
Amazon VPC

AWS Cloud WAN



Amazon VPC: AWS Cloud WAN

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is AWS Cloud WAN?	1
Concepts	1
Getting started	4
Prerequisites	4
Steps to create your global and core network	4
Create a global network	5
Create a core network and core network policy	6
Create a core network while creating a global network	6
Create a core network after creating a global network	7
Create an attachment	7
Add a core network attachment using the command line or API	8
Add a Connect attachment	8
Add a Connect peer	9
Add a VPC attachment	10
Add a Site-to-Site VPN attachment	10
Register a transit gateway	11
Create a site	11
Add a device	12
Work with AWS Cloud WAN	13
Global and core networks	13
Global networks	13
Core networks	14
Create a core network policy version	15
Create a policy version using the AWS Cloud WAN console	15
Network configuration	16
Segments	17
Segment actions	17
Attachment policies	18
Create a policy version using the JSON editor	20
Core network policies	20
Update a core network policy version	21
Implement a policy version	21
Restore an out-of-date policy version	21
Delete a policy version	22
Download a policy	22
Core network policy parameters	23
Core network policy examples	28
Attachments	35
Viewing and editing attachments	35
Attachment acceptance	37
Delete attachments	38
Share a core network	38
Attachments on a shared core network	40
Tag core resources	41
Supported resources	42
Add or remove tags	42
Tag acceptance	43
Sites and links	43
Sites	43
Update or delete a site	44
Links	45
Devices	46
Update or delete a device	46
View details about a device	47

Visualize and monitor global and core networks	52
Global networks	52
Overview	52
Details	54
Topology graph	55
Topology tree	57
Core networks	58
Overview	59
Details	60
Sharing	61
Topology graph	61
Topology tree	62
Logical	64
Routes	65
Events	66
Monitoring	67
Visualize and monitor transit gateways	69
Transit gateway networks	69
Overview	69
Geography	71
Topology tree	71
Events	71
Monitoring	72
Route analyzer	73
Transit gateways	74
Overview	74
Topology tree	75
Events	75
Monitoring	76
On-premises associations	77
Connect peer	78
Tags	78
Security	80
Identity and access management	80
Condition keys	80
Tag core network resources	81
Supported resources	81
Events and metrics	82
Onboard CloudWatch Logs Insights	82
Monitor with CloudWatch Events	83
Topology changes	83
Route changes	84
Status updates	85
Policy updates	86
Segment update events	86
Monitor with CloudWatch metrics	87
View usage metrics for an edge location	87
Quotas	89
General	89
Bandwidth	90
Routing	90
Maximum transmission unit (MTU)	91

What is AWS Cloud WAN?

AWS Cloud WAN is a managed wide-area networking (WAN) service that you can use to build, manage, and monitor a unified global network that connects resources running across your cloud and on-premises environments. It provides a central dashboard from which you can connect on-premises branch offices, data centers, and Amazon Virtual Private Clouds (VPCs) across the AWS global network. You can use simple network policies to centrally configure and automate network management and security tasks, and get a complete view of your global network.

There are a number of ways you can work with AWS Cloud WAN to create and maintain your core network, policies, segments, and attachments:

- **AWS Management console**

The AWS Management console provides a web interface for you to create your global and core networks, policy versions, segments, and attachments. For more information on using the console to create and maintain your global and core networks, see [Getting started \(p. 4\)](#).

- **AWS Command Line Interface (AWS CLI)**

Provides command-line support for a broad set of AWS services using the command line. For more information see the [Amazon EC2 command line reference](#), which includes AWS Transit Gateway and Amazon VPC and the [Network Manager API reference](#).

- **AWS SDKs**

Provides language-specific API operations and takes care of a number of connection details, such as calculating signatures, handling request retries, and handling errors. For more information, see the [Network Manager API reference](#).

- **Query API**

Provides low-level API actions 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 handling errors. For more information, see the [Amazon EC2 API Reference](#).

AWS Cloud WAN concepts

The following are the key concepts for AWS Cloud WAN:

- **Global network**

A single, private network that acts as the high-level container for your network objects. A global network can contain both AWS Transit Gateways and other AWS Cloud WAN core networks. These can be seen in the Network Manager console.

- **Core network**

The part of your global network managed by AWS. This includes Regional connection points and attachments, such as VPNs, VPCs, and Transit Gateway Connects. Your core network operates in the Regions that are defined in your core network policy document.

- **Core network policy**

A core network policy document is a single document applied to your core network that captures your intent and deploys it for you. The core network policy is a declarative language that defines segments,

AWS Region routing, and how attachments should map to segments. With a core network policy, you can describe your intent for access control and traffic routing, and AWS Cloud WAN handles the configuration details. Some examples of advanced architectures that you can create with policy include creating a segment for shared services (for example, service directories or authentication services), providing internet access through a firewall for a segment, automatically assigning VPCs to segments based on tags, and defining which AWS Regions a segment is available in.

Over time you might find that you want to make adjustments or additions to your core network policy. With a policy, you can make any changes or additions to your core network and apply those changes through an updated JSON policy. You can do this using either the visual editor on the console, or through an included JSON editor. You can maintain multiple versions of a policy, although only one policy can be in effect. At any time, you can update your core network to use a new policy or revert to a previous version.

- **Attachments**

Attachments are any connections or resources that you want to add to your core network. Supported attachments include VPCs, VPNs, Transit Gateway route table attachments, and Connect attachments.

- **Core Network Edge**

The Regional connection point managed by AWS in each Region, as defined in the core network policy. Every attachment connects to a Core Network Edge. Under the hood, this is an AWS Transit Gateway, and it inherits many of the same properties.

In your core network policy document, you define the AWS Region where you want connectivity. At any time, you can add or remove AWS Regions using the policy document. For each AWS Region that you define in the policy document, AWS Cloud WAN then creates a Core Network Edge router in the specified Region. All Core Network Edges in your core network create full-mesh peering with each other to form a highly resilient network. Traffic across the AWS global network uses redundant connections and multiple paths.

- **Network segments**

Segments are dedicated routing domains, which means that by default, only attachments within the same segment can communicate. You can define segment actions that share routes across segments in the core network policy. In a traditional network, a segment is similar to a globally consistent Virtual Routing and Forwarding (VRF) table, or a Layer 3 IP VPN over an MPLS network.

AWS Cloud WAN supports built-in segmentation, which means that you can more easily manage network isolation across your AWS and on-premises locations. Using network segments, you can divide your global network into separate isolated networks. For example, you might want to isolate traffic between different parts of your business, such as between retail sites or IT networks.

You can create a segment and define whether resources that ask for access require approval. You can also define explicit route filters to be applied before those routes can be attached to a segment. Each attachment connects to one segment. Each segment will create a dedicated routing domain. You can create multiple network segments within your global network. Resources connected to the same segment can only communicate within the segment. Optionally, resources in the same segment can be isolated from each other, with access only to shared services. With segments, AWS maintains a consistent configuration across AWS Regions for you, instead of you needing to synchronize configuration across every device in your network.

- **Segment actions and attachment policies**

Segment actions define how routing works between segments. After you create a segment, you can choose to map attachments to the segments either by explicitly mapping a resource to a segment (for example, "VpcId: "vpc-2f09a348") or by creating and using attachment policies. Instead of manually associating a segment to each attachment, attachments are tagged. Those tags are then associated with the applicable segment. When attachments are mapped to segments, you can choose how routes are shared between segments. For example, you might want to share access to a VPN

across multiple segments, or allow access between two types of branch offices. You can also choose to configure centralized internet routing for a segment, or route traffic between segments through a firewall.

- **Core network owner and Attachment owner**

When creating a core network within a global network, the user that creates the core network automatically becomes the owner of the core network. A core network owner has full control and visibility over all parts of the AWS Cloud WAN network. The core network owner can then share a core network across accounts or across an organization using AWS Resource Access Manager. For more information, see [the section called "Share a core network" \(p. 38\)](#). The account to which the core network is shared becomes an attachment owner. An attachment owner has permission only to create connections, attachments, or tags, but no permission for any core network tasks. A core network owner can also be an attachment owner.

A core network owner can:

- Create, update, restore, delete, or share a Cloud WAN network.
- Create, update, download, run, delete, or restore core network policy versions.
- Create, update, or delete core network attachments.
- Accept or reject core network attachments.
- Create, update, or remove attachment tags.
- Visualize network topology and policy change sets.
- Track network events, routes, and performance.
- Create sites, links, devices, and other transit gateway associations.

An attachment owner can:

- Create, update, or delete VPC attachments.
- Add, update, or remove attachment tags.

Getting started with AWS Cloud WAN

To get started with AWS Cloud WAN, you first create your global network. Your global network contains all of your network resources, such as core networks, sites, devices, and attachments. During the creation process, you can choose to create your core network and core network policy simultaneously. Or you can choose to create the core network, and then create a policy at a later time. Creating a core network and policy creates the structure of your core network and implements it. Until you finish creating your core network and core network policy, you won't be able to do anything in your global network. After the structure is implemented, you can then add attachments, devices, or sites, and you can register existing transit gateways.

Prerequisites

There are no prerequisites for setting up AWS Cloud WAN. However, some features are not available to you unless you set them up in advance. These features are described in the following table:

Prerequisite	Description
Events and metrics	Before viewing events on the Events dashboard, you must complete a one-time setup that registers your events with CloudWatch Logs Insights. Until you register your events, you'll be unable to view any of your events on the dashboard. See the section called "Onboard CloudWatch Logs Insights" (p. 82) for the steps to register your events.
Transit gateways	<p>A transit gateway must first be created on the Amazon Virtual Private Cloud console at console.aws.amazon.com/vpc/home.</p> <p>Transit gateways that you have created in Amazon VPC can then be registered in AWS Cloud WAN to be part of your AWS Cloud WAN global network.</p>

Steps to create your global and core network

The following high-level steps provide links to the required and optional procedures for setting up the structure of your AWS Cloud WAN global and core network.

Step 1: [the section called "Create a global network" \(p. 5\).](#)

Step 2: [the section called "Create a core network and core network policy" \(p. 6\).](#)

Step 3: [the section called "Create an attachment" \(p. 7\).](#)

Step 4: (Optional) [the section called "Create a core network policy version" \(p. 15\).](#)

Step 5: (Optional) [the section called “Register a transit gateway” \(p. 11\).](#)

Step 6: (Optional) [the section called “Add a device” \(p. 12\).](#)

Step 7: (Optional) [the section called “Create a site” \(p. 11\).](#)

After getting your AWS Cloud WAN network set up, you can work with and modify any aspect of the network. Steps for working with your global and core network can be found in [Work with AWS Cloud WAN \(p. 13\)](#). For example, you can:

- Add new segments and implement an updated policy version.
- Add, edit, or remove attachments, devices, and sites.
- Add new resource tags to further help identify your network resources.
- View logical and topological trees of your global and core networks.

You can also view visualizations of your global and core networks as topological trees and logical diagrams, and you can monitor and track events. See [Visualize and monitor global and core networks \(p. 52\)](#) for the ways you can visualize and monitor your global and core networks.

Create a global network

The first step in setting up AWS Cloud WAN is to create a global network. A global network is a single, private network that acts as the high-level container for your network objects. A Global Network can contain both an AWS Transit Gateway and other Cloud WAN core networks. These will appear in the AWS Network Manager console. When you create a global network, you can create a core network at the same time. You can also choose to create a core network later on.

You can either create a global network using the AWS console or through the command line or API.

Before you can set up your core network, you must first set up your global network.

To create a global network using the AWS console

1. Open the AWS Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. Choose **Create global network**.
4. Enter a **Name** and **Description** for your global network.
5. (Optional) In **Additional settings**, add **Key** and **Value** tags that further help identify an Network Manager resource. To add multiple tags, choose **Add tag** for each tag that you want to add.
6. (Optional) Do one of the following:
 - Keep the **Add core network in your global network** check box selected, and then choose **Next** to set up your core network and policies. For detailed instructions, see [the section called “Create a core network while creating a global network” \(p. 6\)](#).
 - Set up your core network later on.
 1. Clear the **Add core network in your global network** check box, and then choose **Next** to review your global network details.
 2. Choose **Edit** for any detail that you want to change, and then choose **Create global network**.

The **Global networks** page appears with a confirmation box that your global network was created successfully. Later, when you're ready to add your core network, see [the section called “Create a core network after creating a global network” \(p. 7\)](#).

To create a global network using the command line or API

- [create-global-network](#)

Next step: [the section called “Create a core network and core network policy” \(p. 6\).](#)

Create a core network and core network policy

After you've created your global network, you can create a core network within your global network. When you create your core network, you also create the core network policy that deploys your network structure as it sets up the permissions. When the core network has been created, you can then create attachments within the network, and set up transit gateways and devices. At any time, you can also modify your policy and deploy a new version to better suit your business needs. For steps to create a new version of a policy, see [the section called “Create a core network policy version” \(p. 15\).](#)

Note

You can only have one core network for each of your global networks.

Create a core network while creating a global network

To create a core network while creating a global network

Prerequisite: [the section called “Create a global network” \(p. 5\).](#)

1. Create the core network. See [the section called “Create a global network” \(p. 5\).](#)
2. Under **Core network general settings**, enter a **Name** and **Description** to identify the core network.
3. (Optional) Choose **Additional settings** to add one or more **Key** and **Value** tags to help identify this network resource.
4. (Optional) Under **Core network policy settings**, set the beginning and ending **ASN range** (Autonomous System Number). Format the range as **xxxxx - xxxxx**.

Note

ASN is the Border Gateway Protocol (BGP) for the new core network. Valid ranges are **64512 - 65334** and **4200000000 - 4294967294**.

5. Choose the **Edge locations**. These are the Regions where your edges are located. You can have more than one edge location, but you must choose at least one. You can select multiple edge locations from the dropdown list.
6. Enter a **Name** to identify the segment. The name can include up to 100 alphanumeric characters. Blank spaces and hyphens are not allowed. For example, if this core network is going to be used for development work, you can name the segment **development**.
7. Choose **Next** to review the global network details. Choose **Edit** to make any changes.
8. Choose **Create global network**.

Your global network is created. The core network policy starts creating and deploying your core network.

Important

A core network is not deployed instantaneously after creation. It can sometimes take several minutes or longer to complete, depending on the number of edge locations. While the core network is being created, you can't create any attachments within your core network or create policy versions. To view the status of the deployment, in the navigation

pane, choose **Policy versions**. While the policy is being implemented, the **Change set state** is **Executing**. After the policy is implemented, the **Alias** is **LIVE**, and the **Change set state** changes to **Execution succeeded**.

9. After your policy is LIVE and the core network has been created, you can begin to add attachments to your core network. See [the section called "Create an attachment" \(p. 7\)](#).

Create a core network after creating a global network

To create a core network after creating a global network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. Choose the global link that doesn't have a core network assigned to it.
4. The **Core network** displays a message that the core network is not yet enabled. This indicates that there is no core network associated with the global network.
5. Choose **Create core network**.
6. On the **Create core network** page, enter an optional **Name** and **Description** for the core network. The name can include up to 100 alphanumeric characters.
7. (Optional) Under **Additional settings**, add one or more **Key** and **Value** tags to help identify this core network.
8. Choose the **Edge locations**. These are the Regions where your edges are located. You can have more than one edge location, but you must choose at least one. You can select multiple edge locations from the dropdown list.
9. Enter a **Segment name** and **Segment description** to identify the segment. The name can include up to 100 alphanumeric characters. Blank spaces and hyphens are not allowed. For example, if this core network is going to be used for development work, you can name the segment **development**.
10. Choose **Create core network**.
11. Your global network is created, and the core network policy starts creating and deploying your core network.

Important

A core network is not deployed instantaneously after creation. It can sometimes take several minutes or longer to complete, depending on the number of edge locations. While the core network is being created, you can't create any attachments within your core network or create policy versions. To view the status of the deployment, in the navigation pane, choose **Policy versions**. While the policy is being implemented, the **Change set state** is **Executing**. After the policy is implemented, the **Alias** is **LIVE**, and the **Change set state** changes to **Execution succeeded**.

12. After your policy is LIVE and the core network has been created, you can begin to add attachments to your core network. See [the section called "Create an attachment" \(p. 7\)](#).

Next step: [the section called "Create an attachment" \(p. 7\)](#).

Create an attachment

When you attach a VPC to a core network edge, you must specify one subnet from each Availability Zone to be used by the core network edge to route traffic. Specifying one subnet from an Availability Zone enables traffic to reach resources in every subnet in that Availability Zone. Limits mentioned on the [Transit Gateway attachment to VPC](#) page of the *Transit Gateway User Guide* applies also to core

network VPC attachments. You can only add attachments after your core network is deployed and the core network policy is in place.

You can work with core network attachments using the Amazon VPC Console or the command line or API.

Attachment states can be one of the following. Attachment states appear on the Attachments page of the AWS Cloud WAN console.

- **Creating** — Creation of an attachment is in process.
- **Deleting** — Deletion of an attachment is in process.
- **Pending network update** — Waiting for the connection of attachments to the core network.
- **Pending tag acceptance** — Waiting for the core network owner to review the tag change for an attachment.
- **Pending attachment acceptance** — Waiting for the core network owner to accept or reject an attachment.
- **Rejected** — The core network owner rejected the attachment.
- **Available** — The attachment is fully functional.

The following are the supported core network attachment types. The links take you to instructions for adding that attachment type by using the AWS Cloud WAN console:

- [Connect \(p. 8\)](#)
- [Connect peer \(p. 9\)](#)
- [VPC \(p. 10\)](#)
- [VPN \(p. 10\)](#)

Add a core network attachment using the command line or API

You can create a Connect, VPC, or VPN attachment using the command line or API.

To add a core network attachment using the command line or API

- Create a Connect attachment: [create-connect-attachment](#)
- Create a Connect peer: [create-connect-peer](#)
- Create a VPC attachment: [create-vpc-attachment](#)
- Create a VPN attachment: [create-vpn-attachment](#)

Next step: (Optional) [the section called “Create a core network policy version” \(p. 15\)](#).

Add a Connect attachment

You can create a transit gateway Connect attachment to establish a connection between a core network edge and third-party virtual appliances (such as SD-WAN appliances) running in Amazon VPC. A Connect attachment supports the Generic Routing Encapsulation (GRE) tunnel protocol for high performance, and the Border Gateway Protocol (BGP) for dynamic routing. After you create a Connect attachment, you can create one or more GRE tunnels (also referred to as Transit Gateway Connect peers) on the Connect attachment to connect the core network edge and the third-party appliance. You establish two BGP sessions over the GRE tunnel to exchange routing information. The two BGP sessions are for redundancy.

