Amazon Virtual Private Cloud

Transit Gateways

Amazon Virtual Private Cloud: Transit Gateways

Table of Contents

What is a Transit Gateway?

A *transit gateway* is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks.

For more information, see AWS Transit Gateway.

Transit Gateway Concepts

The following are the key concepts for transit gateways:

- **attachment** — You can attach a VPC or VPN connection to a transit gateway.
- **transit gateway route table** — A transit gateway has a default route table and can optionally have additional route tables. A route table includes dynamic and static routes that decide the next hop based on the destination IP address of the packet. The target of these routes could be a VPC or a VPN connection. By default, the VPCs and VPN connections that you attach to a transit gateway are associated with the default transit gateway route table.
- **associations** — Each attachment is associated with exactly one route table. Each route table can be associated with zero to many attachments.
- **route propagation** — A VPC or VPN connection can dynamically propagate routes to a transit gateway route table. With a VPC, you must create static routes to send traffic to the transit gateway. With a VPN connection, routes are propagated from the transit gateway to your on-premises router using Border Gateway Protocol (BGP).

Working with Transit Gateways

You can create, access, and manage your transit gateways using any of the following interfaces:

- **AWS Management Console**— Provides a web interface that you can use to access your transit gateways.
- **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Amazon VPC, and is supported on Windows, Mac, and Linux. For more information, see AWS Command Line Interface.
- **AWS SDKs** — Provides language-specific APIs and takes care of many of the connection details, such as calculating signatures, handling request retries, and error handling. For more information, see AWS SDKs.
- **Query API**— Provides low-level API actions that you call using HTTPS requests. Using the Query API is the most direct way to access Amazon VPC, but it requires that your application handle low-level details such as generating the hash to sign the request, and error handling. For more information, see the Amazon EC2 API Reference.

Pricing

You are charged based on each hour that your VPC or VPN connection are attached to the transit gateway. For more information, see AWS Transit Gateway pricing.

How Transit Gateways Work

A *transit gateway* acts as a regional virtual router for traffic flowing between your virtual private clouds (VPC) and VPN connections. A transit gateway scales elastically based on the volume of network traffic. Routing through a transit gateway operates at layer 3, where the packets are sent to a specific next-hop attachment, based on their destination IP addresses.

Resource Attachments

A transit gateway attachment is both a source and a destination of packets. You can attach the following resources to your transit gateway, if they are in the same Region as the transit gateway:

- One or more VPCs
- One or more VPN connections

Availability Zones

When you attach a VPC to a transit gateway, you must enable one or more Availability Zones to be used by the transit gateway to route traffic to resources in the VPC subnets. To enable each Availability Zone, you specify exactly one subnet. The transit gateway places a network interface in that subnet using one IP address from the subnet. After you enable an Availability Zone, traffic can be routed to all subnets in that Availability Zone, not just the specified subnet.

We recommend that you enable multiple Availability Zones to ensure availability. If one Availability Zone becomes unavailable or has no healthy attachments, the transit gateway can route traffic to your VPC using a healthy attachment in a different Availability Zone.

Routing

Your transit gateway routes IPv4 and IPv6 packets between attachments using transit gateway route tables. You can configure these route tables to propagate routes from the route tables for the attached VPCs and VPN connections. You can also add static routes to the transit gateway route tables. When a packet comes from one attachment, it is routed to another attachment using the route table that matches the destination IP address.

Route Tables

Your transit gateway automatically comes with a default route table. By default, this route table is the default association route table and the default propagation route table. Alternatively, if you disable route propagation, we do not create a default route table for the transit gateway

You can create additional route tables for your transit gateway. This enables you to isolate subnets of attachments. Each attachment can be related to one or more route tables through route table association and route table propagation.

Route Table Association

You can associate a transit gateway attachment with a single route table. Each route table can be associated with zero to many attachments and forward packets to attachments or other route tables.

Route Propagation

Each attachment comes with routes that can be installed to one or more transit gateway route tables. For a VPC attachment, these are the CIDR blocks of the VPC. For a VPN connection attachment, these are the prefixes that are advertised over the BGP session established with the VPN connection. When an attachment is propagated to a transit gateway route table, these routes are installed in the route table.

