. Inter-region mapping changes the mapping of local to regions to across regions as applicable. The regions are locked where a mapping is done across multiple regions. As audit is global in nature, all regions are locked while the audit is on.



Note AWS cloud operations can take up to 40-60 minutes to complete mapping the intent management.

Note Users are responsible for adding specific routes to transit gateway endpoint outside IPs for the tunnels to come up between the branched service and AWS transit gateway while using multiple WAN interfaces. Branch connect mapping only configures the required IPsec tunnel configuration to transit gateway endpoints.

Note The maximum number of supported peerings per core network is 50. If the number of VPN connections exceed this limit, the mapping fails.

Note During the mapping, the Multicloud workflow adds a default route in the VPC main route table. However, this does not happen if the main route table already has a default route. The VPC main route table should not have existing default route before mapping is applied.

IPsec Tunnels Down Due to Weaker Crytpo

When you upgrade Cisco SD-WAN Manager with multi cloud AWS VPN connect or branch connect to Cisco vManage Release 20.11.1 and the Cisco Catalyst 8000V Edge Software to Cisco IOS XE Catalyst SD-WAN Release 17.11.x from earlier 17.x releases, the IPsec tunnels between the TGW (transit gateway) of the Cisco Catalyst SD-WAN device and Cisco Catalyst SD-WAN devices in the cloud gateway will go down.

To bring up the tunnels, do either of the following:

- If you want to continue with older crypto configuration, use the **crypto engine compliance shield disable** command in the Cisco Catalyst SD-WAN devices of the cloud gateway and reload the devices to bring up the tunnels. The tunnels will come up with a weaker crypto. Any inconsistencies that appear in the cloud connections triggers an audit. When the audit triggers, all tunnels from group 2 will change to group 15 crypto and tunnels will still be down. To resolve this issue after the audit, unmap and map the connections using the Intent Management Cloud Connectivity page in Cisco SD-WAN Manager.
- When you upgrade Cisco SD-WAN Manager with multi cloud AWS VPN connect or branch connect to Cisco vManage Release 20.11.1 and the Cisco Catalyst 8000V Edge Software to 17.11 from earlier 17.x releases, instead of using the CLI command you can directly unmap and map the connections using the Intent Management Cloud Connectivity page in Cisco SD-WAN Manager. The tunnels will come up with group 15 crypto.

Note Use the above steps to bring up tunnels with the stronger crypto when you upgrade the AWS CGWExtn in SDCI. Software-Defined Cloud Interconnect (SDCI) has a solution called AWS CGWExtn that is deployed from SDCI. When you create a cloud gateway in Cisco SD-WAN Manager that uses SDCI, the tunnels will be down as AWS is deployed. You can access the gateways from the Intent Management Cloud Connectivity page in Cisco SD-WAN Manager.

Transit Gateway Peering

Table 3: Feature History

Feature Name	Release Information	Description
Transit Gateway Peering	Cisco IOS XE Release 17.3.2 Cisco vManage Release 20.3.2	This feature enables the ability to establish peer connections between transit gateways in different AWS regions. With this feature, you can connect to various Transit Virtual Private Clouds (TVPCs) and on-premise networks using a single gateway. The ability to peer transit gateways between different AWS regions enables you to extend the connectivity and build global networks spanning multiple other regions. To support inter-region connectivity, mapping and audit functions are enhanced.

Inter-region connectivity for multicloud networking allows communication among VPCs spread across a number of regions. It supports the following connectivity options:

- intra-tag communication within VPCs using a single tag across multiple regions.
- tag to tag connectivity with VPCs within them spread across a number of regions.

The VPC and VPN attachments are associated with and propagated to different routing tables within the transit gateway. Depending on the desired connectivity, there are routes within transit gateway route tables towards the VPC and TVPC classless inter-domain routes (CIDRs) of other regions pointing to respective transit gateway peered attachments. This allows VPCs and cloud service routers in one TVPC region to communicate with VPCs and cloud service routers in other TVPCs in other regions. TVPCs are connected in a mesh, whereas connectivity of host VPCs follows the connectivity or the intent matrix defined.

The VPN-to-tag connectivity is limited to VPN-to-VPCs connectivity (VPCs within the tag) within that region. The VPN connectivity does not traverse the transit gateway peered attachments.

The audit functionality is configured at a global level and is enhanced to reinstate the broken transit gateway peered attachments, ensuring inter-CSRs connectivity. For more details on Audit, see Audit Management.

Audit Management

In the Cloud OnRamp for Multicloud dashboard, the audit screen helps to bring the cloud state in sync with the Cisco SD-WAN Manager state. When the mapping fails because of a tagging mismatch or missing host VPCs, audit helps in fixing the mapping for recoverable errors and mismatched tagging issues.

In the **Cloud OnRamp for Multicloud** window, for the desired cloud type, click **...** and choose **Audit**. The Audit report for the desired cloud type appears.

Audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what has been realized in the cloud. The gaps are in terms of cloud resources, their mappings, or connectivity and states. When such gaps are detected, Cisco SD-WAN Manager flags such gaps and takes recovery actions to bring the cloud state in sync with the intents configured. For example, if there's an intent to map all host VPCs in some account or region tagged with some tag to get mapped to some given transit gateway and a new host

VPC tagged with the same tag is found disconnected with transit gateway, Cisco SD-WAN Manager connects the new host VPC back with the transit gateway.