A Connect attachment uses an existing VPC attachment as the underlying transport mechanism. This is referred to as the transport attachment.

The Core Network Edge identifies matched GRE packets from the third-party appliance as traffic from the Connect attachment. It treats any other packets, including GRE packets with incorrect source or destination information, as traffic from the transport attachment.

Note

A Connect attachment must be created in the same AWS account that owns the core network.

To add a Connect attachment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link that for the core network you want to add an attachment to.
4. In the navigation pane, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **Name** identifying the attachment.
7. From the **Edge location** drop-down list, choose the location where the attachment is located.
8. Choose **Connect**.
9. From the **Connect attachment** section, choose the **Transport Attachment ID** that will be used for the Connect attachment.
10. (Optional) In the **Tags** section, add **Key** and **Value** tags to further help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
11. Choose **Create attachment**.

Add a Connect peer

You can create a Connect peer (GRE tunnel) for an existing Connect attachment. When you create the Connect peer, you must specify the GRE outer IP address on the appliance side of the Connect peer.

To add a Connect peer

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Choose an attachment with a resource type of **Connect**.
6. Choose the **Connect peer** tab.
7. Choose **Create Connect peer**.
8. Enter a **Name** to identify the Connect peer.
9. (Optional) For the **Core network GRE address**, enter the GRE outer IP address for the core network edge. By default, the first available address from the Inside CIDR block is used.
10. For the **Peer GRE address**, enter the GRE outer IP address for the Core Network Edge. By default, the first available address from the Inside CIDR block is used.
11. For **BGP Inside CIDR blocks IPv4**, enter the range of inside IPv4 addresses used for BGP peering. Use a /29 CIDR block from the 169.254.0.0/16 range.
12. (Optional) For **BGP Inside CIDR blocks IPv6**, enter the range of inside IPv6 addresses used for BGP peering. Use a /125 CIDR block from the fd00::/8 range.

13. For **Peer ASN**, specify the Border Gateway Protocol (BGP) Autonomous System Number (ASN) for the appliance. You can use an existing ASN that's assigned to your network. If you do not have one, you can use a private ASN in the 64512–65534 range.

The default is the same ASN as the core network edge. If you configure the **Peer ASN** to be different than the core network edge ASN (eBGP), you must configure `ebgp-multihop` with a time-to-live (TTL) value of 2.

14. (Optional) In the **Tags** section, add **Key** and **Value** pairs to further help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
15. Choose **Create Connect peer**.

Add a VPC attachment

When you attach a VPC to a core network edge, you must specify one subnet from each Availability Zone to be used by the core network edge to route traffic. Specifying one subnet from an Availability Zone enables traffic to reach resources in every subnet in that Availability Zone. For more information about limits to core network VPC attachments, see [Transit Gateway attachment to VPC](#) in the *Transit Gateway User Guide*.

To add a VPC attachment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link that for the core network you want to add an attachment to.
4. In the navigation pane, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **Name** identifying the attachment.
7. From the **Edge location** drop-down list, choose the location where the attachment is located.
8. Choose **VPC**.
9. In the VPC attachment section, choose **IPv6 support** if the attachment supports IPv6.
10. From the **VPC IP** dropdown list, choose the VPC ID to attach to the core network.
11. After choosing the VPC ID, you're prompted to choose the **Availability Zone** and **Subnet ID** in which to create the core network VPC attachment. The Availability Zones that are listed are those edge locations that you chose when you created your core network. You must choose at least one Availability Zone and subnet ID.
12. (Optional) In the **Tags** section, add **Key** and **Value** pairs to further help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
13. Choose **Create attachment**.

Add a Site-to-Site VPN attachment

To attach a Site-to-Site VPN connection to your core network edge, you must first create a Site-to-Site VPN connection with **Target Gateway Type** set to **Not Associated**. See [Creating an AWS Cloud WAN Site-to-Site VPN attachment](#) in the *AWS Site-to-Site VPN User Guide*.

Note

- Your Site-to-Site VPN must be attached to a core network before you can start configuring a customer gateway. AWS doesn't provision these endpoints until the Site-to-Site VPN is attached to the core network.

- A Site-to-Site VPN attachment must be created in the same AWS account that owns the core network.

To add a Site-to-Site VPN attachment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link that for the core network you want to add an attachment to.
4. In the navigation pane, choose **Attachments**.
5. Choose **Create attachment**.
6. Enter a **Name** identifying the attachment.
7. From the **Edge location** drop-down list, choose the location where the attachment is located.
8. Choose **VPN**.
9. From the **VPN attachment** section, choose the VPN ID to be used for the VPN attachment.
10. (Optional) In the **Tags** section, add **Key** and **Value** pairs to further help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
11. Choose **Create attachment**.

Register a transit gateway

Prerequisite: A transit gateway must first be created on the Amazon Virtual Private Cloud console at console.aws.amazon.com/vpc/home.

Transit gateways that you've created in Amazon VPC can be registered in AWS Cloud WAN to be part of your AWS Cloud WAN global network.

To register a transit gateway in AWS Cloud WAN

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Choose **Transit gateways**.
5. For **Select Transit Gateway**, choose the transit gateway that you want to register.
6. Choose **Register Transit Gateway**.

Next step: (Optional) [the section called "Create a site" \(p. 11\)](#).

Create a site

A site represents the physical location of your network, using location information. Sites are used in dashboard visualizations.

To create a site

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.

2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose **Create site**.
6. For **Name** and **Description**, enter a name and description for the site.
7. For **Address**, enter the physical address of the site, for example, New York, NY 10004.
8. For **Latitude**, enter the latitude coordinates for the site (for example, 40.7128).
9. For **Longitude**, enter the longitude coordinates for the site (for example, -74.0060).
10. (Optional) Under **Additional settings**, add one or more **Key** and **Value** tags to help identify this site.
11. Choose **Create site**.

Next step: (Optional) [the section called “Add a device” \(p. 12\)](#).

Add a device

Devices represent a physical or virtual appliance.

When you've created a device, you have options for further refining it. For more information on working with devices in AWS Cloud WAN, see [Working with devices \(p. 46\)](#).

To add a device

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose **Create Device**.
6. For **Name** and **Description**, enter a name and description for the device.
7. For **Model**, enter the device model number.
8. For **Serial number**, enter the serial number for the device.
9. For **Type**, enter the device type.
10. For **Vendor**, enter the name of the vendor, for example, **Cisco**.
11. For **Location type**, specify whether the device is located in a remote location (**On-premises, Data center/ Other Cloud Provider**) or in the **AWS Cloud**.

If you choose **AWS Cloud**, specify the location of the device within AWS:

- For the **Zone**, specify the name of an **Availability Zone, Local Zone, Wavelength Zone**, or an **Outpost**.
 - For the **Subnet**, specify the Amazon Resource Name (ARN) of the subnet (for example, `arn:aws:ec2:useast-1:111111111111:subnet/subnet-abcd1234`).
12. For **Address**, enter the physical location of the site (for example **New York, NY 10004**).
 13. For **Latitude**, enter the latitude coordinates for the site (for example, **40.7128**).
 14. For **Longitude**, enter the longitude coordinates for the site (for example, **-74.0060**).

Work with AWS Cloud WAN

With your global and core networks in place, you can modify and change different aspects of your global network and core networks.

Topics

- [Global and core networks \(p. 13\)](#)
- [Create a core network policy version \(p. 15\)](#)
- [Core network policies \(p. 20\)](#)
- [Attachments \(p. 35\)](#)
- [Share a core network \(p. 38\)](#)
- [Attachments on a shared core network \(p. 40\)](#)
- [Tag core resources \(p. 41\)](#)
- [Sites and links \(p. 43\)](#)
- [Devices \(p. 46\)](#)

Global and core networks

A core network owner can maintain all aspects of global and core networks, including viewing, deleting, and updating networks.

Global networks

View, edit, or delete any of your current global networks.

Topics

- [View and edit global network information \(p. 13\)](#)
- [Delete a global network \(p. 14\)](#)

View and edit global network information

To view details about a global network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Choose the **Details** tab.
5. On the **Details** page you can edit the following:
 - (Optional) To edit the description of your global network, in the **Details** section, choose **Edit**. In the **Description** field, enter a new description for your global network, and then choose **Edit global network**.
 - (Optional) To edit, add, or delete tags, in the **Tags** section, choose **Edit tags**.
 - To edit any current tag, change the **Key** or **Value** text as needed.
 - To add additional **Key** and **Value** tags, choose **Add tag** for each tag that you want to add.
 - To remove any existing tag, choose **Remove tag**.

Delete global networks.

Delete a global network

When you delete a global network, the deletion cannot be undone. Before you delete a global network, you must first delete any core networks that are associated with it. For more information on deleting core networks, see [the section called “Delete a core network” \(p. 14\)](#).

To delete a global network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Choose the **Details** tab.
5. On the **Details** page, choose **Delete**, and then confirm that you are deleting the global network.

Core networks

View, edit, or delete core networks.

Topics

- [View or edit core network information \(p. 14\)](#)
- [Delete a core network \(p. 14\)](#)

View or edit core network information

To view or edit details about a core network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. Choose the **Details** tab.
6. On the **Details** page, you can edit the following:
 - (Optional) To edit the description of your core network, in the **Details** section, choose **Edit**. In the **Description** field, enter a new description for your core network, and then choose **Edit core network**.
 - (Optional) To edit, add, or delete tags, in the **Tags** section, choose **Edit tags**.
 - To edit any current tag, change the **Key** or **Value** text as needed.
 - To add additional **Key** and **Value** tags, choose **Add tag** for each tag you want to add.
 - To remove any existing tag, choose **Remove tag**.

Delete a core network

When you delete a core network, the deletion cannot be undone. After you have deleted all core networks that are associated with a global network, you can then delete a global network. For more information on deleting global networks, see [the section called “Delete a global network” \(p. 14\)](#).

To delete a core network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. Choose the **Details** tab.
6. On the **Details** page, choose **Delete**, and then confirm that you are deleting the core network.

Create a core network policy version

You can create a core network policy version at any time from the console, using visual editor mode or JSON mode. When you create a policy version, you can configure settings that determine how your network works. When you create a new policy version, a change set of the proposed core network changes is added. You can then review the changes and implement the new core network and core network policy when you're ready.

When you create a new policy version, the policy version ID increments from the previous LIVE version. For example, if the current policy version ID is 1, and you create a new version of that policy, the new version is numbered 2. The latest version is displayed on the Policy versions screen with a **LATEST** status, indicating that the new policy is ready to implement.

Change set states can be any of the following:

- **Ready to execute** — A policy version change set and a new policy version have been created. This policy version was verified with no issues and is in a state where it can be implemented as the new LIVE policy. You can have multiple policy versions in this state, but you can only have one LIVE policy. When implemented, the policy change set state changes to **Execution succeeded**. For the steps to implement a policy change set state, see [the section called "Implement a policy version" \(p. 21\)](#).
- **Execution succeeded** — A policy version change set state was implemented as the new LIVE policy.
- **Out of date** — If you have multiple policy version change sets, any policy version that's older than the current LIVE policy is set to out-of-date, indicating that it's older than the LIVE policy. You can restore an out-of-date policy. For instructions, see [the section called "Restore an out-of-date policy version" \(p. 21\)](#).
- **Pending generation** — A policy version was created and is waiting to be generated. When the version has been generated, the change set state changes to **Ready to execute**.

You can create a core network policy version using either the AWS Cloud WAN console or by creating a JSON file.

- [the section called "Create a policy version using the AWS Cloud WAN console" \(p. 15\)](#)
- [the section called "Create a policy version using the JSON editor" \(p. 20\)](#)

Create a policy version using the AWS Cloud WAN console

Use the AWS Cloud WAN console to create a core network policy version following these tasks:

1. [Configure the network settings. \(p. 16\)](#)

2. [Create network policy segments within your core network.](#) (p. 17)
3. [Create segment sharing and segment route actions.](#) (p. 17)
4. [Create policy attachments.](#) (p. 18)

Network configuration

You can use the **Network configuration** page to configure the Border Gateway Protocol (BGP) Autonomous System Number (ASN) for your core network. The valid ranges are **64512 – 65534** and **4200000000 – 4294967294**. You can also configure the Inside CIDR blocks that are used for BGP peering on Connect peers. For more information on Transit Gateway Connect attachment and Connect peers, see the [Transit Gateway Connect](#) documentation. Using the network configuration, you can also configure the edge locations where you want the Core Network Edges to be available. At any time, you can add or remove edge locations through the network configuration.

To configure the network settings

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID that for the core network you want to create a policy version for, and then choose **Core network**.
4. In the navigation pane, choose **Policy versions**.
5. Choose **Create policy version**.
6. In **Choose policy view mode**, choose **Visual editor**.
7. The **Network configuration** displays general settings for the policy.
8. In **General settings**, choose **Edit**.
 1. The **Version** can't be changed for a policy version.
 2. Choose **VPN ECMP support** if the core network should forward traffic over multiple-cost routes using VPN.
 3. Choose **Edit general settings**.
9. In the **ASN ranges** section, do the following:
 1. Choose **Create**.
 2. For **ASN range**, enter the ASN range for the policy version. For example, enter **64512–65334**.
 3. Choose **Create ASN range**.
10. In the **Inside CIDR blocks** section, do the following:
 1. Choose **Create**.
 2. For **CIDR**, enter the CIDR block that you want to use for BGP peering on Connect peers.
 3. Choose **Create inside CIDR block**.
11. In the **Edge locations** section, do the following:
 1. Choose **Create**.
 2. From the **Location** dropdown list, choose the **Region** where you want the Core Network Edge router to be created. You can choose only one Region.
 3. For **ASN**, enter the ASN number for the Region.
 4. For **Inside CIDR block**, enter the CIDR block that you want to use for BGP peering on Connect peers. You can enter multiple CIDR blocks by choosing **Add** for each block that you want to add. Choose **Remove** for any block that you don't want.

Note

You can't leave any blank destination CIDR blocks. Choose **Remove** to delete any empty blocks.

5. Choose **Create edge locations**.
12. Next, add your **Segments**. For detailed instructions, see [the section called "Segments" \(p. 17\)](#).

Segments

You can use a network segment to divide your global network into separate isolated networks. On the segments page, you create a segment, and then define the attachment communication mapping. Each segment creates a dedicated routing domain. You can create multiple network segments within your global network. Resources that are connected to the same segment can only communicate within the segment. Optionally, you can also set resources in the same segment to be isolated from each other, with access only to shared services. With segments, AWS maintains a consistent configuration across AWS Regions for you, meaning that you don't need to synchronize configuration across every device in your network.

To configure a segment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID that for the core network you want to create a policy version for, and then choose **Core network**.
4. In the navigation pane, choose **Policy versions**.
5. Choose **Create policy version**.
6. Choose **Segments**.
7. In the **Segments** section, Choose **Create**.
8. Enter the **Segment name** and **Segment description** to identify the segment.
9. From the **Edge locations** dropdown list, choose one or more segments to create.
10. Choose **Require acceptance** if you require approval for attachments to be mapped to this segment.
11. Choose **Isolated attachments** if you need this segment isolated. Attachments in isolated segments can't communicate with other segments, and attachments in other segments can't communicate with the isolated segment.
12. For **Segment filter**, choose if you want to **Allow all** shared routes from other segments, **Allow selected** routes, or **Deny selected** routes.
13. Choose **Create policy**.

Segment actions

Segment actions allow you to optionally share your segments or create routes.

Segment sharing

Create a shared segment.

To create a shared segment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.

2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID that for the core network you want to create a policy version for, and then choose **Core network**.
4. In the navigation pane, choose **Policy versions**.
5. Choose **Create policy version**.
6. Choose **Segment actions**.
7. (Optional) In the **Sharing** section, choose **Create**, and then do the following:
 1. From the **Segment** dropdown list, choose the core network segment that you want to share.
 2. For the **Segment filter**, choose whether you want to allow all shared routes from other segments, to allow only selected routes, or to deny selected routes. The default is **Allow all**.
 3. Choose **Create sharing**.

Segment routes

Create a segment route for a policy version.

To create a segment route

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
 2. Choose **Get started**.
 3. On the **Global networks** page, choose the global network ID that for the core network you want to create a policy version for, and then choose **Core network**.
 4. In the navigation pane, choose **Policy versions**.
 5. Choose **Create policy version**.
 6. (Optional) In the **Routes** section, choose **Create**, and then do the following:
 1. From the **Segment** dropdown list, choose the core network segment that you want to share.
 2. For **Destination CIDR Block**, enter a static route. You can enter multiple CIDR blocks by choosing **Add** for each block that you want to add. Choose **Remove** for any blocks that you don't want.
- Note**
You can't leave any blank destination CIDR blocks. Choose **Remove** to delete any empty blocks.
3. Choose **Blackhole** if you want to "black hole" the route. If you make this choice, you can't add any attachments to the route.
 4. From the **Attachments** list, choose any attachments that you want to include in this route.
 5. Choose **Create segment route**.
 7. (Optional) Add **Attachment policies**. For more information, see [the section called "Attachment policies" \(p. 18\)](#).
 8. Choose **Create route**.

Attachment policies

Attachment policies control how your attachments map to your segments.

To create an attachment policy

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.

2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID that for the core network you want to create a policy version for, and then choose **Core network**.
4. In the navigation pane, choose **Policy versions**.
5. Choose **Create policy version**.
6. (Optional) Choose **Attachment policies**.
7. Choose **Create**.
8. For the **Rule number**, enter the rule number to apply to this attachment. Rule numbers determine the order in which rules are run.
9. Enter an optional **Description** to identify the attachment policy.
10. In the **Action** section, choose how you want to associate the attachment to the segment. Choose one of the following:
 - **Segment name** — associates the attachment by the segment name. After choosing this option, the segment to attach to from the **Attach to segment** dropdown list.
 - **Attachment tag value** — associates the attachment by the tag's value in a key-value pair. Enter the tag value in the **Attachment tag value** field.
11. Choose one of the following:
 - **Inherit segments acceptance value** if the attachment inherits the acceptance setting from a segment when a segment was created. This can't be changed.
 - **Requires attachment acceptance** if you require approval for attachments to be mapped to this segment.
 - If no acceptance option is chosen, attachments are automatically mapped to the segment.
12. (Optional) For **Condition logic**, further refine how the attachment is associated with the segment:
 - Choose **OR** — if you want to associate the attachment with the segment by either the **Segment name/Attachment tag value**, or by the chosen conditions.
 - Choose **AND** — if you want to associate the attachment with the segment by either the **Segment name/Attachment tag value** and by the chosen conditions.