Scenarios

The following are common use cases for transit gateways. Your transit gateways are not limited to these use cases.

Centralized Router

You can configure your transit gateway as a centralized router that connects all of your VPCs and VPN connections. In this scenario, all attachments are associated with the transit gateway route table and propagate to the transit gateway route table. Therefore, all attachments can route packets to each other, with the transit gateway serving as a simple layer 3 IP hub.

Isolated Routers

You can configure your transit gateway as multiple isolated routers. This is similar to using multiple transit gateways, but provides more flexibility in cases where the routes and attachments might change. In this scenario, each isolated router has a single route table. All attachments associated with an isolated router propagate and associate with its route table. Attachments associated with one isolated router can route packets to each other, but cannot route packets to or receive packets from the attachments for another isolated router.

Edge Consolidator

You can configure your transit gateway such that your VPCs can route packets to one or more VPN connections but your VPCs cannot route packets to each other. In this scenario, you create a route table for the VPCs and a route table for the VPN connections.

Getting Started with Transit Gateways

The following tasks help you become familiar with transit gateways. You will create a transit gateway and then connect two of your VPCs using the transit gateway.

Tasks

Prerequisites

- To demonstrate a simple example of using a transit gateway, create two VPCs in the same Region. The VPCs cannot have overlapping CIDRs. Launch one EC2 instance in each VPC. For more information, see Working with VPCs and Subnets in the *Amazon VPC User Guide*.
- You must enable resource sharing from the master account for your organization. For information about enabling resource sharing, see Enable Sharing with AWS Organizations in the *AWS RAM User Guide*.
- You cannot have identical routes pointing to two different VPCs. A transit gateway does not propagate the CIDRs of a newly attached VPC if an identical route exists in the transit gateway route tables.
- Verify that you have the permissions required to work with transit gateways. For more information, see Authentication and Access Control for Your Transit Gateways (p. 20).

Step 1: Create the Transit Gateway

When you create a transit gateway, we create a default transit gateway route table and use it as the default association route table and the default propagation route table.

To create a transit gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the Region selector, choose the Region that you used when you created the VPCs.
3. On the navigation pane, choose **Transit Gateways**.
4. Choose **Create Transit Gateway**.
5. (Optional) For **Name tag**, type a name for the transit gateway. This creates a tag with "Name" as the key and the name that you specified as the value.
6. (Optional) For **Description**, type a description for the transit gateway.
7. For **Amazon side ASN**, type the private Autonomous System Number (ASN) for your transit gateway. This should be the ASN for the AWS side of a Border Gateway Protocol (BGP) session.

The range is 64512 to 65534 for 16-bit ASNs.

The range is 4200000000 to 4294967294 for 32-bit ASNs.

8. (Optional) You can modify the default settings if you need to disable DNS support, or if you don't want the default association route table or default propagation route table.
9. Choose **Create Transit Gateway**.
10. After you see the message **Create Transit Gateway request succeeded**, choose **Close**. The initial state of the transit gateway is `pending`.

Step 2: Attach Your VPCs to Your Transit Gateways

Wait until the transit gateway you created in the previous section shows as available before proceeding with creating an attachment.

Confirm that you have created two VPCs and launched an EC2 instance in each, as described in Prerequisites (p. 4).

Create a Transit Gateway Attachment to a VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose **Create Transit Gateway Attachment**.
4. For **Transit Gateway ID**, choose the transit gateway to use for the attachment.
5. For **Attachment type**, choose **VPC**.
6. (Optional) For **Attachment name tag**, type a name for the attachment.
7. Choose whether to enable **DNS support**. For this exercise, do not enable **IPv6 support**.
8. For **VPC ID**, choose the VPC to attach to the transit gateway.
9. For **Subnet IDs**, select one subnet for each Availability Zone to be used by the transit gateway to route traffic. You must select at least one subnet. You can select only one subnet per Availability Zone.
10. Choose **Create attachment**.

Each attachment is always associated with exactly one route table. Route tables can be associated with zero to many attachments.

Step 3: Add Routes between the Transit Gateway and your VPCs

A route table includes dynamic and static routes that determine the next hop for associated VPCs based on the destination IP address of the packet.