Types of Audit:

- On-Demand
  - Invoked by the user.
  - If the report is out of sync, you can initiate audit-with-fix-option to fix the issue.
- Periodic - Invoked by the system automatically, periodically every 2 hrs. The first periodic audit will start in 15 minutes after the system startup.

The audit functionality is configured at a global level and is enhanced to reinstate the broken transit gateway peered attachments, ensuring inter-CSRs connectivity.

(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1) For AWS Cloud WAN, you can view and compare the policy documents on Cisco SD-WAN Manager and the core network policy that are available on cloud resources inventory for each cloud gateway. You can identify the discrepencies in these policy documents and troubleshoot accordingly.

For more information on AWS integration, see:

- Amazon Virtual Private Cloud Getting Started Guide
- Amazon Virtual Private Cloud Network Administrator Guide
- Transit gateway VPN Attachment

Multicloud Audit-reported Anomalies and Fixes

Table 4: Examples of AWS audit discrepancies

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Transit Gateway Attachment with Resource Type as **VPC** in AWS (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details**: Mapping issue Connectivity element was missing from response: [srcType:VPC ID dstType: <C8kv-device1-UUID]> Connectivity element was missing from response: [srcType: <C8kv-device1-UUID >dstType: VPCID]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the applicable solution type.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing site-to-site VPN Attachment (Transit Gateway Attachment Type VPN) in AWS	Transit Gateway–VPN based (using TVPC) / Cloud WAN–VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: Mapping **Details**: Mapping issue vpnAttachSpec with tunnelId: <C8kv-device1-UUID >:<VPNID> was missing from the cloud.	Yes, audit-fix workflow - 1 is triggered.
Missing Transit Gateway Attachment > VPC Attachment in secondary AWS account (Applicable when CGW and workload hosts are in different accounts) (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:VPC src: VPC1-Account1 dstType: VPC2 dst: VPC2] Connectivity element was missing from response: [srcType:VPC src: vpc-1 dstType: <C8kv-device1-UUID>]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the solution type.
Missing Transit Gateway Attachment with resource type as **Connect** in AWS	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC)	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:<C8kv-device1-UUID> dstType:VPC dst:VPCID] Connectivity element was missing from response: [srcType: C8kv-device2-UUID> dstType:VPC dst:VPCID]	Yes, audit-fix workflow - 2 is triggered.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Host VPC (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: HOSTVPC **Details:** Host Vpc issue: <VPC ID> Hostvpc: <VPC ID> Tag mismatch- [<TAG NAME>! =] Hostvpc: <VPC ID> Couldn't find in the cloud.	Yes, audit will remove the missing VPC from tag(s) and from discovered VPC list.
Missing TGW	Transit Gateway–VPN based (using TVPC) / Cloud WAN VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TGW **Details:** Cloud Gateway (TGW) issue: TGW missing from the cloud. Name: <TGW Name>, region: <Region>. Please recreate the Cloud Gateway	Not fixable
Missing C8kv	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC) / Transit Gateway–VPN based (using TVPC) / Cloud WAN – VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TVPC **Details:** Cloud Gateway (TVPC) issue. Name: <CGW Name>, Id:<TVPC Id>. Please recreate the Cloud Gateway.	Not fixable
Invalid credentials	All	Could not perform audit at this time. Please retry after 10 minutes. Audit Failure.	Not fixable

Note Network connectivity disturbance is expected when the audit-fix (on-demand or periodic) is in progress, as the fix workflow deletes and recreates attachments and mappings in all the regions.

Note VPCs referred to are those discovered and tagged by Cisco SD-WAN Manager. “Missing” is defined in the context of the Cisco SD-WAN Manager’s database/knowledge.

Note Audit-fix performs the same steps in both on-demand (that is, clicking the **Fix Sync Issues** button) and periodic audit scenarios.

Note Audit-fix deletes all out-of-band attachments (VPC, TGW-peering, and Connect) to TGW or CloudWAN that users have manually created or mapped outside of CoR workflow, if any exist.

Monitor AWS Integration using Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

Multicloud Deployments

You can view the following information about multicloud deployments from **Monitor** > **Multicloud** on Cisco SD-WAN Manager:

- For each cloud type:
  - Number of cloud gateways and the health of each gateway.
  - Number of WAN edge devices and its health.
  - Number of sites connected to cloud gateways.
  - Number of VPN connection tunnels through cloud gateways.
  - Number of connected tags.
  - Number of mapped host VPCs or vNETs.
  - Number of VPN connections.
- For AWS Cloud WAN solution, you can view the operational AWS Cloud WAN core network policy in the AWS cloud.

Multicloud Dashboard

You can view the multicloud dashboard from **Configuration** > **Cloud OnRamp for Multicloud** on Cisco SD-WAN Manager. The multicloud dashboard summarizes the whole network snapshot where you can view information about each cloud gateway.

You can view the state of BGP sessions from each of the WAN edge devices for site-to-site communication through AWS Cloud WAN in **Additional Details** section on the dashboard.