If no acceptance option is chosen, attachments are automatically mapped to the segment.

13. In **Conditions**, set the condition logic by doing the following:
 1. From the **Type** dropdown list, choose one of the following condition types:
 - **Resource Id** — Set an **OR** or **AND** condition that uses a Resource ID.
 - **Attachment type** — Set an **OR** or **AND** condition that matches a specific attachment type.
 - **Account** — Set an **OR** or **AND** condition that matches an account.
 - **Tag name** — Set an **OR** or **AND** condition that matches a specific tag name.
 - **Tag value** — Set an **OR** or **AND** condition that matches a specific tag value.
 2. From the **Operator** dropdown list, choose the operator. The operator determines the relationship of the Type.
 - **Equals** — Filters results that match the passed **Condition value**.
 - **Not equals** — Filters results that do not match the passed **Condition value**. This option is not used for **Attachment type**.
 - **Begins with** — Filters results that start with the passed **Condition value**. This option is not used for **Attachment type**.
 - **Contains** — Filters results that match a substring within a string. This option is not used for **Attachment type**.
 - **Any** — Filters results that match any field. This option is not used for **Attachment type**.

3. In the **Condition values** field, enter the value that corresponds to the **Type** and **Operator**. This option is not used for **Attachment type**.
4. Choose **Add** to include additional conditions or choose **Remove** to delete any conditions.
14. Choose **Create attachment policy**.
15. Choose **Create policy**.

Create a policy version using the JSON editor

You can create a core network policy version by using the AWS Cloud WAN JSON editor. In the JSON editor, you add the parameters of your core network and policies. For a description of the required and optional parameters in the JSON file, see [the section called "Core network policy parameters" \(p. 23\)](#).

Note

Familiarity with creating JSON files is required.

To create a policy version using a JSON editor

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID that for the core network you want to create a policy version for, and then choose **Core network**.
4. In the navigation pane, choose **Policy versions**.
5. Choose **Create policy version**.
6. In **Choose policy view mode**, choose **JSON**.
7. In the JSON editor, create your new policy. For the required and optional parameters in your JSON policy, see [the section called "Core network policy parameters" \(p. 23\)](#).
8. Choose **Create policy**.

A new policy version is generated.

Next step: Optional: [the section called "Register a transit gateway" \(p. 11\)](#).

Core network policies

You can update, delete, or restore an out-of-date AWS Cloud WAN policy. You can also download a policy as a JSON file, and then edit the JSON file to create a new policy version. For examples of JSON policies, see [the section called "Core network policy examples" \(p. 28\)](#).

When you make an update to a policy version, it creates a new change set for that new policy version. When a change set has been created, you can then implement it as your new core network policy.

Topics

- [Update a core network policy version \(p. 21\)](#)
- [Implement a policy version \(p. 21\)](#)
- [Restore an out-of-date policy version \(p. 21\)](#)
- [Delete a policy version \(p. 22\)](#)
- [Download a policy \(p. 22\)](#)
- [Core network policy parameters \(p. 23\)](#)
- [Core network policy examples \(p. 28\)](#)

Update a core network policy version

Before deploying a new policy version, review the proposed change set.

To access a core network policy change set

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**, and then choose **Policy versions**.
5. Under **Policy version ID**, choose the policy version that you want to edit, and then choose **Edit**.
6. Change any information on the **Network configuration**, **Segments**, **Segment actions**, or **Attachment policies** tabs. For more information about creating policy versions, see [the section called "Create a core network policy version" \(p. 15\)](#).
7. Choose **Create policy**. This creates a new version of the policy. The policy version is incremented by 1 from the last version.

The **Change set state** of the new version is set to **Pending generation** on the Policy versions page, and the alias is set to **LATEST**, indicating that this is the most recent version of the policy. When a policy version has been generated, the **Change set state** changes to **Ready to execute**. You can then implement the new policy version as your **LIVE** policy. See [the section called "Implement a policy version" \(p. 21\)](#).

Implement a policy version

A policy version is never implemented automatically. After creating a version of a policy, you can implement the policy version as your new **LIVE** policy.

To implement a core policy version

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**, and then choose **Policy versions**.
5. Under **Policy version ID**, choose the policy version that you want to implement.
6. On the **Policy version - ID** page, review the details about the change set.
7. Choose **View or apply change set**. This creates a new version of the policy. The policy version is incremented by 1 from the last policy version.
8. On the Change set page, choose **Apply change set**.
9. The **Change set state** of the new policy is set to **Executing**, indicating that the chosen policy version is being implemented as the new LIVE policy. When finished, the change set state changes to **Execution succeeded**, and the **Alias** changes to **LIVE**. If any previous policies were in the **Ready to execute** change set state, those change to **Out of date**. This indicates that those policies are now considered older than the current LIVE policy.

Restore an out-of-date policy version

An out-of-date policy can be restored as a new version of a policy.

To restore an out-of-date policy version

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**, and then choose **Policy versions**.
5. Under **Policy version ID**, choose the out-of-date policy version that you want to restore and then choose **Restore**.

The Policy version ID is incremented by 1 from the last version listed on the **Policy versions** page, and the Change set state displays as **Pending generation**.

When generated, the change set state changes to **Ready to execute**, and the **Alias** changes to **LATEST**. If any previous policies were in the **Ready to execute** change set state, those change to **Out of date**. This indicates that those policies are now considered older than the **LATEST**.

Delete a policy version

Any policy except your current LIVE policy can be deleted.

To delete a core policy version

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**, and then choose **Policy versions**.
5. Under **Policy version ID**, choose the policy version that you want to delete and then choose **Delete**.
6. Confirm that you want to delete the policy version, and then choose **Delete** again.

Deleted policy versions are removed from the **Policy versions** page.

Download a policy

Download any policy version or your current LIVE policy as a JSON file.

To download a core policy

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**, and then choose **Policy versions**.
5. Under **Policy version ID**, choose the policy version that you want to download and then choose **Download**.

The policy downloads to your system as a JSON file. You can make changes to this JSON file as needed.

6. To submit a policy that was created outside of the AWS Cloud WAN, follow the preceding steps to go to the **Policy versions** page.
7. Choose **Create policy version**, and then choose **JSON**.
8. Copy the contents of your modified JSON file, and paste those contents into the AWS Cloud WAN JSON editor.
9. Choose **Create policy**.

A policy version is generated.

Core network policy parameters

The following sections describe the parameters that you use to create a core network policy version using JSON. Your JSON file contains two sections that describe the policy network settings and segments. You can then add two optional sections for defining segment actions and attachment policies.

For example JSON policies, see [the section called “Core network policy examples” \(p. 28\)](#).

Topics

- [core-network-configuration \(p. 23\)](#)
- [segments \(p. 24\)](#)
- [segment-actions \(p. 25\)](#)
- [attachment-policies \(p. 26\)](#)

core-network-configuration

The core network configuration section defines the Regions where a core network should operate.

For AWS Regions that are defined in the policy, the core network creates a Core Network Edge where you can connect attachments. After it's created, each Core Network Edge is peered with every other defined Region and is configured with consistent segment and routing across all Regions. Regions cannot be removed until the associated attachments are deleted. `core-network-configuration` is required.

Parameters

The following parameters are used in `core-network-configuration`:

- `asn-ranges` — The Autonomous System Numbers (ASNs) to assign to Core Network Edges. By default, the core network automatically assigns an ASN for each Core Network Edge but you can optionally define the ASN in the `edge-locations` for each Region. The ASN uses an array of integer ranges only from 64512 to 65534 and 4200000000 to 4294967294. No other ASN ranges can be used.
- `inside-cidr-blocks` — (Optional) The Classless Inter-Domain Routing (CIDR) block range used to create tunnels for AWS Transit Gateway Connect. The format is standard AWS CIDR range (for example, `10.0.1.0/24`). You can optionally define the inside CIDR in the Core Network Edges section per Region. The minimum is a /24 for IPv4 or /64 for IPv6. You can provide multiple /24 subnets or a larger CIDR range. If you define a larger CIDR range, new Core Network Edges will be automatically assigned /24 and /64 subnets from the larger CIDR. an Inside CIDR block is required for attaching Connect attachments to a Core Network Edge.
- `vpn-ecmp-support` — (Optional) Indicates whether the core network forwards traffic over multiple equal-cost routes using VPN. The value can be either `true` or `false`. The default is `true`.
- `edge-locations` — An array of AWS Region locations where you're creating Core Network Edges. The array is composed of the following parameters:
 - `location` — An AWS Region code, such as `us-east-1`.

- `asn` — (Optional) The ASN of the Core Network Edge in an AWS Region. By default, the ASN will be a single integer automatically assigned from `asn-ranges`.
- `inside-cidr-blocks` — (Optional) The local CIDR blocks for this Core Network Edge for AWS Transit Gateway Connect attachments. By default, this CIDR block will be one or more optional IPv4 and IPv6 CIDR prefixes auto-assigned from `inside-cidr-blocks`.

segments

The segments section defines the different segments in the network. Here you can provide descriptions, change defaults, and provide explicit Regional operational and route filters. The names defined for each segment are used in the segment-actions and attachment-policies section. Each segment is created, and operates, as a completely separated routing domain. By default, attachments can only communicate with other attachments in the same segment. `segments` is a required section.

Parameters

The following parameters are used in `segments`:

- `segments` — At least one segment must be defined, composed of the following parameters:
 - `name` — The name of the segment. The `name` is a string used in other parts of the policy document, as well as in the console for metrics and other reference points. Valid characters are a–z, and 0–9.

Note

There is no ARN or ID for a segment.

- `description` — (Optional) A user-defined string describing the segment.
- `edge-locations` — (Optional) Allows you to define a more restrictive set of Regions for a segment. The edge location must be a subset of the locations that are defined for `edge-locations` in the `core-network-configuration`. These locations use the AWS Region code. For example, you might want to use `us-east-1` as an edge location.
- `isolate-attachments` — (Optional) This Boolean setting determines whether attachments on the same segment can communicate with each other. If set to `true`, the only routes available will be either shared routes through the share actions, which are attachments in other segments, or static routes. The default value is `false`. For example, you might have a segment dedicated to development that should never allow VPCs to talk to each other, even if they're on the same segment. In this example, you would keep the default parameter of `false`.
- `require-attachment-acceptance` — (Optional) This Boolean setting determines whether attachment requests are automatically approved or require acceptance. The default is `true`, indicating that attachment requests require acceptance. For example, you might use this setting to allow a `sandbox` segment to allow any attachment request so that a core network or attachment administrator does not need to review and approve attachment requests. In this example, `require-attachment-acceptance` is set to `false`.
- `deny-filter` — (Optional) An array of segments that disallows routes from the segments listed in the array. It is applied only after routes have been shared in `segment-actions`. If a segment is listed in the `deny-filter`, attachments between the two segments will never have routes shared across them. For example, you might have a financial payment segment that should never share routes with a development segment, regardless of how many other share statements are created. Adding the `payments` segment to the `deny-filter` parameter prevents any shared routes from being created with other segments.
- `allow-filter` (optional) — An array of segments that explicitly allows only routes from the segments that are listed in the array. Use the `allow-filter` setting if a segment has a well-defined group of other segments that connectivity should be restricted to. It is applied after routes have been shared in `segment-actions`. If a segment is listed in `allow-filter`, attachments between the two segments will have routes if they are also shared in the `segment-actions` area. For example, you might have a segment named `video-producer` that should only ever share routes with a `video-distributor` segment, no matter how many other share statements are created.

Note

You can use either `allow-filter` or `deny-filter`, but you can't use both of them simultaneously. These are optional fields used to more explicitly control segment sharing. These parameters are not required in order to receive or send routes between segments.

segment-actions

`segment-actions` define how routing works between segments. By default, attachments can only communicate with other attachments in the same segment. You can use `segment-actions` to:

- `share` attachments across segments. Use the `share` action so that attachments from two different segments can reach each other. For example, if you've set a segment to `isolate-attachments`, the segment can't reach anything unless it has a `share` relationship with other segments. The `share` statement creates routes between attachments in the provided segments. If you're creating a `share` between one segment and an array of segments, the segment to share allows attachments from the segments in the array. However, sharing does not occur between the segments within the array. For example, if a segment named `shared-service` is defined as a segment with a `share-with` array of segments named `prod` and `prod2`, the network policy will allow the attachments in both `prod` and `prod2` to reach `shared-service`. But the network policy will not allow sharing of attachments between `prod` and `prod2`.
- `create-route` to define a static route in a segment.

Note

Sharing routes occurs between segments. All attachments connected to the same segment will share a similar routing behavior globally. If some attachments differ from other attachments in the same segment, those attachments should be within their own segments. This is intentional to prevent a proliferation of segments where one segment equals one attachment.

`segment-actions` is an optional section.

Parameters

The following parameters are used in `segment-actions`:

- `action` — The action to take for the chosen segment. The `action` must be either `share` or `create-route`. The following parameters are described for these actions.
- `share` parameters. If the action to take is `share`, the following parameters are required. `share` is the default action behavior.
 - `segment` — The name of the segment created in the `segments` section to share.
 - `mode` — `attachment-route` is the only supported value. This mode places the attachment and return routes in each of the `share-with` segments. For example, if there are static routes or routes shared from other segments, those will not be shared through the `attachment-route` mode.
 - `share-with` — An array of segments that will have reachability with the segment defined. The core network will create mutual advertisements between these `share-with` segments and the defined segment attachments.

For example, if you create a `share` between a segment named `shared-services` and `share-with` "A" and "B", this allows the attachments from "A" and "B" to reach "Shared services". "A" and "B" cannot reach each other, and any static routes or routes propagated from other segments are not shared among these segments.

Use `"` as a wild card to reference all segments instead of explicitly calling out segments individually.

- `except` — Explicitly exclude segments, typically used when sharing with `"`.

- `create-route` parameters. If the action is `create-route`, the following are the required and optional parameters.
 - `segment` — The name of the segment created in the `segments` section, which must be a static route. If you need to duplicate the static route in multiple segments, use multiple `create-route` statements.
 - `destination-cidr-blocks` — The static route to create. A segment should have the same routing behavior for a certain destination. This means if one Region has a route to a destination, other Regions should also have that route, but with potentially different paths. You can define the IPv4 and IPv6 CIDR notation for each AWS Region. For example, `10.1.0.0/16` or `2001:db8::/56`. This is an array of CIDR notation strings.
 - `destinations` — Defines the list of attachments to send the traffic to, with up to one `attachment-id` per Region. Because a segment is a global object, you should design your routing so that every AWS Region has an attachment in the `destinations` list. Regions that do not have attachments in this list will receive a propagated version of this route through cross-Region peering connections, and will use the static route of another Region. If multiple attachments are defined for a single Region, a single attachment will be chosen at random (deterministically random). Instead of an array of attachments, you can also provide a `blackhole`, which drops all traffic to the `destination-cidr-blocks`.
 - `description` — (Optional) A user-defined description to help further identify this route.

attachment-policies

In a core network, all attachments use the `attachment-policies` section to map an attachment to a segment. Instead of manually associating a segment to each attachment, attachments use tags, and then the tags are used to associate the attachment to the specified segment. A core network supports the following types of attachments:

- Transit Gateway Connect — `connect`
- VPC — `vpc`
- VPN — `site-to-site-vpn`

For example, to attach a VPC to a core network, either the VPC owner or the core network owner would create a core network attachment in the core network using either the AWS Cloud WAN console or the Network Manager `create-attachment` command line or API. The attachment itself will have tags analyzed by the attachment policy, and not the tags associated with the VPC resource. A tag on the attachment such as `"environment" : "development"` would then map to a development segment. Attachment policy rules can also use available metadata from within the conditions, such as `account ID`, `type of attachment`, the `resource ID` (for example, `vpc-id`), or the AWS Region.

Rules are assigned numbers for processing, and are processed in order by number, from lowest to highest. When a match is made, the action is taken and no further rules are processed. A single attachment can only be associated to a single segment. If no rules are matched (for example, there might be a misspelled tag value), the attachment won't be associated to a segment.

When an attachment matches a rule, the attachment attaches to the segment defined `segment`. Each attachment can either be associated without acceptance or require a separate action to approve the attachment association. By default, every segment requires all attachments to be accepted. The acceptance requirement can be turned off with `"require-attachment-acceptance" : false` in the segment definition. When `require-acceptance` is `false`, any attachment that maps to the segment is automatically added. For example, a developer `sandbox` segment might want to allow any attachment with the correct tag to be added to the network. With the `attachment-policies`, you can add additional controls on a per-rule basis. For example, if attachments from the `us-east-2` Region require acceptance but other Regions do not, you can set the `"require-acceptance" : true` setting on a rule that is specific to `us-east-2`.

You can apply multiple conditions using either `and` or `or` logic to create a single rule. For example, you can state that if the account is 111122223333 and includes the tag `"stage" : "development"` it should map to a specified segment. If you don't want to use tags to map attachments, you could use the `resource-id` to manually map each incoming connection to a segment. However, this approach requires changing the policy document every time new attachments are added and can reduce the operability of your current LIVE policy.

`attachment-policies` is an optional section.

Parameters

The following parameters are used in `attachment-policies`:

- `rule-number` — An integer from 1 to 65535 indicating the rule's order number. Rules are processed in order from the lowest numbered rule to the highest. Rules stop processing when a rule is matched. It's important to make sure that you number your rules in the exact order that you want them processed.
- `description` — (Optional) A user-defined description that further helps identify the rule.
- `condition-logic` — Evaluates a condition on either `and` or `or`. This is a mandatory parameter only if you have more than one condition. The conditions themselves are unordered, so the `condition-logic` applies to all of the conditions for a rule, which also means nested conditions of `and` or `or` are not supported. Use `or` if you want to associate the attachment with the segment by either the segment name or attachment tag value, *or* by the chosen conditions. Use `and` if you want to associate the attachment with the segment by either the segment name or attachment tag value *and* by the chosen conditions.
- `conditions` — An array composed of one of the four following types:
 1. `type` where the value is `any` — This matches any request. For example, you could use `any` if you're only using one segment that everything should map to. Or, you could use this as a fallback segment if you want all attachments that don't match a rule to map to a known segment.
 2. `type` where
 - `value` = `resource-id` | `account-id` | `region` | `attachment-type`
 - `operator` = `equals` | `not-equals` | `contains` | `begins-with`

This type is the value compared against the operator. For example, you might use the `condition type` in the following way:

- where the `resource-id` uses the resource associated with the attachment (for example, `vpc-1234567890123456`)
 - where the `account-id` uses the account ID of the requesting attachment (for example, `111122223333`)
 - where the `Region` uses the Region code for the requesting attachment (for example, `us-east-1`), and
 - where the `attachment-type` uses `vpc`, `site-to-site-vpn`, `connect`, or `transit-gateway-route-table` strings
3. `type` where the value is `tag-exists` — A string that matches against any of the keys defined on the attachment. Use this type when the value of the tag is not important, or if there is only a key without a value.
 4. `type` where the value is `tag-value` — Evaluates the following key value parameters:
 - `key` — A string that matches against any of the keys defined on the attachment. It must be an exact match of the key.
 - `operator` — The operation to perform against the key value. Must be one of `equals` | `not-equals` | `contains` | `begins-with`.
 - `value` — The value of the key to be evaluated for the operator.