To add a route to a VPC route table

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Route Tables**.
3. Choose the route table associated with your VPC.
4. Choose the **Routes** tab, then choose **Edit routes**.

5. Choose **Add route**.
6. In the **Destination** column, enter an IP address range that includes the transit gateway you used to create the transit gateway attachment.
7. Choose **Close**.

Step 4: Testing the Transit Gateway

You can confirm that the transit gateway was successfully created by connecting to an EC2 instance in each VPC, and then sending data between them, such as a ping command. For more information, see Connect to Your Linux Instance or Connecting to Your Windows Instance.

Step 5: Delete the Transit Gateway

When you no longer need a transit gateway, you can delete it. You cannot delete a transit gateway that has resource attachments. As soon as the transit gateway is deleted, you stop incurring charges for it.

To delete your transit gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the attachments and then choose **Actions**, **Delete**. When prompted for confirmation, choose **Delete**.
4. On the navigation pane, choose **Transit Gateways**.
5. Select the transit gateway and then choose **Actions**, **Delete**. When prompted for confirmation, choose **Delete**.

Working with Transit Gateways

You can work with transit gateways using the Amazon VPC console or the AWS CLI.

Contents

Transit Gateways

A transit gateway enables you to attach VPCs and VPN connections in the same Region and route traffic between them. A transit gateway works across AWS accounts, and you can use AWS Resource Access Manager to share your transit gateway with other accounts. After you share a transit gateway with another AWS account, the account owner can attach their VPCs to your transit gateway. A user from either account can delete the attachment at any time.

Each VPC or VPN attachment is associated with a single route table. That route table decides the next hop for the traffic coming from that resource attachment. A route table inside the transit gateway allows for both IPv4 or IPv6 CIDRs and targets. The targets are VPCs and VPN connections. When you attach a VPC or create a VPN connection on a transit gateway, the attachment is associated with the default route table of the transit gateway.

You can create additional route tables inside the transit gateway, and change the VPC or VPN association to these route tables. This enables you to segment your network. For example, you can associate development VPCs with one route table and production VPCs with a different route table. This enables you to create isolated networks inside a transit gateway similar to virtual routing and forwarding (VRFs) in traditional networks.

Transit gateways support dynamic and static routing between attached VPCs and VPN connections. You can enable or disable route propagation for each attachment.

Create a Transit Gateway

When you create a transit gateway, we create a default transit gateway route table and use it as the default association route table and the default propagation route table.

You must enable resource sharing from the master account for your organization. For information about enabling resource sharing, see Enable Sharing with AWS Organizations in the *AWS RAM User Guide*.

To create a transit gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateways**.
3. Choose **Create Transit Gateway**.
4. For **Name tag**, optionally enter a name for the transit gateway. A name tag can make it easier to identify a specific gateway from the list of gateways. When you add a **Name tag**, a tag is created with a key of **Name** and with a value equal to the value you enter.
5. For **Description**, optionally enter a description for the transit gateway.

6. For **Amazon side ASN**, either leave the default value to use the default Autonomous System Number (ASN), or enter the private ASN for your transit gateway. This should be the ASN for the AWS side of a Border Gateway Protocol (BGP) session.

   The range is 64512 to 65534 for 16-bit ASNs.

   The range is 4200000000 to 4294967294 for 32-bit ASNs.
7. For **DNS support**, choose **enable** if you need the VPC to resolve public IPv4 DNS host names to private IPv4 addresses when queried from instances in another VPC attached to the transit gateway.
8. For **VPN ECMP support**, choose **enable** if you need Equal Cost Multipath (ECMP) routing support between VPN connections. If connections advertise the same CIDRs, the traffic is distributed equally between them.
9. For **Default route table association**, choose **enable** to automatically associate transit gateway attachments with the default route table for the transit gateway.
10. For **Default route table propagation**, choose **enable** to automatically propagate transit gateway attachments to the default route table for the transit gateway.
11. For **Auto accept shared attachments**, choose **enable** to automatically accept cross-account attachments.
12. Choose **Create Transit Gateway**.
13. After you see the message **Create Transit Gateway request succeeded**, choose **Close**.

To create a transit gateway using the AWS CLI

Use the create-transit-gateway command.

View Your Transit Gateways

To view your transit gateways using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateways**. The details for the transit gateway are displayed below the list of gateways on the page.

To view your transit gateways using the AWS CLI

Use the describe-transit-gateways command.

Add or edit tags for a transit gateway

Add tags to your resources to help organize and identify them, such as by purpose, owner, or environment. You can add multiple tags to each transit gateway. Tag keys must be unique for each transit gateway. If you add a tag with a key that is already associated with the transit gateway, it updates the value of that tag. For more information, see Tagging Your Amazon EC2 Resources.

Add tags to a transit gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateways**.
3. Choose the transit gateway for which to add or edit tags.
4. Choose the **Tags** tab in the lower part of the page.
5. Choose **Add/Edit Tags**.
6. Choose **Create Tag**.

7. Enter a **Key** and **Value** for the tag.
8. Choose **Save**.

Sharing a Transit Gateway

You can use AWS Resource Access Manager (RAM) to share a transit gateway across accounts or across your organization in AWS Organizations. Use the following procedure to share a transit gateway that you own.

To share a transit gateway

1. Open the AWS Resource Access Manager console at https://console.aws.amazon.com/ram/.
2. Choose **Create a resource share**.
3. Under **Description**, for **Name**, type a descriptive name for the resource share.
4. For **Select resource type**, choose **Transit Gateways**. Select the transit gateway.
5. (Optional) For **Principals**, add principals to the resource share. For each AWS account, OU, or organization, specify its ID and choose **Add**.

   For **Allow external accounts**, choose whether to allow sharing for this resource with AWS accounts that are external to your organization.
6. (Optional) Under **Tags**, type a tag key and tag value pair for each tag. These tags are applied to the resource share but not to the transit gateway.
7. Choose **Create resource share**.

Accepting a Resource Share

If you were added to a resource share, you receive an invitation to join the resource share. You must accept the resource share before you can access the shared resources.

To accept a resource share

1. Open the AWS Resource Access Manager console at https://console.aws.amazon.com/ram/.
2. On the navigation pane, choose **Shared with me**, **Resource shares**.
3. Select the resource share.
4. Choose **Accept resource share**.
5. To view the shared transit gateway, open the **Transit Gateways** page in the Amazon VPC console.

Delete a Transit Gateway

You can't delete a transit gateway with existing attachments. You need to delete all attachments before you can delete a transit gateway.

To delete a transit gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose the transit gateway to delete.
3. Choose **Actions**, **Delete**, then choose **Delete** to confirm the deltion.

To delete a transit gateway using the AWS CLI

Use the delete-transit-gateway command.

Transit Gateway Attachments to a VPC

When you attach a VPC to a transit gateway, you must specify one subnet from each Availability Zone to be used by the transit gateway to route traffic. Specifying one subnet from an Availability Zone enables traffic to reach resources in every subnet in that Availability Zone.

Limits

The resources in a VPC attached to a transit gateway and that have the transit gateway in a subnet route table can only forward traffic to the transit gateway, when the transit gateway has an attachment in any subnet in that VPC in the same Availability Zone.

The resources in a VPC attached to a transit gateway cannot access the security groups of a different VPC that is also attached to the same transit gateway.

Create a Transit Gateway Attachment to a VPC

To create a VPC attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose **Create Transit Gateway Attachment**.
4. For **Transit Gateway ID**, choose the transit gateway for the attachment. You can choose a transit gateway that you own or a transit gateway that was shared with you.
5. For **Attachment type**, choose **VPC**.
6. Under **VPC Attachment**, optionally type a name for **Attachment name tag**.
7. Choose whether to enable **DNS Support** and **IPv6 Support**.
8. For **VPC ID**, choose the VPC to attach to the transit gateway.

   This VPC must have at least one subnet associated with it.
9. For **Subnet IDs**, select one subnet for each Availability Zone to be used by the transit gateway to route traffic. You must select at least one subnet. You can select only one subnet per Availability Zone.
10. Choose **Create attachment**.

To create a VPC attachment using the AWS CLI

Use the create-transit-gateway-vpc-attachment command.