In this example,

```
"type" : "tag-value",  
  
"key" : "project",  
  
"operator" : "begins-with",  
  
"value" : "sta"
```

Any condition where the value of `project` begins with `sta` is matched against the condition. This would return `staging`, `stage`, etc.

- **description** — A user-defined description to help further identify the attachment policy.
- **action** — The action to take when a condition is true.
 - **association-method** — Defines how a segment is mapped. Values can be `constant` or `tag`. `constant` statically defines the segment to associate the attachment to. `tag` uses the value of a tag to dynamically try to map to a segment.
 - **segment** — The name of the segment to share as defined in the `segments` section. This is used only when the `association-method` is `constant`.
 - **tag-value-of-key** — Maps the attachment to the value of a known key. This is used with the `association-method` is `tag`. For example a tag of `"stage" : "test"`, will map to a segment named `test`. The value must exactly match the name of a segment. This allows you to have many segments, but use only a single rule without having to define multiple nearly identical conditions. This prevents creating many similar conditions that all use the same keys to map to segments.
 - **require-acceptance** — Determines if this mapping should override the segment value for `require-attachment-acceptance`. You can only set this to `true`, indicating that this setting applies only to segments that have `require-attachment-acceptance` set to `false`. If the segment already has the default `require-attachment-acceptance`, you can set this to `inherit` segment's acceptance value.

Core network policy examples

This section provides example JSON AWS Cloud WAN policies. You can modify any of these examples for your own use. For a description of the required and optional parameters in the JSON file, see [the section called "Core network policy parameters" \(p. 23\)](#).

Topics

- [Example: One segment, one AWS Region \(p. 28\)](#)
- [Example: Two segments and multiple AWS Regions \(p. 29\)](#)
- [Example: Edge consolidation with isolated VPCs \(p. 30\)](#)
- [Example: Three-stage development environment using both tag values and manual shared services mapping \(p. 31\)](#)
- [Example: Distributed WAN without VPCs \(p. 32\)](#)
- [Example: Insert firewalls between on-premises and VPCs \(p. 34\)](#)

Example: One segment, one AWS Region

This policy sets up one network in `us-east-1` with the name `my-network`. Any attachment is automatically added to the network without requiring approval.

```
{  
  "version": "2021.12",
```



```
"core-network-configuration": {
  "asn-ranges": ["64512-65534"],
  "edge-locations": [
    {"location": "us-east-1"}
  ]
},
"segments": [
  {
    "name": "my-network",
    "require-attachment-acceptance": false
  }
],
"attachment-policies": [
  {
    "rule-number": 100,
    "condition-logic": "and",
    "conditions": [{ "type": "any" }],
    "action": {
      "association-method": "constant",
      "segment": "my-network"
    }
  }
]
}
```

Example: Two segments and multiple AWS Regions

This policy sets up two networks, Secured and Non-Secured, across three AWS Regions. Attachments with the tag "Network" : "Secured" map to "Secured", while attachments with the tag "Network" : "Non-Secured" map to "Non-Secured". All attachments require acceptance. Attachments can only talk within their segment but not across segments.

```
{
  "version": "2021.12",
  "core-network-configuration": {
    "asn-ranges": ["64512-65534"],
    "edge-locations": [
      {"location": "us-east-1"},
      {"location": "us-east-2"},
      {"location": "eu-west-1"}
    ]
  },
  "segments": [
    {"name": "secured"},
    {"name": "non-secured"}
  ],
  "attachment-policies": [
    {
      "rule-number": 100,
      "conditions": [{
        "type": "tag-value",
        "key": "Network",
        "value": "Secured",
        "operator": "equals"
      }],
      "action": {
        "association-method": "constant",
        "segment": "secured"
      }
    },
    {
      "rule-number": 200,
      "conditions": [{
```

```
        "type": "tag-value",
        "key": "Network",
        "value": "Non-Secured",
        "operator": "equals"
    }],
    "action": {
        "association-method": "constant",
        "segment": "non-secured"
    }
}
]
```

Example: Edge consolidation with isolated VPCs

This policy creates two segments, development and hybrid. If an attachment comes from a VPC, it will be mapped automatically to the development segment. VPCs that are attached to the development segment cannot talk to each other, and can talk only to the VPN. The development segment has a default route that points to the two attachments (one for each Region) and that routes all traffic back on-premises.

```
{
  "version": "2021.12",
  "core-network-configuration": {
    "asn-ranges": ["64512-65534"],
    "edge-locations": [
      {"location": "us-east-1"},
      {"location": "eu-west-1"}
    ]
  },
  "segments": [
    {
      "name": "development",
      "isolate-attachments": true,
      "require-attachment-acceptance": false
    },
    {"name": "hybrid"}
  ],
  "segment-actions": [
    {
      "action": "share",
      "mode": "attachment-route",
      "segment": "development",
      "share-with": ["hybrid"]
    },
    {
      "action": "create-route",
      "destination-cidr-blocks": ["0.0.0.0/0"],
      "segment": "development",
      "destinations": ["attachment-12355678901234567",
"attachment-23456789012345678"]
    }
  ],
  "attachment-policies": [
    {
      "rule-number": 10,
      "conditions": [
        {
          "type": "attachment-type",
          "operator": "equals",
          "value": "vpc"
        }
      ]
    }
  ],
}
```

```

        "action": {
          "association-method": "constant",
          "segment": "development"
        }
      },
      {
        "rule-number": 20,
        "conditions": [{
          "type": "attachment-type",
          "operator": "equals",
          "value": "vpn"
        }],
        "action": {
          "association-method": "constant",
          "segment": "hybrid"
        }
      }
    ]
  }
}

```

Example: Three-stage development environment using both tag values and manual shared services mapping

This policy creates a common software development lifecycle policy. It includes three development stages: development, testing, and production. VPCs in any one of these segments can't talk to each other because `isolate-attachments` is set to `true`. These VPC attachments are tagged with their stage, which directly maps to the name of the segment that they should belong to. If developers use the Development or Testing stages, the VPC is automatically mapped without approval, but Production requires approval. There is an additional `sharedservices` segment, which includes both a VPC and a site-to-site VPN. These attachments don't use tags, but are instead mapped by their explicit resource-id. The `sharedservices` segment is shared with the isolated development environments so that they can reach on-premises through VPN and can also reach the shared services VPC.

```

{
  "version": "2021.12",
  "core-network-configuration": {
    "asn-ranges": ["64512-65534"],
    "edge-locations": [
      {"location": "us-east-1"},
      {"location": "us-west-2"}
    ]
  },
  "segments": [
    {
      "name": "development",
      "isolate-attachments": true,
      "require-attachment-acceptance": false
    },
    {
      "name": "testing",
      "isolate-attachments": true,
      "require-attachment-acceptance": false
    },
    {
      "name": "production",
      "isolate-attachments": true,
      "require-attachment-acceptance": true
    },
    {"name": "shared-services"}
  ],
  "segment-actions": [
    {

```

```

        "action": "share",
        "mode": "attachment-route",
        "segment": "sharedservices",
        "share-with": "*"
    }
],
"attachment-policies": [
    {
        "rule-number": 1000,
        "conditions": [{
            "type": "tag-exists",
            "key": "Stage"
        }],
        "action": {
            "association-method": "tag",
            "tag-value-of-key": "Stage"
        }
    },
    {
        "rule-number": 1500,
        "conditions": [{
            "type": "resource-id",
            "operator": "equals",
            "value": "vpc-1234567890123456"
        }],
        "action": {
            "association-method": "constant",
            "segment": "sharedservices"
        }
    },
    {
        "rule-number": 1600,
        "conditions": [{
            "type": "resource-id",
            "operator": "equals",
            "value": "vpn-1234567890123456"
        }],
        "action": {
            "association-method": "constant",
            "segment": "sharedservices"
        }
    }
]
}

```

Example: Distributed WAN without VPCs

This network policy creates a network across four Regions for a global wide area network (WAN). This WAN has no connectivity to AWS workloads, and is using the AWS network only as transport between sites and for internet access for sales offices. The IoT network is still under security scrutiny, so attachments within the IoT segment cannot reach each other. However, in this example, SD-WAN has been deployed to the engineering sites and parts of the IoT network. Engineering needs direct access to the IoT network, which is currently a mixture of VPN and SD-WAN. In some cases, the SD-WAN network takes a direct route between sites. When crossing the engineering and IoT segments, it uses the AWS backbone as transport. Because the SD-WAN solution uses Transit Gateway Connect, there is a general pool assigned for Core Network Edge IP address pools. To reduce effort, the administrators allowed the Assign-to tag to define which segment the new attachments should be mapped to, but all attachments need to be approved (using the default value for require-attachment-acceptance).

```

{
  "version": "2021.12",
  "core-network-configuration": {

```

```
    "asn-ranges": ["64512-65534"],
    "inside-cidr-blocks": ["100.65.0.0/16"],
    "edge-locations": [
      {"location": "eu-central-1"},
      {"location": "us-west-2"},
      {"location": "us-east-1"},
      {"location": "eu-west-1"}
    ]
  },
  "segments": [
    {"name": "sales"},
    {"name": "testing"},
    {
      "name": "iot",
      "isolate-attachments": true
    },
    {"name": "internet"},
    {"name": "engineering"}
  ],
  "segment-actions": [
    {
      "action": "share",
      "mode": "attachment-route",
      "segment": "internet",
      "share-with": ["sales"]
    },
    {
      "action": "share",
      "mode": "attachment-route",
      "segment": "iot",
      "share-with": ["engineering"]
    },
    {
      "action": "create-route",
      "destination-cidr-blocks": ["0.0.0.0/0"],
      "segment": "sales",
      "destinations": [
        "attachment-12355678901234567",
        "attachment-23456789012345678",
        "attachment-35567890123456790",
        "attachment-4567890123456789a"
      ]
    }
  ]
},
  "attachment-policies": [
    {
      "rule-number": 1000,
      "conditions": [
        {
          "type": "tag-exists",
          "key": "Assign-to"
        }
      ],
      "action": {
        "association-method": "tag",
        "tag-value-of-key": "Assign-to"
      }
    }
  ]
}
```

Example: Insert firewalls between on-premises and VPCs

In this policy, the goal is to send all traffic from on-premises to AWS through a firewall. The customer has a VPC with a firewall (AWS Network Firewall, Gateway Load Balancer, or EC2/Marketplace offering) already configured in the VPC. The firewall is responsible for inspecting traffic from on-premises to AWS, and from AWS VPCs in the Internal-apps segment to the internet.

Similar to [Example: Edge consolidation \(p. 30\)](#), the VPC and VPNs are mapped to segments based on the attachment type. The one exception is the firewall VPC, which needs its own specific segment so that it can be shared separately with the other segments. In order to force the traffic coming in from the VPN to a firewall, static routes are configured that point to the firewall. In this case, the AWS VPCs in the Internal-apps segment are using the 172.16.0.0/16 CIDR space. All other private (RFC1918) space is advertised from the VPN connection. In this case, the policy uses the share and static-route options to define how each of the three segments receive the correct routes to send traffic through a middle box.

```
{
  "version": "2021.12",
  "core-network-configuration": {
    "asn-ranges": ["64512-65534"],
    "edge-locations": [
      { "location": "us-east-1"},
      { "location": "us-west-2"}
    ]
  },
  "segments": [
    { "name": "internal-apps"},
    { "name": "firewall"},
    { "name": "on-premises"}
  ],
  "segment-actions": [
    {
      "action": "create-route",
      "destination-cidr-blocks": ["0.0.0.0/0"],
      "segment": "internal-apps",
      "destinations": ["attachment-deadbeef901234567", "attachment-
eeeeee000000000000"],
      "description": "Send all internet headed on-premises through the firewall"
    },
    {
      "action": "create-route",
      "destination-cidr-blocks": ["0.0.0.0/0"],
      "segment": "on-premises",
      "destinations": [ "attachment-deadbeef901234567", "attachment-
eeeeee00000000000000"],
      "description": "Send all traffic received from the VPN through the firewall"
    },
    {
      "action": "share",
      "mode": "attachment-route",
      "segment": "firewall",
      "share-with": ["internal-apps", "on-premises"]
    }
  ],
  "attachment-policies": [
    {
      "rule-number": 500,
      "description": "We'll do our specific policies before we do attachment types.",
      "conditions": [{
        "type": "tag-value",
        "key": "core-network",
        "operator": "equals",
        "value": "firewall"
      }],
    }
  ]
}
```

```

        "action": {
            "association-method": "constant",
            "segment": "firewall"
        }
    },
    {
        "rule-number": 1000,
        "description": "Let's assume all VPCs are internal apps",
        "conditions": [{
            "type": "attachment-type",
            "operator": "equals",
            "value": "vpc"
        }],
        "action": {
            "association-method": "constant",
            "segment": "internal-apps"
        }
    },
    {
        "rule-number": 1500,
        "description": "Let's also assume all VPNs are from on-premises",
        "conditions": [{
            "type": "attachment-type",
            "operator": "equals",
            "value": "site-to-site-vpn"
        }],
        "action": {
            "association-method": "constant",
            "segment": "on-premises"
        }
    }
]
}

```

Attachments

You can modify or delete any of your core network attachments on the **Attachments** page by using either the AWS Cloud WAN console or the command line or API.

Viewing and editing attachments

This section describes viewing and editing your core network attachments either by using the console, or by using the command line or API.

Topics

- [Connect attachments \(p. 35\)](#)
- [Connect peer attachments \(p. 36\)](#)
- [VPC attachments \(p. 36\)](#)
- [Site-to-Site VPN attachments \(p. 37\)](#)
- [View and edit attachments using the command line or API \(p. 37\)](#)

Connect attachments

To view and edit a Connect peer attachment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.

2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for an attachment where the **Resource Type** is **Connect**. Details about the attachment are displayed, as well as any Connect peers and tags that are associated with the attachment. You can add new Connect peers and add, remove, or edit tags.
 - To add a new Connect peer attachment, see [the section called “Add a Connect peer” \(p. 9\)](#).
 - To add or edit attachment Tags, choose the **Tags** tab. The current list of tags associated with this attachment are displayed. Choose **Edit tags** to modify or delete current tags, and to add new tags.
6. Choose **Edit**.
7. On the Edit attachment page, you can edit the subnet configuration and the tags.
8. If you made any changes, choose **Edit attachment** to save the changes. The **Attachments** page displays along with a confirmation that the attachment was modified successfully.

Connect peer attachments

To view and edit a Connect peer attachment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for an attachment where the **Resource Type** is **Connect**. Details about the attachment are displayed in the lower part of the page. In this section, you can also edit the attachment Tags by choosing the **Tags** tab.
6. Choose **Edit**.
7. On the Edit attachment page, you can edit the subnet configuration and the tags.
8. If you made any changes, choose **Edit attachment** to save the changes. The **Attachments** page displays along with a confirmation that the attachment was modified successfully.

VPC attachments

To view and edit a VPC attachment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for an attachment where the **Resource Type** is **VPC**. Details about the attachment are displayed in the lower part of the page. In this section, you can also edit the attachment Tags by choosing the **Tags** tab.
6. Choose **Edit**.
7. On the Edit attachment page, you can edit the subnet configuration and the tags.
8. If you made any changes, choose **Edit attachment** to save the changes. The **Attachments** page displays along with a confirmation that the attachment was modified successfully.

Site-to-Site VPN attachments

To view and edit a Site-to-Site VPN attachment

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for an attachment where the **Resource Type** is **VPN**. Details about the attachment are displayed in the lower part of the page. You can add, remove, or edit the current attachment tags by choosing the **Tags** tab.
6. Choose **Edit**.
7. On the **Edit attachment** page, you can edit the subnet configuration and the tags.
8. If you made any changes, choose **Edit attachment** to save your changes. The **Attachments** page displays along with a confirmation that the attachment was modified successfully.

View and edit attachments using the command line or API

Use the command line or API to view and edit any of your core network attachments.

To view or edit a core network attachment using the command line or API

- For a Connect attachment, see [get-connect-attachment](#).
- For a Connect peer attachment, see [get-connect-peer](#).
- For a VPC attachment, see [get-vpc-attachment](#).
- For a Site-to-Site VPN attachment, see [get-site-to-site-vpn-attachment](#).

Attachment acceptance

When you create an attachment and associate it to a segment that requires an acceptance from the core network owner, the newly created attachment goes into a **Pending attachment acceptance** state. The core network owner has to review the attachment and choose to accept or reject the request.

To accept or reject an attachment using the console

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for the specific attachment that is in the **Pending attachment acceptance** state. Details about the attachment are displayed in the lower part of the page.
6. Choose **Accept** or **Reject**.
7. If you chose **Accept**, the attachment goes into a **Creating (Accept)** state. If you chose **Reject**, the attachment goes into a **Rejected (Reject)** state.

Delete attachments

You can delete any attachment from your core network. Deleted attachments can't be recovered. This section including the steps to delete an attachment using the AWS Cloud WAN console or by using the command line or API.

To delete an attachment using the console

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for the attachment that you want to delete.
6. Choose **Delete**.
7. Confirm that you want to delete the attachment by choosing **Delete** again.

The attachment is removed from the **Attachments** page.

Use the command line or API to delete any of your core network attachments.

To delete a core network attachment using the command line or API

- For a Connect, VPC, or Site-to-Site VPN attachment, see [delete-attachment](#).
- For a Connect peer attachment, see [delete-transit-gateway-connect-peer](#).

Share a core network

You can use AWS Resource Access Manager to share a core network across accounts or across your organization. By default, AWS Identity and Access Management (IAM) users do not have permission to create or modify AWS RAM resources. To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant permission to use specific resources and API actions. You then attach those policies to the IAM users or groups that require those permissions.

Only the network owner can perform the following operations:

- Create a resource share.
- Create a core network.
- Update a resource share.
- View a resource share.
- View the resources shared by your account, across all resource shares.
- View the principals with whom you're sharing your resources, across all resource shares. Viewing these principals provides you with the information to determine who has access to your shared resources.
- Delete a resource share.