View Your VPC Attachments

To view your VPC attachments using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose the search bar, select **Resource type** from the menu, and then select **VPC**.
4. The VPC attachments are displayed. Choose an attachment to view its details or to add tags.

To view your VPC attachments using the AWS CLI

Use the describe-transit-gateway-vpc-attachments command.

Delete a VPC Attachment

To delete a VPC attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the VPC attachment.
4. Choose **Actions**, **Delete**.
5. When prompted for confirmation, choose **Delete**.

To delete a VPC attachment using the AWS CLI

Use the delete-transit-gateway-vpc-attachment command.

Transit Gateway VPN Attachments

To attach a VPN connection to your transit gateway, you must specify the customer gateway.

For static VPNs, add the static routes to the transit gateway route table.

Create a Transit Gateway Attachment to a VPN

To create a VPN attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose **Create Transit Gateway Attachment**.
4. For **Transit Gateway ID**, choose the transit gateway for the attachment. You can choose a transit gateway that you own or a transit gateway that was shared with you.
5. For **Attachment type**, choose **VPN**.
6. For **Customer Gateway**, do one of the following:
    - To use an existing customer gateway, choose **Existing**, and then select the gateway to use.

      If your customer gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device, and adjust your firewall rules to unblock UDP port 4500.
    - To create a customer gateway, choose **New**, then for **IP Address**, type a static public IP address and **BGP ASN**.

      For **Routing options**, choose whether to use **Dynamic** or **Static**.
7. For **Tunnel Options**, see Site-to-Site VPN Routing Options in the *AWS Site-to-Site VPN User Guide*.
8. For **Inside IP CIDR**, For more information about VPN tunnels, see Configuring the VPN Tunnels for Your Site-to-Site VPN Connection, and Overview of Setting Up a Site-to-Site VPN Connection in the *AWS Site-to-Site VPN User Guide*.
9. Choose **Create attachment**.

To create a VPN attachment using the AWS CLI

Use the create-vpn-connection command.

View Your VPN Attachments

To view your VPN attachments using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose the search bar, select **Resource type** from the menu, and then select **VPN**.
4. The VPN attachments are displayed. Choose an attachment to view its details or to add tags.

To view your VPN attachments using the AWS CLI

Use the describe-transit-gateway-attachments command.

Transit Gateway Route Tables

Use transit gateway route tables to configure routing for your transit gateway attachments.

Create a Transit Gateway Route Table

To create a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Choose **Create Transit Gateway Route Table**.
4. (Optional) For **Name tag**, type a name for the transit gateway route table. This creates a tag with the tag key "Name", where the tag value is the name that you specify.
5. For **Transit Gateway ID**, select the transit gateway for the route table.
6. Choose **Create Transit Gateway Route Table**.

To create a transit gateway route table using the AWS CLI

Use the create-transit-gateway-route-table command.

Associate a Transit Gateway Route Table

You can associate a transit gateway route table with a transit gateway attachment.

To associate a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table.
4. In the lower part of the page, choose the **Associations** tab.
5. Choose **Create association**.
6. Choose the attachment to associate and then choose **Create association**.

To associate a transit gateway route table using the AWS CLI

Use the associate-transit-gateway-route-table command.

Delete an Association for a Transit Gateway Route Table

You can disassociate a transit gateway route table from a transit gateway attachment.

To disassociate a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table.
4. In the lower part of the page, choose the **Associations** tab.
5. Choose the attachment to disassociate and then choose **Delete association**.
6. When prompted for confirmation, choose **Delete association**.

To disassociate a transit gateway route table using the AWS CLI

Use the disassociate-transit-gateway-route-table command.

View Transit Gateway Route Tables

To view transit gateway route tables using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. To find a specific route table or set of tables, enter all or part of the name, keyword, or attribute in the filter field.

Choose a route table to display the settings for it.

To view transit gateway route tables using the AWS CLI

Use the describe-transit-gateway-route-tables command.

Propagate a Route to a Transit Gateway Route Table

Use route propagation to add a route from a route table to an attachment.

To propagate a route to a transit gateway attachment route table

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table for which to create a propagation.
4. Choose **Actions**, **Create propagation**.
5. On the **Create propagation** page, choose the attachment.
6. Choose **Create propagation**.
7. Choose **Close**.

To enable route propagation using the AWS CLI

Use the enable-transit-gateway-route-table-propagation command.

Disable Route Propagation

Remove a propagated route from a route table attachment.

To disable route propagation using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table to delete the propagation from.
4. On the lower part of the page, choose the **Propagations** tab.
5. Select the attachment and then choose **Delete propagation**.
6. When prompted for confirmation, choose **Delete propagation**.

To disable route propagation using the AWS CLI

Use the disable-transit-gateway-route-table-propagation command.

View Route Table Propagations

To view route propagations using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table to view propagations for.
4. On the lower part of the page, choose the **Propagations** tab.

To view route propagations using the AWS CLI

Use the get-transit-gateway-route-table-propagations command.

Export Route Tables to Amazon S3

You can export your route tables to an Amazon S3 bucket for backup or accessing them to import to another transit gateway.

To export transit gateway route tables using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Choose the route table that includes the routes to export.
4. Choose **Actions**, **Export routes**.
5. On the **Export routes** page, for **S3 bucket name**, type the name of the S3 bucket.
6. To filter the routes exported, specify filter parameters in the **Filters** section of the page.
7. Choose **Export routes**.

Delete a Transit Gateway Route Table

To delete a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table to delete.
4. Choose **Actions**, **Delete route table**.
5. Choose **Delete** again to confirm the deletion.

To delete a transit gateway route table using the AWS CLI

Use the delete-transit-gateway-route-table command.

Monitor Your Transit Gateways

You can use the following features to monitor your transit gateways, analyze traffic patterns, and troubleshoot issues with your transit gateways.

CloudWatch metrics

You can use Amazon CloudWatch to retrieve statistics about data points for your transit gateways as an ordered set of time series data, known as *metrics*. You can use these metrics to verify that your system is performing as expected. For more information, see CloudWatch Metrics for Your Transit Gateways (p. 16).

VPC Flow Logs

You can use VPC Flow Logs to capture detailed information about the traffic going to and from your transit gateways. For more information, see VPC Flow Logs in the *Amazon VPC User Guide*.

CloudTrail logs

You can use AWS CloudTrail to capture detailed information about the calls made to the transit gateway API and store them as log files in Amazon S3. You can use these CloudTrail logs to determine which calls were made, the source IP address where the call came from, who made the call, when the call was made, and so on. For more information, see Logging API Calls for Your Transit Gateway Using AWS CloudTrail (p. 17).

CloudWatch Metrics for Your Transit Gateways

Amazon VPC publishes data points to Amazon CloudWatch for your transit gateways. CloudWatch enables you to retrieve statistics about those data points as an ordered set of time series data, known as *metrics*. Think of a metric as a variable to monitor, and the data points as the values of that variable over time. Each data point has an associated timestamp and an optional unit of measurement.

You can use metrics to verify that your system is performing as expected. For example, you can create a CloudWatch alarm to monitor a specified metric and initiate an action (such as sending a notification to an email address) if the metric goes outside what you consider an acceptable range.

Amazon VPC reports metrics to CloudWatch only when requests are flowing through the transit gateway. If there are requests flowing through the transit gateway, Amazon VPC measures and sends its metrics in 60-second intervals. If there are no requests flowing through the transit gateway or no data for a metric, the metric is not reported.

For more information, see the Amazon CloudWatch User Guide.

Contents

Transit Gateway Metrics

The `AWS/TransitGateway` namespace includes the following metrics.

Metric	Description
`BytesIn`	The number of bytes received by the transit gateway.
`BytesOut`	The number of bytes sent from the transit gateway.
`PacketsIn`	The number of packets received by the transit gateway.
`PacketsOut`	The number of packets sent by the transit gateway.
`PacketDropCountBlackhole`	The number of packets dropped because they matched a blackhole route.
`PacketDropCountNoRoute`	The number of packets dropped because they did not match a route.

Metric Dimensions for Transit Gateways

To filter the metrics for your transit gateways, use the following dimensions.

Dimension	Description
`TransitGateway`	Filters the metric data by transit gateway.