You can perform the following operations on resources that are shared with you:

- Accept or reject a resource share invitation.
- View a resource share.

- View the shared resources that you can access.
- View a list of all of the principals that are sharing resources with you.
- Run the `describe-core-network` API. See [describe-core-network](#).
- Run the APIs that create, view, and delete VPC attachments:

Note

A shared core network supports only VPC attachments.

- Create a VPC attachment: [create-vpc-attachment](#)
- Get a VPC attachment: [get-vpc-attachment](#)
- Delete a VPC attachment: [delete-vpc-attachment](#)
- Leave a resource share.

When a core network is shared with an account, the account that accepts the shared core network can't make any changes to it, but it can create VPC attachments to the shared network.

Important

You must share your global resource from the N. Virginia (us-east-1) Region so that all other Regions can see the global resource.

To share a core network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Sharing** tab.
7. To create a resource share, choose **Share core network**.
8. In the **Resource sharing** field, choose an existing resource share.
9. For the **Available resource share**, choose the resource that you want to share, and then choose **Create resource share**.
10. If there are no resources available to share, you'll need to create a new resource share:
 1. Choose **Create resource share**. See [Create a resource share](#) in the *AWS RAM User Guide*.
 2. After creating the resource share in AWS RAM, return to the **Sharing** page of your core network.
 3. Choose the **Refresh** icon. The page updates to show the new resource share that you created.
 4. Choose the newly added resource.
11. Choose **Share core network**.

On the **Sharing** page, you can stop sharing any core network resource.

To stop sharing a core network share

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.

5. The **Overview** page opens by default.
6. Choose the **Sharing** tab.
7. To create a resource share, choose **Share core network**.
8. In the **Resource sharing** field, choose an existing shared resource.
9. Choose **Stop sharing**.

Attachments on a shared core network

When a core network owner shares their core network with your account, you are then able to create new VPC attachments for the shared core network, view the current attachments, and delete an attachment from the shared core network.

Important

A shared core network currently supports only VPC attachments.

To access attachments on a sharedcore network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Choose **Attachments shared by me**.
5. Choose **Create attachment**.
6. Enter a **Name** to identify the attachment.
7. From the **Core network** dropdown list, choose the core network that is shared with you and where you want to create the VPC attachment.
8. From the **Edge location** dropdown list, choose the location where the attachment is located.
9. In the **VPC attachment** section, choose **IPv6 support** if the attachment supports IPv6.
10. Choose the **VPC ID**. You're then prompted to choose the **Availability Zone** and **Subnet Id** in which to create the core network VPC attachment. The Availability Zones that are listed are those edge locations that you chose when you created your core network. You must choose at least one Availability Zone and subnet ID.
11. (Optional) In the **Tags** section, add **Key** and **Value** pairs to further help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
12. Choose **Create attachment**.
13. The **Attachment** page displays the following information about your shared attachments:
 - **Attachment ID**
 - **Name**
 - **Edge location**
 - **Resource Type**
 - **Resource ID**
 - **State**
 - **Core network**
 - **Core network status**
14. Choose **Create attachment** to create the new shared VPC attachment. See [the section called "Create an attachment" \(p. 7\)](#).

To view shared attachments

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Choose **Attachments shared by me**.
5. The **Attachment** page displays the following information about your shared attachments:
 - **Attachment ID**
 - **Name**
 - **Edge location**
 - **Resource Type**
 - **Resource ID**
 - **State**
 - **Core network**
 - **Core network status**
6. Select the check box for the specific attachment that you want to view. Details about the attachment are displayed on the lower part of the page.
7. You can edit some of attachment information:
 1. Choose the attachment, and then choose **Edit**.
 2. On the **Edit attachment** page, you can edit the subnet configuration and the tags.
 3. If you made any changes to update the VPC attachment, choose **Edit attachment**. The **Attachments** page displays a confirmation that the attachment was modified successfully.

To delete attachments from a shared core network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Choose **Attachments shared by me**.
5. Select the check box for the specific attachment that you want to delete, and then choose **Delete**.
6. Confirm that you want to delete the attachment by choosing **Delete** again. The attachment is removed from the **Attachments** page.

Tag core resources

A tag is a metadata label that either you or AWS assigns to an AWS resource. Each tag consists of a key and a value. For tags that you assign, you define the key and the value. For example, you might define the key as `purpose` and the value as `test` for one resource.

Tags help you do the following:

- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related.
- Control access to your AWS resources. For more information on controlling access to resources, see [Controlling access to AWS resources using tags](#) in the *AWS Identity and Access Management User Guide*.

Supported resources

The following core network resources support tagging:

- Core network
- Core network attachments
- Connect peer

For tagging support resources in Network Manager, see [Tag your Network Manager resources](#) in the *Network Manager User Guide*.

Add or remove tags

Tags have an important role in AWS Cloud WAN. In a core network, all attachments use the attachment policy to map an attachment to a segment. Instead of manually associating a segment to each attachment, you can add tags to attachments. You can then use the tags to associate the attachments to the desired segment as defined in the attachment policies. For example, a tag on an attachment that's labeled "segment": "development" would map to a "development" segment.

To add or update attachment tags

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for the specific attachment that you want to view or update. Details about the attachment are displayed in the lower part of the page. Choose the **Tags** tab.
6. Choose **Add/Update tags**.
7. Remove or add tags as needed.
 - To remove a tag, choose **Remove tag**, choose **Remove tag** for the tag you want to delete, and then choose **Edit tags**.
 - To add a tag, choose **Add tags**, and then choose **Add tag** to add a new key-value pair. Or edit the **Value** of any existing tag. Choose **Edit tags** when finished.

If the change that you made to the tags requires a tag acceptance from the core network owner, you will see the new proposed tags in the **Proposed Tags** tab.

To remove a tag

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for the specific attachment that you want to remove. Details about the attachment are displayed in the lower part of the page. Choose the **Tags** tab.
6. Choose **Remove tag**.
7. Choose **Edit tags** to save your changes.

8. If the removal of the tag requires acceptance from the core network owner, you will see the new proposed tags in the **Proposed Tags** tab.

Tag acceptance

When you add, update, or remove tags, and the result is a segment change that requires an acceptance from the core network owner, the attachment goes into a **Pending tag acceptance** state. The core network owner has to review segment changes for the attachment, and either accept or reject the request.

To accept or reject an attachment tag

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. Under **Core network** in the navigation pane, choose **Attachments**.
5. Select the check box for the specific attachment that's in a **Pending tag acceptance** state. Details about the attachment are displayed on the lower part of the page.
6. Choose **Accept or Reject**, and then choose **Accept or Reject** again to confirm and save your changes.

Sites and links

Use the AWS Cloud WAN console to manage the sites and links in your core network.

Topics

- [Sites](#) (p. 43)
- [Update or delete a site](#) (p. 44)
- [Links](#) (p. 45)

Sites

Use the AWS Cloud WAN console to manage the physical locations of your core network.

View details about a site

View details about a core network site using the AWS Cloud WAN console.

To access details about a site

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose the link that you want to see site details for.
6. The **General details** page provides information about the site.
7. Choose the **Devices** tab. This page displays information about the devices that are connected to the site. If you don't see a device listed, you'll need to add it. For more information on adding devices, see [the section called "Add a device" \(p. 12\)](#).

8. Choose the **Links** tab. This page displays the links that represent a connection from a device. If you don't see a link listed, you'll need to create the link. For the steps to create a link, see [the section called "Add a link" \(p. 45\)](#).
9. Choose the **VPNs** tab. This page displays site-related VPN information.
10. Choose the **Monitoring** tab. This page displays **Data In** and **Data Out** information for your links.
11. From the dropdown list, choose the link that you want to view information for.
12. (Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

Update or delete a site

Update or delete a core network site using the AWS Cloud WAN console.

To update a site

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose the site that you want to update, and then choose **Edit**.
6. On the **Edit site** page, you can make changes to the following information:

Note

You can't change the site **Name**.

- **Description**
 - **Address**
 - **Latitude**
 - **Longitude**
 - **Tags**
7. Choose **Edit site**.

To delete a site

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose the site that you want to delete, and then choose **Delete**.
6. Confirm that you want to delete the site by choosing **Delete** again.

Links

Links represent an internet connection from a device. A link is created for a specific site, and therefore you must create a site before you create a link. For the steps to create a site, see [the section called "Create a site" \(p. 11\)](#).

Add a link

Add a link to a device.

To add a link

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose the link **ID** of the site that you want to add a link to, and then choose the **Links** tab.

Note

Choose the link. Do not select the check box.

6. On the **Links** page, choose **Create link**.
7. For **Name** and **Description**, enter a name and description for the link.
8. For **Upload speed (Mbps)**, enter the upload speed in Mbps.
9. For **Download speed (Mbps)**, enter the download speed in Mbps.
10. (Optional) For **Provider**, enter the name of the service provider.
11. (Optional) For **Type**, enter the type of link, for example, **broadband**.
12. (Optional) Under **Additional settings**, add one or more **Key** and **Value Tags** to help identify this link.
13. Choose **Create link**.

Update or delete a link

Update or delete current links.

To update a link

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose the **Links** tab.
6. On the **Links** page, select the check box for the link that you want to update, and then choose **Edit**.
7. Modify any of the link settings as needed, including adding, editing, or removing tags.
8. Choose **Edit link**.

To delete a link

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.

2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Sites**.
5. Choose the **Links** tab.
6. On the **Links** page, select the check box for the link that you want to delete, and then choose **Delete**.
7. Confirm that you want to delete the link by choosing **Delete** again.

Devices

Update or delete devices using the AWS Cloud WAN console.

Update or delete a device

Update or delete a device using the AWS Cloud WAN console.

To update a device

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Select the check box of the device that you want to update, and then choose **Edit**.
6. Choose **Edit device**.
7. Add or update any of the following device information:
 - **Description**
 - **Model**
 - **Serial number**
 - **Type**
 - **Vendor**
 - **Location type**
 - **Latitude**
 - **Longitude**
 - **Tags**
8. Choose **Edit device**.

To delete a device

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Select the check box of the device that you want to delete, and then choose **Delete**.
6. Confirm that you want to delete the device by choosing **Delete** again.

View details about a device

View details of a device using the AWS Cloud WAN console.

To access details about a device

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the link that you want to see device details for.
6. Choose any of the following tabs to see more details:
 - the section called **"Overview"** (p. 47)
 - the section called **"Links"** (p. 48)
 - the section called **"On-premises associations"** (p. 48)
 - the section called **"Connect peer associations"** (p. 49)
 - the section called **"Connections"** (p. 49)
 - the section called **"VPNs"** (p. 50)
 - the section called **"Monitoring"** (p. 50)

Overview

The **Overview** page provides general details about the device. On this page you can associate or disassociate sites from the device, delete a device, or add, edit, or remove tags.

To associate a device with a site

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. On the **Overview** page, choose **Associate site**.
6. From the **Site Association** dropdown list, choose the site where the device is located.
7. Choose **Edit site association**.

The **Overview** page displays the site association in the **General details** section.

Remove the association of a device and a site.

To disassociate a site from a device

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. In the General details section of the Overview page, choose **Disassociate site**.

Note

There is no confirmation to delete the association.

Links

Associate a device with a link.

To associate a device with a link

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the device link that you want to create an association for.
6. Choose the **Links** tab.
7. Choose **Associate link**.
8. Choose the link that you want to associate with the site, and then choose **Create link**. If you do not see the link that you want, you'll need to create it. See [the section called "Add a link" \(p. 45\)](#)

Remove the association of a device and a link.

To disassociate a device from a link

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **Links** tab.
6. Choose the device link that you want to remove the association from.
7. Choose **Disassociate**.

On-premises associations

Create an on-premises association.

To create an on-premises association

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **On-premises associations** tab.
6. Choose **Associate**.
7. Choose the **Customer gateway**.
8. (Optional) Choose the **Link** for the connection from the device.
9. Choose **Create on-premises association**.

To disassociate an on-premises association

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **On-premises association** tab.
6. Choose the device link that you want to remove the association from.
7. Choose **Disassociate**.

Connect peer associations

Create a Connect peer association.

To create a Connect peer association

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **Connect peer** tab.
6. Choose **Associate**.
7. Choose the **Connect peer**.
8. (Optional) Choose the **Link** for the connection from the device.
9. Choose **Create Connect peer association**.

To disassociate a Connect peer association

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **Connect peer** tab.
6. Choose the device link that you want to remove the association from.
7. Choose **Disassociate**.

Connections

Create a device connection.

To create a device connection

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.

5. Choose the **Connections** tab.
6. Choose **Create connection**.
7. For **Name** and **Description**, enter a name and description for the connection.
8. (Optional) For **Link**, choose a link to associate with the first device in the connection.
9. For **Connected device**, choose the ID of the second device in the connection.
10. (Optional) For **Connected link**, choose a link to associate with the second device in the connection.
11. (Optional) In the **Tags** section, add **Key** and **Value** pairs to further help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
12. Choose **Create connection**.

To delete a device connection

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **On-premises association** tab.
6. Choose the device that you want to delete the connection for.
7. Choose **Delete**.

VPNs

The VPNs page displays a list of your VPN connections for a device.

To access device VPN connections

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the device that you want to view the VPN connections for.
6. Choose **VPNs**.

Monitoring

Monitor device events on the AWS Cloud WAN Monitoring page.

To access monitoring information

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Devices**.
5. Choose the **Monitoring** tab.
6. The **Monitoring** page displays data for the following:

- **Data In**

- **Data Out**
- **Tunnel down count Average**

(Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

Visualize and monitor global and core networks

The AWS Cloud WAN console uses dashboard visualizations to help you view and monitor all aspects of your global and core networks. Some of the dashboards include:

- World maps that pinpoint where your network resources are located, including edge locations, devices, and attachments.
- Monitoring data that uses CloudWatch Events to track 15-months' worth of statistics, giving you a better perspective on how your networks are performing.
- Event tracking that streams real-time events to an events dashboard.
- Topological and logical diagrams of your global and core networks.

There are separate dashboards for your global networks and for your core networks.

Topics

- [Visualize AWS Cloud WAN global networks \(p. 52\)](#)
- [Visualize AWS Cloud WAN core networks \(p. 58\)](#)

Visualize AWS Cloud WAN global networks

The AWS Cloud WAN console provides a dashboard where you can visualize and monitor your global network. It includes information about the resources in your global network, their geographic locations, the network topology, and the logical network associations.

Topics





- [Overview \(p. 52\)](#)
- [Details \(p. 54\)](#)
- [Topology graph \(p. 55\)](#)
- [Topology tree \(p. 57\)](#)

Overview

On the AWS Cloud WAN console **Overview** page, you can view the following information:

- Your global network resource inventory, which includes any core networks and transit gateway networks.
- The location of core network edges and transit gateways within your global network, displayed as icons on global map. Connections are shown between resources.

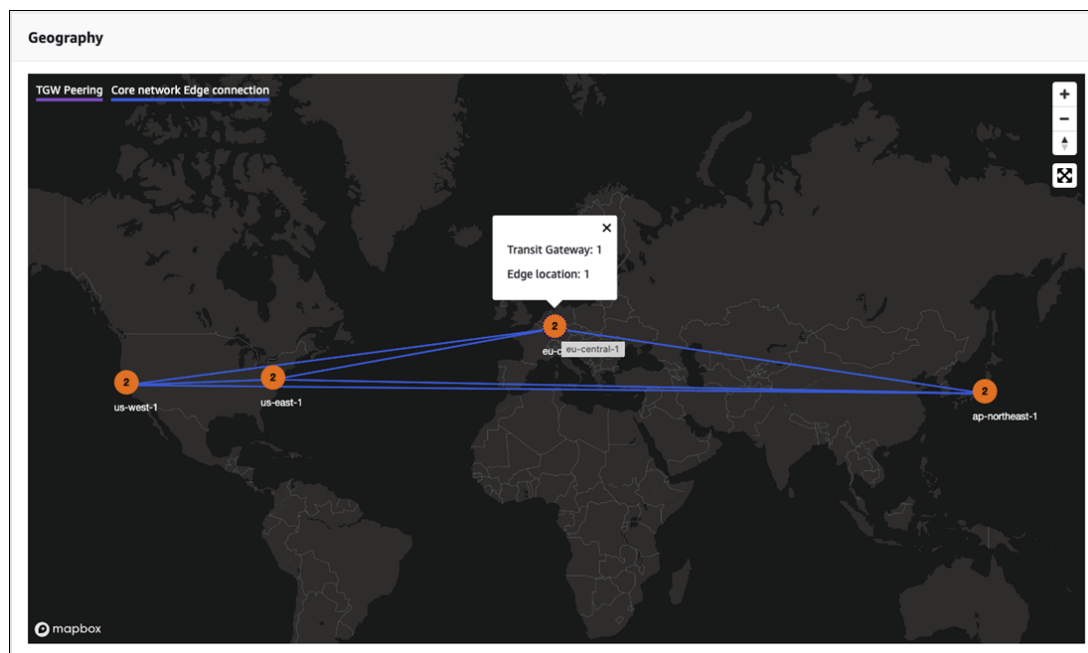
Use the following legend to understand the icons on your global network map:

Description
<p>Edge locations</p>  <p>The total number of edge locations in your global network. The number is shown in the Inventory section and as an icon on the map for each edge location in your global network.</p>
<p>Transit gateways</p>  <p>The total number of transit gateways in your global network. The number is shown in the Inventory section and as an icon on the map for each transit gateway in your global network.</p>
<p>Devices</p>  <p>The total number of devices in your global network. The number is shown in the Inventory section and as an icon on the map for each device in your global network.</p>
<p>Sites</p>  <p>The total number of sites in your global network. The number is shown in the Inventory section and as an icon on the map for each site in your global network.</p>

To access your global network resource inventory list

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Dashboard**.
5. The **Overview** page opens by default. This page shows information about the network resources in your global network:
 - The **Inventory** section shows the number of **Edge locations** in your global network, the number of **Transit gateways**, the number of **Devices**, and the number of **Sites**.

In the following example, you'll see that there are four Regions, **us-west-2**, **us-east-1**, **eu-central-1**, and **ap-northeast-1**. Some Regions are represented by a number (for example, **eu-central-1** is represented by the number 2.). This indicates that there are two network resources associated with that region. Choosing 2 opens a displays what those network resources are: one transit gateway and one edge location.



6. The **Details** page shows the add **Key** and **Value** pairs to further help identify this resource. You can add multiple tags by choosing **Add tag**, or remove any tag by choosing **Remove tag**.
7. Choose **Create attachment**.