Logging API Calls for Your Transit Gateway Using AWS CloudTrail

AWS CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service. CloudTrail captures all transit gateway API calls as events. The calls captured include calls from the AWS Management Console and code calls to the transit gateway API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for transit gateways. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to the transit gateway API, the IP address from which the request was made, who made the request, when it was made, and additional details.

For more information about CloudTrail, see the AWS CloudTrail User Guide.

Transit Gateway Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs through the transit gateway API, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for the transit gateway API, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail

- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All calls to transit gateway actions are logged by CloudTrail. For example, calls to the `CreateTransitGateway` action generates entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding Transit Gateway Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The log files include events for all AWS API calls for your AWS account, not just transit gateway API calls. You can locate calls to the transit gateway API by checking for `eventSource` elements with the value `ec2.amazonaws.com`. To view a record for a specific action, such as `CreateTransitGateway`, check for `eventName` elements with the action name.

The following are example CloudTrail log records for the transit gateway API for a user who created a transit gateway using the console. You can identify the console using the `userAgent` element. You can identify the requested API call using the `eventName` elements. Information about the user (`Alice`) can be found in the `userIdentity` element.

Example Example: CreateTransitGateway

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Authentication and Access Control for Your Transit Gateways

AWS uses security credentials to identify you and to grant you access to your AWS resources. You can use features of AWS Identity and Access Management (IAM) to allow other users, services, and applications to use your AWS resources fully or in a limited way, without sharing your security credentials.

By default, IAM users don't have permission to create, view, or modify AWS resources. To allow an IAM user to access resources, such as a transit gateway, and perform tasks, you must create an IAM policy that grants the IAM user permission to use the specific resources and API actions they'll need, then attach the policy to the IAM user or the group to which the IAM user belongs. When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources.

To work with a transit gateway, one of the following AWS managed policies might meet your needs:

- **PowerUserAccess**
- **ReadOnlyAccess**
- **AmazonEC2FullAccess**
- **AmazonEC2ReadOnlyAccess**

For more information, see IAM Policies for Amazon EC2 in the *Amazon EC2 User Guide*.

Transit Gateway Service-Linked Role

Amazon VPC uses service-linked roles for the permissions that it requires to call other AWS services on your behalf. For more information, see Using Service-Linked Roles in the *IAM User Guide*.

Permissions Granted by the Service-Linked Role

Amazon VPC uses the service-linked role named **AWSServiceRoleForVPCTransitGateway** to call the following actions on your behalf when you work with a transit gateway:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterface`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`

AWSServiceRoleForVPCTransitGateway trusts the `transitgateway.amazonaws.com` service to assume the role.

Create the Service-Linked Role

You don't need to manually create the **AWSServiceRoleForVPCTransitGateway** role. Amazon VPC creates this role for you when you attach a VPC in your account to a transit gateway.

For Amazon VPC to create a service-linked role on your behalf, you must have the required permissions. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Edit the Service-Linked Role

You can edit the description of **AWSServiceRoleForVPCTransitGateway** using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Delete the Service-Linked Role

If you no longer need to use transit gateways, we recommend that you delete **AWSServiceRoleForVPCTransitGateway**.

You can delete this service-linked role only after you delete all transit gateway VPC attachments in your AWS account. This ensures that you can't inadvertently remove permission to access your VPC attachments.

You can use the IAM console, the IAM CLI, or the IAM API to delete service-linked roles. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

After you delete **AWSServiceRoleForVPCTransitGateway**, Amazon VPC creates the role again if you attach a VPC in your account to a transit gateway.

Limits for Your Transit Gateways

Your AWS account has the following limits related to transit gateways. To request a limit increase, use the Limits form.

- Total number of transit gateway attachments per Region per account: 5,000
- Number of transit gateways per Region per account: 5
- Number of transit gateway attachments per VPC: 5
- Number of transit gateway route tables per transit gateway: 20
- Number of routes per transit gateway route table: 10,000
- Maximum bandwidth per VPN connection[1]: 1.25 Gbps
- Maximum bandwidth (burst) per VPC connection: 50 Gbps

1:You can use ECMP to get higher VPN bandwidth by aggregating multiple VPN connections.

Document History for Transit Gateways

The following table describes the releases for transit gateways.

Feature	Description	Release Date
Initial release	This release introduces transit gateways.	26 November 2018