Details

The **Details** page provides information about your global network resources. You can view information about your global network, as well as edit the Description, or add and remove tags.

To access global network details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Dashboard**.
5. Choose the **Details** tab.

The **Details** page shows the following information:








- **Name** — The name that you gave to the global network when you created it.
 - **State** — The current state of the network. Possible states are **Pending**, **Available**, **Deleting**, and **Updating**.
 - **Global network ARN** — The unique Amazon Resource Number (ARN) of the global network.
 - **AWS account** — The AWS account that's associated with the global network.
 - **Description** — The description given to the global network when it was created.
 - **Tags** — The key-value tags associated with the global network when it was created.
6. (Optional) Change the global network **Description**. Choose **Edit** in the **Details** section, and then in the **Description - optional** field, replace the current description with a new description. Then choose **Edit global network** to save your change.

7. (Optional) Edit, remove or add tags. In the **Tags** section, choose **Edit tags** and do any of the following. When finished, choose **Edit global network** to return to the **Details** page.
 1. Choose **Add tag** to add a new tag. Add **Key** and **Value** pairs to help identify this resource. You can add multiple tags.
 2. Choose **Remove tag** to delete any tag. You are not prompted to confirm the deletion.
 3. To edit an existing tag, enter the new **Key** or **Value** into the applicable field.

Topology graph

On the **Topology graph** page, you can view a topology diagram of your global network that includes core network and transit gateway networks. It includes information about AWS Regions, core network edges, transit gateways, segments, VPCs, VPNs, and Connect attachments. Icons represent specific resource types, and lines represent connections between resources. The line colors represent the state of the connection between AWS and the on-premises resources. You can filter the topology view to show specific segments and exclude AWS Regions and labels from being shown.

Use the following legend to understand the icons on your topology graph:

Description
 Core network edge The core network edges in your global network.
 Transit Gateway The transit gateways in your global network.
 VPC The VPC attachments in your global network.
 Connect The Connect attachments in your global network.
 Segment The segments in your global network.
 Devices The devices in your global network.
 Region The Regions in your global network.

To access the topology graph for a global network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Dashboard**.

5. Choose the **Topology graph** tab.

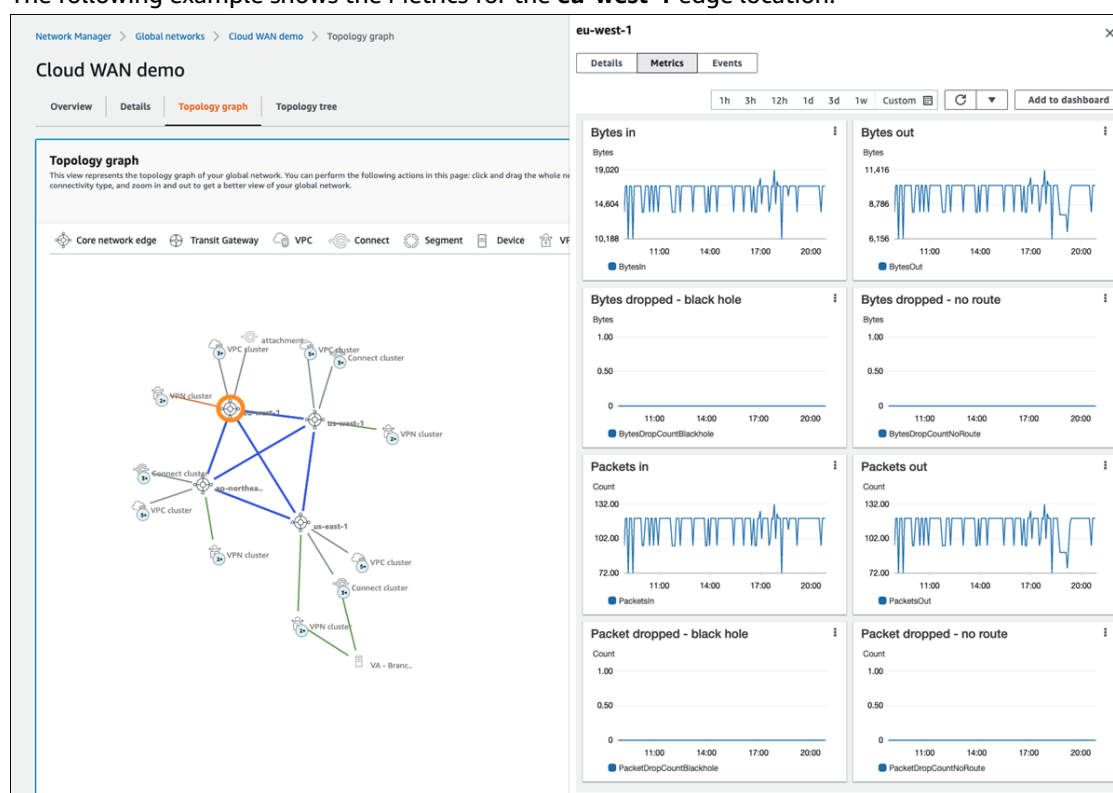
A topological representation of your global network is displayed. Connect lines are created between your resources.

6. (Optional) Filter the information that is displayed in the topology by making choices for any combination of the following:

- **Label** — Turns resource labels on or off.
- **Region** — Turns the display of a Region on or off.
- **Segment** — Turns the display Segments on or off.
- **Cluster** — Turns the display of clusters on or off.

7. On the **Topology graph**, choose any of your network resources to view details about that resource. A panel opens on the right-hand side of the graph.

The following example shows the Metrics for the **eu-west-1** edge location.



Depending on the resource chosen, the following information is available in the panel:

- **Core network edge** — **Details, Metrics, and Events.** See [Events and metrics \(p. 82\)](#) for more information about the types of events that can be tracked.
- **Transit Gateway** — **Transit Gateway details.**
- **VPC, Connect, and VPC** — **Attachment details.**
- **Segment** — **Segment details.**
- **Device** — **Device details.**
- **Region** — **Region details.**

Topology tree

The **Topology tree** page shows a logical diagram of your global network. Here you can view the network tree for your global network, which includes core network and transit gateway networks. By default, the page displays all resources in your global network and the logical relationships between them. You can filter the network tree to show specific on-premises resource types only. For example, the preceding image shows sites and devices, and excludes customer gateways. You can choose any of the nodes to view information about the specific resource that it represents. The line colors represent the state of the relationships between AWS and any on-premises resources.

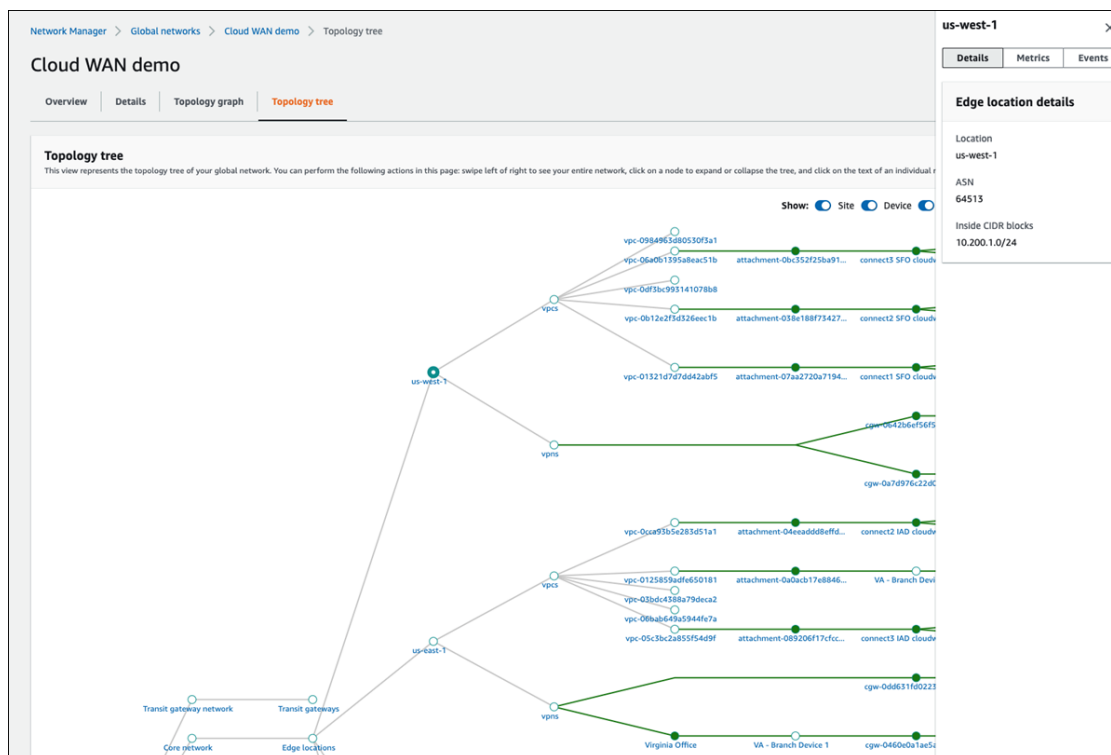
To access the topology tree for a global network

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Dashboard**.
5. Choose the **Topology tree** tab.

A logical representation of your global network is displayed, along with the details of your global network configuration.

6. (Optional) Filter the information that is displayed in the topology tree by making choices for any combination of the following:
 - **Site** — Turns the display of sites on or off.
 - **Device** — Turns the display of devices on or off.
 - **Customer gateway** — Turns the display of customer gateways on or off.
7. In the **Topology tree**, choose any of your network resources to view details about that resource. A panel opens on the right-hand side of the graph.

The following example shows the **Details** for the **us-west-1** edge location.



Depending on the resource chosen, the following information is available in the panel:

- **Edge locations** — **Details, Metrics, and Events.** See [Events and metrics \(p. 82\)](#) for more information about the types of events that can be tracked.
- **VPC, Connect, and VPC attachments** — **Attachment details.**
- **Transit Gateways** — **Transit Gateway details.**
- **Device** — **Device details.**
- **Sites** — **Site details.**

Visualize AWS Cloud WAN core networks

The AWS Cloud WAN console provides a dashboard where you can visualize and monitor your global network. It includes information about the resources in your global network, their geographic locations, the network topology, and the logical network associations.

Topics





- [Overview \(p. 59\)](#)
- [Details \(p. 60\)](#)
- [Sharing \(p. 61\)](#)
- [Topology graph \(p. 61\)](#)
- [Topology tree \(p. 62\)](#)
- [Logical \(p. 64\)](#)
- [Routes \(p. 65\)](#)
- [Events \(p. 66\)](#)
- [Monitoring \(p. 67\)](#)

Overview

On the AWS Cloud WAN console **Overview** page, you can view the following information:

- Your core network resource inventory.
- The location of core network edges and transit gateways within your global network, displayed as icons on a map. Connections are shown between resources.
- Throughput information between core network edges.
- The number of core network attachments per edge, shown as a stacked column chart. You can filter this chart to display specific attachment types.

Use the following legend to understand the icons on your core network map:

Description
 Edge locations The total number of edge locations in your core network. The number is shown in the Inventory section and as an icon on the map for each edge location in your core network.
 Segments The total number of segments in your core network. The number is shown in the Inventory section and as an icon on the map for each section in your core network.
 Devices The total number of devices in your core network. The number is shown in the Inventory section and as an icon on the map for each device in your core network.
 Sites The total number of sites in your core network. The number is shown in the Inventory section and as an icon on the map for each site in your core network.

To view the core network map

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. The **Inventory** section shows information about your core network: the number of **Edge locations** in your core network, the number of **Segments**, the number of **Devices**, and the number of **Sites**.
7. The **Geography** section displays a world map with the locations of your resources.
8. The **Throughput** section shows throughput information between the core network edges.
 - (Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

9. The **Attachment** section displays information about each attachment for each core network edge location. Choose the **Filter by attachment type** dropdown list. By default all attachment types are chosen. Clear the check box for any attachment type that you don't want to include in the graph. You can filter by any combination of:
 - **VPN**
 - **VPC**
 - **Connect**

Details

The **Details** page provides information about your core network resources.

To view your core network details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Details** tab.

The **Details** page shows the following information:

- **Name** — The name that you gave to the core network when you created it.
 - **State** — The current state of the core network. Possible states are **Pending**, **Available**, **Deleting**, and **Updating**.
 - **Core network ARN** — The unique Amazon Resource Number (ARN) of the core network.
 - **AWS account** — The AWS account that's associated with the core network.
 - **Description** — The description given to the core network when it was created.
 - **Tags** — The key-value tags that were associated with the core network when it was created.
7. (Optional) Change the core network **Description**. Choose **Edit** in the **Core network details** section, and then in the **Description** field, replace the current description with a new description. Then choose **Edit core network** to save your change.
 8. (Optional) Edit, remove or add Tags. In the **Tags** section choose **Edit tags** and do any of the following. When finished, choose **Edit core network** to return to the **Details** tab.
 1. Choose **Add tag** to add a new tag. Add **Key** and **Value** pairs to help identify this resource. You can add multiple tags.
 2. Choose **Remove tag** to delete any tag. You are not prompted to confirm the deletion.
 3. To edit an existing tag, enter the new **Key** or **Value** into the applicable field.

Sharing

On the **Sharing** page, you can view your currently shared network resources. You can also use AWS Resource Access Manager (RAM) to share a core network across accounts or across your organization in AWS organizations.

To view shared network resources

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Sharing** tab.







The **Resource sharing** page displays a list of the resources that you're currently sharing.

7. If you want to share a network resource. See [the section called "Share a core network" \(p. 38\)](#) for the steps to share a network resource.

Topology graph

On the **Topology graph** page, you can view a topology diagram of your core network that includes core network and transit gateway networks. It includes information about AWS Regions, core network edges, segments, VPCs, VPNs, and Connect attachments. Icons represent specific resource type and lines represent connections between resources. The line colors represent the state of the connection between AWS and the on-premises resources. You can filter the topology view to show specific segment, and exclude AWS Regions and labels that are shown.

Use the following legend to understand the icons on your core network topology graph:

Description
 Core network edge The core network edges in your network.
 VPC The VPC attachments in your core network.
 Connect The Connect attachments in your core network.
 Segment The segments in your core network.
 Devices The devices in your core network.
 VPN

Description
The VPN attachments in your core network.

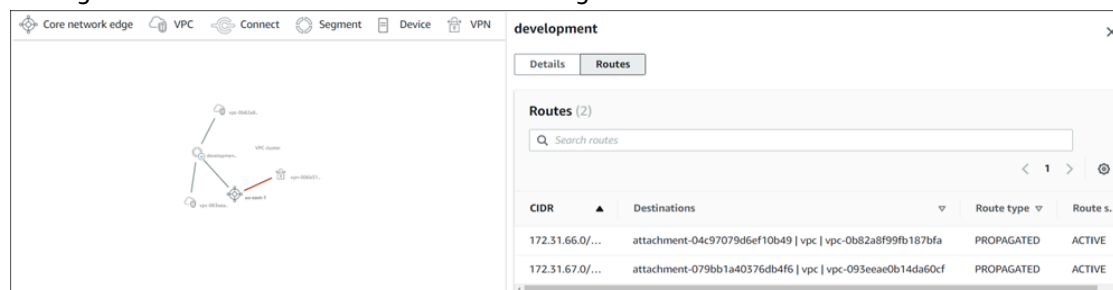
To view the core network topology graph

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Topology graph** tab.

A topological representation of your global network is displayed. Connect lines are created between your resources.

7. (Optional) Filter the information that is displayed in the topology by making choices for any combination of the following:
 - **Label** — Turns resource labels on or off.
 - **Segment** — Turns the display segments on or off.
 - **Cluster** — Turns the display of a Cluster on or off.
8. On the graph, choose any of your network resources to view details about that resource. A panel opens on the right-hand side of the graph.

In this example, the **development** segment is chosen in the graph. The panel displays **Details** about the segment. Choose the **Routes** tab to view the segment routes.



Depending on the resource chosen, the following information is available in the panel:

- **Core network edge** — **Details, Metrics, and Events**. See [Events and metrics \(p. 82\)](#) for more information about the types of metrics and events that can be tracked.
- **VPC, Connect, and VPN** — **Details and Events**.
- **Segment** — **Details and Routes**.
- **Device** — **Device Details**.

Topology tree

The **Topology tree** page shows a logical diagram of your core network. Here you can view the network tree for your core network. By default, the page displays all resources in your core network and the logical relationships between them. You can filter the network tree to show specific on-premises resource types only. For example, the preceding image shows sites and devices, and excludes customer

gateways. You can choose any of the nodes to view information about the specific resource it represents. The line colors represent the state of the relationships between AWS and the on-premises resources.

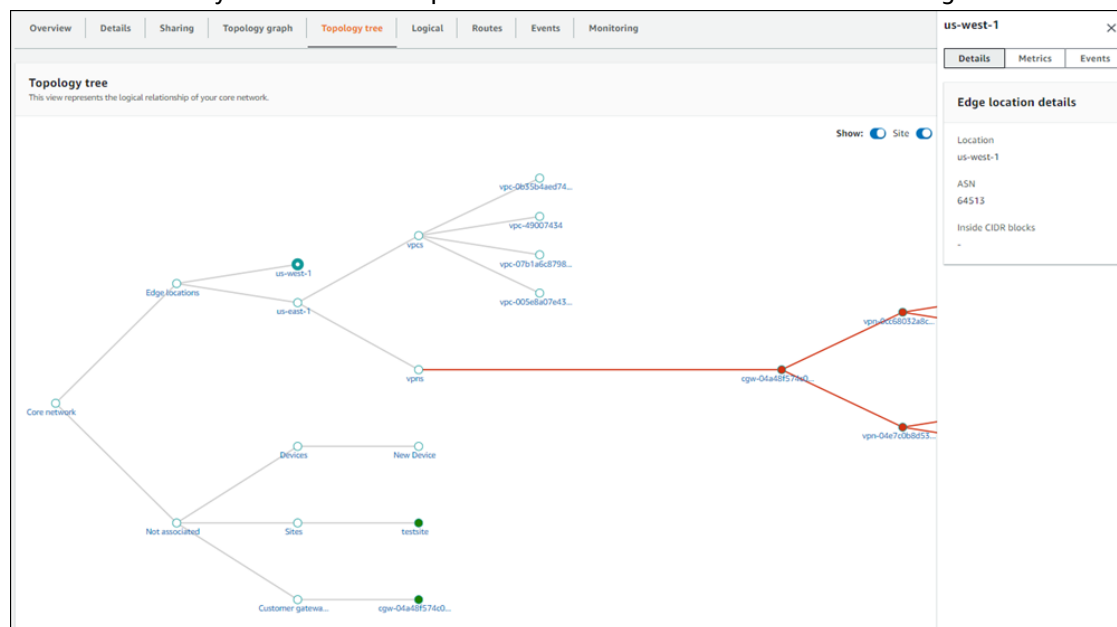
To view the topology tree

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Topology tree** tab.

A logical representation of your global network is displayed, along with the details of your global network configuration.

7. (Optional) Filter the information that is displayed in the topology by making choices for any combination of the following:
 - **Site** — Turns the display of sites on or off.
 - **Device** — Turns the display of devices on or off.
 - **Customer gateway** — Turns the display of customer gateways on or off.
8. On the tree, choose the label of any of your network resources to view details about that resource. A panel opens on the right-hand side of the tree.

In this example, an edge location, **us-west-1**, is chosen in the tree. The panel displays **Edge location details**. Choose any of the tabs in the panel to view more information about that edge location.







Depending on the resource chosen, the following information is available in the panel:

- **Attachments** — Attachment **Details** and **Events**. See [Events and metrics \(p. 82\)](#) for more information about the types of events that can be tracked.
- **Devices** — **Device details**.
- **Sites** — **Site details**.
- **Not associated** — There is no information to return.

Logical

The **Logical** page shows a logical representation of the segments in your core network. You can filter by a specific source or destination segment, or by a source or destination attachment. You can view the network tree for your global network, which includes core network and transit gateway networks. By default, the page displays all resources in your global network and the logical relationships between them. You can filter the network tree to show specific on-premises resource types only. For example, the preceding image shows sites and devices, and excludes customer gateways. You can choose any of the nodes to view information about the specific resource that it represents. The line colors represent the state of the relationships between AWS and any on-premises resources.

Use the following legend to understand the icons on your core network logical graph:

Description
 <p>VPC The VPC attachments in your core network.</p>
 <p>Connect The Connect attachments in your core network.</p>
 <p>Segment The segments in your core network.</p>
 <p>VPN The VPN attachments in your core network.</p>

To access the logical diagram for a core network

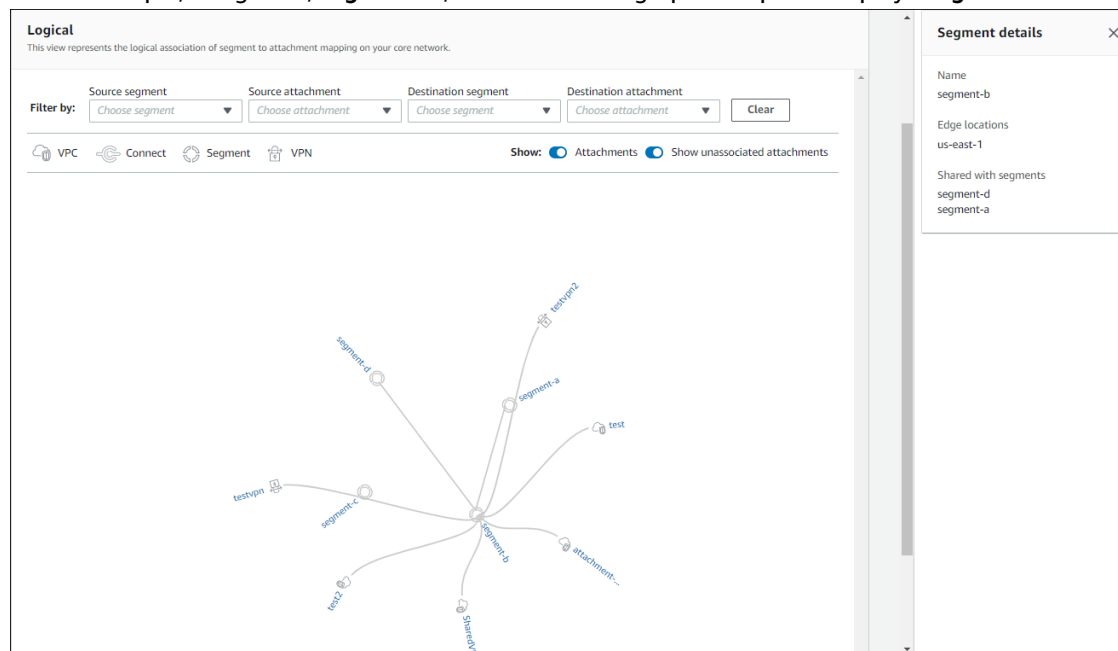
1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Logical** tab.

By default, all segments and all attachments are displayed in the logical representation.
7. (Optional) Do any of the following:
 - From the **Source segment** dropdown list, choose a segment from the core network.
 - From the **Source attachment** dropdown list, choose an attachment from the source segment.
 - From the **Destination segment** dropdown list, choose a destination segment from the core network.
 - From the **Destination attachment** dropdown list, choose an attachment from the destination segment.

The logical graph updates based on your choices. Choose **Clear** to reset the page.
8. (Optional) Filter the information that is displayed in the topology by making choices for any combination of the following:

- **Attachments** — Turns the display of attachments on or off.
 - **Show unassociated attachments** — Turns the display of unassociated attachments on or off.
9. On the graph, choose any of your network resources to view details about that resource. A panel opens on the right-hand side of the graph.

In this example, a segment, **segment-b**, is chosen in the graph. The panel displays **Segment details**.



Depending on the resource chosen, the following information is available in the panel:

- **VPC, Connect, and VPN** — **Details** and **Events**. See [Events and metrics \(p. 82\)](#) for more information about the types of events that can be tracked.
- **Segment** — **Segment details** and **Routes**.

Routes

On the **Routes** page, you can search for and view core network routes. On this page, you can refine results to show routes for specific segments and edge locations.

To access core network routes

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Routes** tab.
7. In the **Routes filter** section, do the following:
 - From the **Segment** dropdown list, choose a core network segment to filter on.
 - From the **Edge location** dropdown list, choose a core network edge location to filter on.

8. The **Routes** table updates to display the routes for the chosen segment and edge location and includes the following:
 - **CIDR** — All CIDRs used by this route.
 - **Destinations** — All destination addresses.
 - **Route types** — The type of route. This will be either **PROPAGATED** or **STATIC**.
 - **Route state** — The current state of a route. This will be either **ACTIVE** or **BLACKHOLE**.

Events

You can monitor your core network using CloudWatch Events, which delivers a near-real-time stream of system events that describe changes in your resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. For more information about CloudWatch Events, see the [Amazon CloudWatch Events User Guide](#).

Prerequisites: Before monitoring CloudWatch Events you must first onboard CloudWatch Logs Insights. This is a one-time process that needs to be completed at the account level. After this is set up for your core network, you'll be able to see event updates on this page. For more information on AWS Cloud WAN events, see [Events and metrics](#) (p. 82).

To access core network events

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Events** tab.

The **Events** section updates with the CloudWatch events that occurred during the selected time frame.

7. (Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

8. In the following example, the **Events** section shows two events occurring within a custom 15-month time frame:
 - A change set was executed successfully for a core network policy update.
 - An edge location was added to the core network.



For a full list of tracked events, see [the section called “Monitor with CloudWatch Events” \(p. 83\)](#).

Monitoring

You can monitor your core network by using Amazon CloudWatch, which collects raw data and processes it into readable, near-real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your network is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the [Amazon CloudWatch Events User Guide](#).

On the monitoring page you can view usage metrics for your core network, filtering by specific edge locations.

To access core network monitoring details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Monitoring** tab.
7. From the **Core network edge** dropdown list, choose the core network edge that you want to monitor.
8. (Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

9. The page updates the following monitors:
 - Bytes in
 - Bytes out
 - Bytes dropped – black hole
 - Bytes dropped – no route
 - Packets in
 - Packets out

- **Packets dropped – black hole**
- **Packets dropped – no route**

Visualize and monitor transit gateways

The AWS Cloud WAN console uses dashboard visualizations to help you view and monitor all aspects of your transit gateways and transit gateway networks. Some of the dashboards include:

- World maps that pinpoint where your transit gateway resources, such as VPNs, VPCs, sites, and devices are located.
- Monitoring data that uses CloudWatch Events to track 15-months' worth of statistics, giving you a better perspective on how your transit gateways are performing.
- Event tracking that streams transit gateway real-time events to an events dashboard.
- Topological and logical diagrams of your transit gateways.

There are separate dashboards for your transit gateway networks and for individual transit gateways.

Topics

- [Transit gateway networks \(p. 69\)](#)
- [Transit gateways \(p. 74\)](#)

Transit gateway networks

View dashboard information about transit gateways that are registered in AWS Cloud WAN.

Topics

- [Overview \(p. 69\)](#)
- [Geography \(p. 71\)](#)
- [Topology tree \(p. 71\)](#)
- [Events \(p. 71\)](#)
- [Monitoring \(p. 72\)](#)
- [Route analyzer \(p. 73\)](#)




Overview

The **Overview** page displays details about your transit gateways, their VPN, their Connect peer status, and any network events affecting your transit gateways.

To access transit gateway details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.

2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Transit Gateway network**.
5. The **Overview** page opens by default, showing information about your transit gateways.
6. On the **Overview** page, you can view the following information:
 - Your transit gateway **Inventory**:

Description
 Transit gateways The total number of registered transit gateways in. Choose the link to open the Transit gateways page to view more information about your transit gateways.
 Sites The total number of sites that are associated with your transit gateways. Choose the link to open the Sites page to view more information about your transit gateway sites.
 Devices The total number of devices that are associated with your transit gateways. Choose the link to open the Devices page to view more information about your transit gateway devices.

- **Transit gateways VPN status:**
 - **ID** — The ID of the transit gateway. Choose the link to open details about the transit gateway.
 - **Name** — The name of the transit gateway.
 - **Region** — The Region where the transit gateway is located.
 - **Down VPN** — The percentage of your total transit gateway VPNs that are down.
 - **Impaired VPN** — The percentage of your total transit gateways VPNs that are impaired.
 - **Up VPN** — The percentage of your total transit gateway VPNs that are up.
- **Transit gateways connect peer status:**
 - **ID** — The ID of the transit gateway.
 - **Name** — The name of the transit gateway.
 - **Region** — The Region where the transit peer is located.
 - **Down Connect peer** — The percentage of your total transit gateway Connect peers that are down.
 - **Impaired Connect peer** — The percentage of your total transit gateway Connect peers that are impaired.
 - **Up VPN** — The percentage of your total transit gateway Connect peers that are up.
- The **Network events summary** displays CloudWatch Events and the number of core network attachments per edge, shown as a stacked column chart.

(Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

Geography

The **Geography** page displays a world map showing the locations of your transit gateways.

To access transit gateway details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Transit Gateway network**.
5. The **Overview** page opens by default, showing information about your transit gateways.
6. Choose the **Geography** tab.

A world map displays, showing you the locations of the following:

- **AWS TGWs and VPCs.**
- The **Connectivity of VPNs, Direct Connects, and Connect peers.**
- **On-premises Sites and Devices.**
- **Not associated Sites and Devices.**

Topology tree

The **Topology tree** page shows a logical diagram of your transit gateways.

To access the topology tree for a transit gateway

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Transit Gateway network**.
5. The **Overview** page opens by default, showing information about your transit gateways.
6. Choose the **Topology tree** tab.
7. By default, the **Topology tree** page displays all **Sites, Devices, and Customer Gateways** of your transit gateway and the logical relationships between them. You can filter the network tree to show specific resource types to view information about the specific resource represented. The line colors represent the state of the relationships between AWS and the on-premises resources.

Events

Track your transit gateway events by using CloudWatch Events, which delivers a near-real-time stream of system events that describe changes in your resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. For more information about CloudWatch Events, see the [Amazon CloudWatch Events User Guide](#).

To track transit gateway events

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Transit Gateway network**.
5. The **Overview** page opens by default, showing information about your transit gateways.
6. Choose the **Events** tab.

The **Events** section updates with the CloudWatch transit events that occurred during the time frame.

(Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

Monitoring

You can monitor your transit gateways using Amazon CloudWatch, which collects raw data and processes it into readable, near-real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your network is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the [Amazon CloudWatch Events User Guide](#).

On the monitoring page you can view usage metrics for your transit gateways, filtering by specific transit gateways.

To access transit monitoring details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Transit Gateway network**.
5. The **Overview** page opens by default, showing information about your transit gateways.
6. Choose the **Monitoring** tab.
7. Choose a transit gateway that you want to monitor.
8. (Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

9. The page updates the following transit gateway monitors:
 - **Bytes in**
 - **Bytes out**
 - **Bytes dropped – black hole**
 - **Bytes dropped – no route**
 - **Packets in**
 - **Packets out**
 - **Packets dropped – black hole**
 - **Packets dropped – no route**
10. (Optional) Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option works only if your registered transit gateway is in the US West (Oregon) Region.

Route analyzer

The Route Analyzer analyzes the routing path between a specified source and destination.

Note

Route Analyzer checks the routes on Transit Gateway route tables only.

To analyze route information

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Transit Gateway network**.
5. The **Overview** page opens by default, showing information about your transit gateways.
6. Choose the **Route Analyzer** tab.
7. In the **Source** section, do the following:
 - Choose the source **Transit Gateway** for the route that you want to analyze.
 - Choose the source **Transit Gateway attachment** for the route.
 - Enter either the IPv4 or IPv6 **IP address**.
 - Clear the **Include return path in results** check box if you don't want to include a return path.
 - Indicate whether this is a **Middlebox appliance**. For more information on middlebox configurations, see [Route analysis with a middlebox configuration](#).
8. In the Destination section, do the following:
 - Choose the destination **Transit Gateway**.
 - Choose the destination **Transit Gateway attachment** for the route.
 - Enter either the IPv4 or IPv6 **IP address**.

9. Choose **Run route analysis**.
10. The Results of route analysis return the **Source** and **Destination** transit gateways and the current **Status**. An error message is returned if no information is found in the transit gateway route table. For more information on route tables, see [Transit gateway route tables](#).

Transit gateways

View dashboard information about transit gateways that are registered in AWS Cloud WAN.

Topics



- [Overview \(p. 74\)](#)
- [Topology tree \(p. 75\)](#)
- [Events \(p. 75\)](#)
- [Monitoring \(p. 76\)](#)
- [On-premises associations \(p. 77\)](#)
- [Connect peer \(p. 78\)](#)
- [Tags \(p. 78\)](#)




Overview

The **Overview** page displays details about your transit gateways, their VPN, their Connect peer status, and any network events affecting the transit gateway.

To view transit gateway details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link.
4. In the navigation pane, choose **Transit Gateways**.
5. On the **Transit gateways** page, choose the **ID** link that you want to view the dashboard for.
6. The **Overview** page opens by default.
7. On the **Overview** page, you can view the following sections:
 - The **Transit Gateway** details section displays the transit gateway **ID**, **Name**, **Region**, and **State**. Choose a different transit gateway to view those details.
 - The **Attachments** section shows the number of each resource attached to the transit gateway. The following legend describes the attachments:

Description
 The total number of VPCs attached to your transit gateway.
 The total number of VPNs attached to your transit gateway.

Description
 Direct Connect Gateways The total number of Direct Connect Gateways attached to your transit gateway.
 Connect The total number of Connect attachments on your transit gateway.
 Transit Gateway The total number of transit gateways.

- The **VPNs** section displays the **VPN ID**, **Device**, **Link**, **VPN status**, and **Tunnel status**.
- The **Connect peers** section displays the Connect peer **ID**, **Device**, **Link**, **Status**, and **BGP status**.
- The **Network events summary** displays CloudWatch Events and the number of core network attachments per edge, shown as a stacked column chart.

(Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

Topology tree

The **Topology tree** page shows a logical diagram of each AWS Transit Gateway.

To access the topology tree for a transit gateway

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link.
4. In the navigation pane, choose **Transit Gateways**.
5. On the **Transit gateways** page, choose the **ID** link that you want to view the dashboard for.
6. The **Overview** page opens by default.
7. Choose the **Topology tree** tab.
8. By default, the **Topology tree** page displays the **Sites**, **Devices**, and **Customer Gateways** of the chosen transit gateway and the logical relationships between them. You can filter the network tree to show specific resource types to view information about the specific resource represented. The line colors represent the state of the relationships between AWS and the on-premises resources.

Events

Track your transit gateway **Events** using CloudWatch Events, which delivers a near-real-time stream of system events that describe changes in your resources. Using simple rules that you can quickly set up,

you can match events and route them to one or more target functions or streams. For more information about CloudWatch Events, see the [Amazon CloudWatch Events User Guide](#).

To track transit gateway events

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link.
4. In the navigation pane, choose **Transit Gateways**.
5. On the **Transit gateways** page, choose the **ID** link that you want to view the dashboard for.
6. The **Overview** page opens by default.
7. Choose the **Events** tab.

The **Events** section updates with the CloudWatch transit events that occurred during the time frame for the chosen transit gateway.

(Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

Monitoring

On the **Monitor** page, monitor your transit gateways using Amazon CloudWatch, which collects raw data and processes it into readable, near-real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your network is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the [Amazon CloudWatch Events User Guide](#).

On the monitoring page, you can view usage metrics for your transit gateways, filtering by specific transit gateways.

To access transit monitoring details

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link.
4. In the navigation pane, choose **Transit Gateways**.
5. On the **Transit gateways** page, choose the **ID** link that you want to view the dashboard for.
6. The **Overview** page opens by default.
7. Choose the **Monitoring** tab.
8. Monitoring statistics display for the chosen transit gateway. Choose a different transit gateway to see those monitoring statistics.

9. (Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

10. The page updates the following transit gateway monitors:

- **Bytes in**
- **Bytes out**
- **Bytes dropped – black hole**
- **Bytes dropped – no route**
- **Packets in**
- **Packets out**
- **Packets dropped – black hole**
- **Packets dropped – no route**

11. (Optional) Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option works only if your registered transit gateway is in the US West (Oregon) Region.

On-premises associations

The **On-premises** page displays information about your on-premises devices for this transit gateway. On this page you can associate or disassociate any of your devices..

To access transit gateway on-premises associations

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link.
4. In the navigation pane, choose **Transit Gateways**.
5. On the **Transit gateways** page, choose the **ID** link that you want to view the dashboard for.
6. The **Overview** page opens by default.
7. Choose the **On-premises associations** tab.
8. The **Transit Gateway** on-premises association page displays the **Customer gateway**, **Device**, **Link**, and **State** of the transit gateway.

To associate a device

1. Choose the **Customer gateway** that you want to associate a device with.
2. Choose **Associate**.
3. On the **Edit on-premises association** page, choose the **Device** and optional **Link** for the association.

4. Choose **Edit on-premises association**.

To disassociate an on-premises device

1. Choose the **Customer gateway** that you want to disassociate.
2. Choose **Disassociate**.

Connect peer

The Connect peer page displays information about your associated Connect peers for this transit gateway. On this page you can disassociate any of your devices.

To access on-premises associations

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link.
4. In the navigation pane, choose **Transit Gateways**.
5. On the **Transit gateways** page, choose the **ID** link that you want to view the dashboard for.
6. The **Overview** page opens by default.
7. Choose the **Connect peer associations** tab.
8. The **Connect peer associations** page displays the **Connect peer**, **Device**, **Link**, and **State** of the transit gateway.

To disassociate a Connect peer device

1. Choose the **Connect peer** that you want to disassociate.
2. Choose **Disassociate**.

Tags

The **Tags** page displays the tags that are associated with the transit gateway. You can edit any of your transit gateway tags.

Note

Editing transit gateway tags is done through the Amazon Virtual Private Cloud console at console.aws.amazon.com/vpc/home.

To view transit gateway tags

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network link.
4. In the navigation pane, choose **Transit Gateways**.
5. On the **Transit gateways** page, choose the **ID** link that you want to view the dashboard for.
6. The **Overview** page opens by default.
7. Choose the **Tags** tab.
8. A list of the transit gateway key-value tags is displayed.

9. To add, edit, or delete any tags, choose **Edit tags** to open the Amazon Virtual Private Cloud console at console.aws.amazon.com/vpc/home. See [Add or edit tags for a transit gateway](#) in the *AWS Transit Gateway User Guide* for the steps to add or edit transit gateway tags.

AWS Cloud WAN security

AWS Cloud WAN uses service-linked roles for the permissions that it requires to call other AWS services on your behalf. For more information on the Network Manager service-linked role, see [service-linked role](#) in the *Transit Gateway User Guide*.

Identity and access management for AWS Cloud WAN

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use AWS Cloud WAN resources. IAM is an AWS service that you can use with no additional charge. You can use features of 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 global network, and perform tasks, you must:

- Create an IAM policy that grants the IAM user permission to use the specific resources and API actions they need
- Attach the policy to the IAM user or to 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 user permissions to perform the specified tasks on the specified resources.

Important

If you grant access to a global network you grant access to all AWS service data associated with the core network edges across all AWS Regions. For more information, see [Identity and access management for Transit Gateway Network Manager](#) in the *Transit Gateway User Guide*.

Condition keys

The `Condition` element (or Condition block) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can build conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. For more information, see [IAM JSON policy elements: Condition operators](#) in the *AWS Identity and Access Management User Guide*.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name.

You can attach tags to AWS Cloud WAN resources or pass tags in a request to Cloud WAN. To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys. See [IAM JSON policy elements: Condition](#) in the *AWS Identity and Access Management User Guide* for more information.

To see all AWS global condition keys, see [AWS global condition context keys](#) in the *AWS Identity and Access Management User Guide*.

AWS Cloud WAN supports the following condition keys:

- `networkmanager:vpcArn` — Filters access by which VPC can be used to create or update an attachment.
- `networkmanager:subnetArns` — Filters access by which VPC subnets can be added or removed from a VPC attachment.
- `networkmanager:vpnConnectionArn` — Filters access by which site-to-site VPN can be used to create or update an attachment.

For more information see the following:

- For information on supported condition keys, see [Identity and access management](#) in the *Transit Gateway User Guide*.
- For example policies to manage, see [Example policies to manage](#) in the *Transit Gateway User Guide*.

Tag core network resources

A tag is a metadata label that either you or AWS assigns to an AWS resource. Each tag consists of a key and a value. For tags that you assign, you define the key and the value. For example, you might define the key as `purpose` and the value as `test` for one resource. Tags help you do the following:

- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related.
- Control access to your AWS resources. For more information, see [Controlling access to AWS resources using tags](#) in the *AWS Identity and Access Management User Guide*.

Supported resources

The following core network resources support tagging:

- Core network
- Core network attachments
- Connect peer

For tagging supported resources, see [Tag your Network Manager resources](#) in the *Transit Gateway User Guide*.

AWS Cloud WAN Events and metrics

AWS provides the following monitoring tools to watch the resources in your global network, report when something is wrong, and take automatic actions when appropriate.

- *Amazon CloudWatch* monitors your AWS resources and the applications that you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For more information, see the [Amazon CloudWatch User Guide](#).
- *Amazon CloudWatch Events* delivers a near-real-time stream of system events that describe changes in AWS resources. CloudWatch Events enables automated event-driven computing, as you can write rules that watch for certain events and then trigger automated actions in other AWS services when these events happen. For more information, see the [Amazon CloudWatch Events User Guide](#).

You must first onboard CloudWatch Logs Insights before you can view Events on the AWS Cloud WAN dashboards. See [the section called “Onboard CloudWatch Logs Insights” \(p. 82\)](#) for the onboarding steps.

Topics

- [Onboard CloudWatch Logs Insights \(p. 82\)](#)
- [Monitor with CloudWatch Events \(p. 83\)](#)
- [Monitor with CloudWatch metrics \(p. 87\)](#)

Onboard CloudWatch Logs Insights

Before viewing events on the Events dashboard, you must complete a one-time setup that registers your events with CloudWatch Logs Insights. Until you register your events, you'll be unable to view any of your events on the dashboard.

To onboard CloudWatch Logs Insights

Before you begin, verify that an AWS Identity and Access Management (IAM) principal in your account, such as an IAM user, has the appropriate permissions to onboard to CloudWatch Logs Insights. Ensure that the IAM policy contains the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "events:PutTargets",
        "events:DescribeRule",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "events:PutRule",
        "logs:CreateLogGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

```
} ]
```

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core network**.
5. The **Overview** page opens by default.
6. Choose the **Events** tab.
7. Choose **Onboard to CloudWatch Logs Insights**.
8. When you onboard to CloudWatch Logs Insights, the following occurs:
 - A CloudWatch Events rule with the name `DO_NOT_DELETE_networkmanager_rule` is created in the US West (Oregon) Region.
 - A CloudWatch Logs group with the name `/aws/events/networkmanagerloggroup` is created in the US West (Oregon) Region.
 - A CloudWatch Events rule is configured with the CloudWatch Logs group as a target.
 - A CloudWatch resource policy named `DO_NOT_DELETE_networkmanager_TrustEventsToStoreLogEvents` is created in the US West (Oregon) Region.

To view this policy, run the following AWS CLI command:

```
aws logs describe-resource-policies --region us-west-2
```

Monitor with CloudWatch Events

You can monitor your core network using Amazon CloudWatch Events, which delivers a near-real-time stream of system events that describe changes in your resources. You set up simple rules, which then can match events and route them to one or more target functions or streams. For more information, see the [Amazon CloudWatch Events User Guide](#).

The following events can be sent to CloudWatch Events:

- [the section called "Topology changes" \(p. 83\)](#)
- [the section called "Route changes" \(p. 84\)](#)
- [the section called "Status updates" \(p. 85\)](#)
- [the section called "Policy updates" \(p. 86\)](#)
- [the section called "Segment update events" \(p. 86\)](#)

Topology changes

Topology change events occur when there are changes to your core network resources. These changes include the following:

- An edge location was added to the core network.
- An edge location was deleted from a core network.
- A Site-to-Site VPN attachment was created for a core network.
- A Site-to-Site VPN attachment was deleted from a core network.

- A VPC attachment was created for a core network.
- A VPC attachment was deleted from a core network.
- A VPN attachment was created for a core network.
- A VPN attachment was deleted from a core network.
- A Connect attachment was created for a core network.
- A Connect attachment was deleted from a core network.
- A Connect peer attachment was created for a core network.
- A Connect peer attachment was deleted from a core network.

The following example shows a topology update event where a core network VPC attachment was deleted.

```
{
  "version": "0",
  "id": "13143a7e-806e-a904-300b-ef874c56eaac",
  "detail-type": "Network Manager Topology Change",
  "source": "aws.networkmanager",
  "account": "166889823465",
  "time": "2021-09-02T12:00:38Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:networkmanager::166889823465:global-network/global-network-0de3af1d5c665d6d8",
    "arn:aws:networkmanager::166889823465:core-network/core-network-03ad314394f3f014d"
  ],
  "detail": {
    "changeType": "VPC-ATTACHMENT-DELETED",
    "changeDescription": "A VPC attachment has been deleted from a Core Network.",
    "edgeLocation": "us-east-2",
    "attachmentArn": "arn:aws:networkmanager::166889823465:attachment/attachment-092077875ecbe596b",
    "vpcArn": "arn:aws:ec2:us-east-2:212869205455:vpc/vpc-049a3a24f48fcc47d",
    "coreNetworkArn": "arn:aws:networkmanager::166889823465:core-network/core-network-03ad314394f3f014d"
  }
}
```

Route changes

Routing events occur when there are changes to your core network routes. These changes include the following:

- Routes in one or more segments have been installed.
- Routes in one or more segments have been uninstalled.

The following example shows a routing update event where a route was installed in one or more segments.

```
{
  "version": "0",
  "id": "13143a7e-806e-a904-300b-ef874c56eaac",
  "detail-type": "Network Manager Routing Update",
  "source": "aws.networkmanager",
  "account": "166889823465",
  "time": "2021-09-02T12:00:38Z",
  "region": "us-west-2",
```



```
"resources": [
  "arn:aws:networkmanager::166889823465:global-network/global-
network-0de3af1d5c665d6d8",
  "arn:aws:networkmanager::166889823465:core-network/core-network-092077875ecbe596b"
],
"detail": {
  "changeType": "SEGMENT-ROUTES-INSTALLED",
  "changeDescription": "Routes in one or more Segments have been installed.",
  "region": "us-east-2",
  "segments": [
    "development"
  ],
  "sequenceNumber": 1630585228195,
  "routes": [
    {
      "destinationCidrBlock": "169.254.137.220/30",
      "attachments": [
        {
          "attachmentId": "attachment-06d30d085574773ee",
          "attachmentType": "vpn",
          "vpnOutsideIpAddress": "3.138.83.40"
        }
      ],
      "routeType": "route_propagated",
      "routeState": "active",
      "propagatedRouteFamily": "bgp",
      "bgpAttributes": {
        "med": "0",
        "asPath": [ "AS_SEQ: [65001]" ]
      }
    }
  ],
  "coreNetworkArn": "arn:aws:networkmanager::166889823465:core-network/core-
network-03ad314394f3f"
}
}
```

Status updates

Routing events occur when there are changes to your core network status. These changes include the following:

- IPsec for a VPN connection has gone down.
- IPsec for a VPN connection has come back up.
- BGP for a VPN connection has gone down.
- BGP for a VPN connection has come back up.
- BGP for a Connect peer connection has gone down.
- BGP for a Connect peer connection has come back up.

The following example shows a status update event where IPsec for a VPN connection has come up.

```
{
  "version": "0",
  "id": "13143a7e-806e-a904-300b-ef874c56eaac",
  "detail-type": "Network Manager Status Update",
  "source": "aws.networkmanager",
  "account": "166889823465",
  "time": "2021-09-02T12:00:38Z",
  "region": "us-west-2",
```

```
"resources": [
  "arn:aws:networkmanager::166889823465:global-network/global-
network-0de3af1d5c665d6d8",
  "arn:aws:networkmanager::166889823465:core-network/core-network-092077875ecbe596b"
],
"detail": {
  "changeType": "VPN-CONNECTION-IPSEC-UP",
  "changeDescription": "IPsec for a VPN connection has come up.",
  "region": "us-west-2",
  "attachmentArn": "arn:aws:networkmanager::166889823465:attachment/
attachment-092077875ecbe596b",
  "outsideIpAddress": "35.161.41.136",
  "coreNetworkArn": "arn:aws:networkmanager::166889823465:core-network/core-
network-03ad314394f3f014d"
}
}
```

Policy updates

Routing events occur when there are changes to your core network policies. These changes include the following:

- A change set is ready to run for a core network policy.
- A change set was run successfully for a core network policy.

The following example shows a policy update event where a change set was run successfully.

```
{
  "version": "0",
  "id": "13143a7e-806e-a904-300b-ef874c56eaac",
  "detail-type": "Network Manager Policy Update",
  "source": "aws.networkmanager",
  "account": "166889823465",
  "time": "2021-09-02T12:00:38Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:networkmanager::166889823465:global-network/global-
network-0de3af1d5c665d6d8",
    "arn:aws:networkmanager::166889823465:core-network/core-network-092077875ecbe596b"
  ],
  "detail": {
    "changeType": "CHANGE-SET-EXECUTED",
    "changeDescription": "A change-set has been sucessfully executed for a Core Network
policy.",
    "policyVersionId": "1",
    "coreNetworkArn": "arn:aws:networkmanager::166889823465:core-network/core-
network-03ad314394f3f014d"
  }
}
```

Segment update events

Routing events occur when there are changes to your core network segments. These changes include the following:

- An attachment was associated with a segment.
- An attachment was mapped to a different segment.
- An attachment was disassociated from a segment.

The following example shows a segment update event where an attachment was mapped to a different segment.

```
{
  "version": "0",
  "id": "13143a7e-806e-a904-300b-ef874c56eaac",
  "detail-type": "Network Manager Segment Update",
  "source": "aws.networkmanager",
  "account": "166889823465",
  "time": "2021-09-02T12:00:38Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:networkmanager::166889823465:global-network/global-network-0de3af1d5c665d6d8",
    "arn:aws:networkmanager::166889823465:core-network/core-network-092077875ecbe596b"
  ],
  "detail": {
    "changeType": "ATTACHMENT-ASSOCIATION-MODIFIED",
    "changeDescription": "An attachment has been mapped to a different Segment.",
    "attachmentArn": "arn:aws:networkmanager::166889823465:attachment/attachment-092077875ecbe596b",
    "previousSegmentName": "development",
    "segmentName": "production",
    "edgeLocation": "us-west-2",
    "coreNetworkArn": "arn:aws:networkmanager::166889823465:core-network/core-network-03ad314394f3f014d"
  }
}
```

Monitor with CloudWatch metrics

You can monitor your core network using Amazon CloudWatch, which collects raw data and processes it into readable, near-real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your network is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the [Amazon CloudWatch User Guide](#).

You can view usage metrics for any of your core network edge locations.

View usage metrics for an edge location

View usage metrics for a specific core network edge.

To access usage metrics for a core network edge location

1. Access the Network Manager console at <https://console.aws.amazon.com/vpc/home#networkmanager/>.
2. Choose **Get started**.
3. On the **Global networks** page, choose the global network ID.
4. In the navigation pane, choose **Core networks**, and then choose the **Monitoring** tab.
5. On the **Core network** page, choose the **Show metrics** dropdown list, and then choose **Usage**.
6. From the **Core network edge** dropdown list, choose the edge location that you want to see metrics for.
7. (Optional) Metrics and events use the default time set up in the CloudWatch Events event. To set a custom time frame, choose **Custom** and then choose a **Relative** or **Absolute** time, and then choose if you want to see that date range in **UTC** or the edge location's **Local time zone**.

Choose **Add to dashboard** to add this metric to your CloudWatch dashboard. For more information about using CloudWatch dashboards, see [Using Amazon CloudWatch Dashboards](#) in the *Amazon CloudWatch User Guide*.

Note

The **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

8. The Metrics page displays the following usage metrics for the specified edge location during the chosen time frame.
 - Bytes in
 - Bytes out
 - Bytes dropped - black hole
 - Bytes dropped - no route
 - Packets in
 - Packets out

Quotas

Your AWS account has the quotas shown in the following table for AWS Cloud WAN.

The Service Quotas console also provides information about AWS Cloud WAN quotas. You can use the Service Quotas console to view default quotas and [request quota increases](#) for adjustable quotas. For more information, see [Requesting a quota increase](#) in the *Service Quotas User Guide*.

General

The following AWS Cloud WAN general quotas apply.

Quota	Default	Adjustable
Global networks per AWS account	5	Yes
Core networks per global network	1	No
Edges per Region per core network	1	No
Segments per core network	20	Yes
Retention duration (in seconds) for core network policies with out-of-date change sets	777,6000	Yes
Number of policy versions per core network	10,000	Yes
Size of a core network policy (in KB)	100	No
Number of attachments per core network	5000	Yes
Number of core network attachments per VPC	5	No
Number of Connect peers per Connect attachment	4	No
Number of devices per global network	200	Yes
Number of sites per global network	200	Yes
Number of links per global network	200	Yes

Quota	Default	Adjustable
Number of connections per global network	500	Yes

Bandwidth

Your AWS account has the following bandwidth quotas for AWS Cloud WAN.

You can use equal-cost multipath routing (ECMP) to get higher VPN bandwidth by aggregating multiple VPN tunnels. To use ECMP, the VPN connection must be configured for dynamic routing. ECMP is not supported on VPN connections that use static routing.

You can create up to four Connect peers per Connect attachment (up to 20 Gbps in total bandwidth per Connect attachment). You can use ECMP to get higher bandwidth by scaling horizontally across multiple Connect peers of the same Connect attachment or across multiple Connect attachments. Core network cannot use ECMP between the BGP peerings of the same Connect peer.

Quota	Default	Adjustable
Maximum bandwidth per VPC attachment	Up to 50 Gbps	No
Maximum bandwidth per VPN tunnel	Up to 1.25 Gbps	No
Maximum bandwidth per Connect peer (GRE tunnel) per Connect attachment	Up to 5 Gbps	No

Routing

Your AWS account has the following routing quotas for AWS Cloud WAN.

Quota	Default	Adjustable
Routes per core network (across all segments)	10,000	No
Routes advertised from VPC to core network	1,000	No
Routes advertised from core network to VPC	5,000	No
Routes advertised over VPN to core network	1,000	No
Routes advertised from core network over VPN	5,000	No
Routes advertised over Connect peer to core network	1,000	No

Quota	Default	Adjustable
Routes advertised from core network over Connect peer	5,000	No

Maximum transmission unit (MTU)

Your AWS account has the following MTU quotas for AWS Cloud WAN:

- The MTU of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data that can be passed in a single packet. A Cloud WAN core network supports an MTU of 8500 bytes for traffic between VPCs. Traffic over VPN connections can have an MTU of 1500 bytes.
- Packets with a size larger than 8500 bytes that arrive at the core network are dropped.
- The core network does not generate the FRAG_NEEDED for ICMPv4 packet, or the Packet Too Big (PTB) for ICMPv6 packet. Therefore, the Path MTU Discovery (PMTUD) is not supported.
- The core network enforces Maximum Segment Size (MSS) clamping for all packets. For more information, see [RFC879](#).